

Standardy wolności wypowiedzi na jednolitym rynku cyfrowym

Instrumenty i metody regulacji



PRAWO PUBLICZNE

Joanna Taczowska-Olszewska

**Standardy wolności wypowiedzi
na jednolitym rynku cyfrowym
Instrumenty i metody regulacji**

RECENZENCI *prof. zw. dr hab. Jacek Sobczak*
dr hab. Jędrzej Skrzypczak, prof. UAM

REDAKCJA JĘZYKOWA, KOREKTA *Agnieszka Kosińska-Gałka* AT ONCE

SKŁAD, ŁAMANIE *Wiaczesław Kryształ* AT ONCE

PROJEKT OKŁADKI *Marta Turska* AT ONCE

OKŁADKA *Juan Gris, Portrait of Josette Gris*

© Copyright by Instytut Wymiaru Sprawiedliwości, Warszawa 2024

ISBN 978-83-67149-82-2

WYDAWNICTWO INSTYTUTU WYMIARU SPRAWIEDLIWOŚCI

ul. Krakowskie Przedmieście 25, 00-071 Warszawa

SEKRETARIAT tel.: (22) 630-94-53, e-mail: wydawnictwo@iws.gov.pl

DRUK, OPRAWA „Elpil”, ul. Artyleryjska 11, 08-110 Siedlce

Spis treści

Wykaz skrótów	9
Wstęp	13
I. Standard wolności wypowiedzi – konstrukcja i zakres terminu . .	29
1. Uzasadnienie i źródła ochrony wolności wypowiedzi	29
A. Standard normatywny	32
B. Standard jurydyczny	49
C. Standard etyczny (zawodowy, korporacyjny)	63
2. Ewolucja ochrony – uwarunkowania (determinanty) jednolitego rynku cyfrowego	76
A. Internet – nowa przestrzeń korzystania z wolności wypowiedzi	76
B. Transpozycja klasycznego standardu na jednolitym rynku cyfrowym	90
3. Konstrukcja standardu	109
II. Kategorie wypowiedzi – złożoność standardu	121
1. Wypowiedzi mające znaczenie dla debaty publicznej	124
A. Wypowiedź publiczna	133
B. Wypowiedź prywatna	142
2. Treść i forma wypowiedzi	151
3. Autor wypowiedzi – zakresy odpowiedzialności	163
4. Graniczne formy wolności wypowiedzi	164

III. Wolność wypowiedzi na rynku usług cyfrowych 183

1. Harmonizacja prawa – zastępowalność standardu 183
2. Standard negocjowany – rola państw członkowskich 191
 - A. Margines swobody państwa 193
 - B. Mechanizm gilotyny 206
3. Standard kontraktowy 212
 - A. Kształtowanie treści stosunku prawnego –
dialog regulacyjny 214
 - B. Rola Komisji Europejskiej 234
 - C. Delegowanie uprawnień na podmioty prywatne –
aspekt formalny 244
 - D. Obowiązek starannego działania i neutralności
jako kontratyp – aspekt materialnoprawny 254
 - E. Instytucja dobrego samarytanina – domniemanie
prawne wzruszalne 265

IV. Mechanizmy i instrumenty ograniczania wolności wypowiedzi na rynku usług cyfrowych 273

1. Status dostawców usług społeczeństwa informacyjnego –
zakresy wpływów 273
 - A. Pośrednicy internetowi – zmiana kontratypu 276
 - B. Dostawcy usług udostępniania treści online 285
 - C. Strażnicy dostępu 289
2. Rodzaje usług cyfrowych – usługi społeczeństwa
informacyjnego 299
 - A. Usługi pośredników internetowych. 309
 - a. Usługa zwykłego przekazu 312
 - b. Caching 316
 - c. Hosting 317
 - d. Usługa wyszukiwarki internetowej 323
 - e. Usługi przetwarzania w chmurze 328

B. Usługi udostępniania treści online	331
a. Usługa udostępniania treści online	331
b. Usługa dostarczania treści cyfrowych	347
C. Usługi cyfrowe i usługi kluczowe w sektorze publicznym	361
3. Ustawowe i umowne mechanizmy ingerencji w wolność wypowiedzi	368
A. Moderowanie treści	374
B. Monitorowanie treści	389
C. Systemy rekomendacji	405
V. Odwrócony standard wolności wypowiedzi	417
1. Prejudycjalne przesłanki ochrony – aspekty materialnoprawne	417
A. Ochrona praw autorskich	417
B. Przeciwdziałanie treściom nielegalnym	439
C. Niezgodność z warunkami świadczenia usługi	458
2. Usprawiedliwiona ingerencja – aspekty formalnoprawne	469
A. Mechanizm zgłaszania i reagowania (zawisłość sporu) – środki zabezpieczające	470
B. Ryzyko systemowe – środki prewencyjne	479
C. Wykonywanie nakazów	487
3. Przesłanki legalizujące ingerencję w wolność wypowiedzi (granice ograniczeń).	496
A. <i>Ex post</i> – test szkodliwości	496
B. Antycypacyjne (<i>ex ante</i>)	506
Zakończenie	521
Bibliografia	525

Wykaz skrótów

ARC – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828 (akt o rynkach cyfrowych) (Dz.U. UE L Nr 265, s. 1)

AUC – Rozporządzenie Parlamentu Europejskiego i Rady UE 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych) (Dz.U. UE L Nr 277, s. 1 z późn. zm.)

AWM – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1083 z dnia 11 kwietnia 2024 r. w sprawie ustanowienia wspólnych ram dla usług medialnych na rynku wewnętrznym i zmiany dyrektywy 2010/13/UE (europejski akt o wolności mediów). Tekst mający znaczenie dla EOG (Dz.U. UE L poz. 1083)

Dyrektywa 2000/31 *albo* dyrektywa o handlu elektronicznym – Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (Dz.U. UE L Nr 178, s. 1)

Dyrektywa 2017/541 – Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępująca decyzję ramową Rady 2002/475/WSiSW oraz zmieniająca decyzję Rady 2005/671/WSiSW (Dz.U. UE L Nr 88, s. 6)

Dyrektywa 2019/770 albo dyrektywa o dostarczaniu treści cyfrowych – Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/770 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych i usług cyfrowych (Dz.U. UE L Nr 136, s. 1; Dz.U. UE L Nr 305, s. 60)

Dyrektywa cyfrowa – Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/770 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych i usług cyfrowych (Dz.U. UE L Nr 136, s. 1; Dz.U. UE L Nr 305, s. 60)

Dyrektywa DSM albo dyrektywa 2019/790 – Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790 z dnia 17 kwietnia 2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektywy 96/9/WE i 2001/29/WE (Dz.U. UE L Nr 130, s. 92)

Dyrektywa NIS – Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. UE L Nr 194, s. 1)

Dyrektywa towarowa – Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/771 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów sprzedaży towarów, zmieniająca rozporządzenie (UE) 2017/2394 oraz dyrektywę 2009/22/WE oraz uchylająca dyrektywę 1999/44/WE (Dz.U. UE L Nr 136, s. 28; Dz.U. UE L Nr 305, s. 63)

Dyrektywa w sprawie usług społeczeństwa informacyjnego albo dyrektywa 2015/1535 – Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/1535 z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji

w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (ujednolicenie) (Dz.U. UE L Nr 241, s. 1)

EKPC – Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5, 8, 15 oraz uzupełniona Protokołem nr 2 (Dz.U. z 1993 r. Nr 61, poz. 284 z późn. zm.)

JAŁ – Jednolity akt europejski

k.c. – Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz.U. z 2024 r., poz. 1061)

k.k. – Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. Dz.U. z 2024 r., poz. 17 z późn. zm.)

k.p.c. – Ustawa z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (t.j. Dz.U. z 2023 r., poz. 1550 z późn. zm.)

k.p.k. – Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (t.j. Dz.U. z 2024 r., poz. 37 z późn. zm.)

KPP – Karta praw podstawowych Unii Europejskiej (Dz.U. UE C z 2007 r. Nr 303, s. 1 z późn. zm.)

MPPOiP – Międzynarodowy pakt praw obywatelskich i politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (Dz.U. z 1977 r. Nr 38, poz. 167)

pr. aut. – Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz.U. z 2022 r., poz. 2509)

pr.pr. – Ustawa z dnia 26 stycznia 1984 r. – Prawo prasowe (t.j. Dz.U. z 2018 r., poz. 1914)

RODO – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. UE L Nr 119, s. 1 z późn. zm.)

Rozporządzenie w sprawie treści terrorystycznych – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym (Dz.U. UE L Nr 172, s. 79)

TFUE – Traktat o funkcjonowaniu Unii Europejskiej (Dz.U. UE C Nr 202 z 2016 r., s. 47)

TUE – Traktat o Unii Europejskiej (Dz.U. z 2004 r. Nr 90, poz. 864/30 z późn. zm.)

UKSCB – Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2023 r., poz. 913)

uos – Ustawa z dnia 14 czerwca 2024 r. o ochronie sygnalistów (Dz.U. z 2024 r., poz. 928)

usude – Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz.U. z 2020 r., poz. 344)

Wstęp

Inspiracją do podjęcia nienowej, bo wielokrotnie obecnej w doktrynie prawa, tematyki dotyczącej standardów wolności wypowiedzi były spostrzeżenia z jednej strony dotyczące zachowań komunikacyjnych użytkowników internetu i przeniesienia debaty publicznej do sfery cyfrowej oraz skutków starcia się użytkowników internetu, w tym podmiotów publicznych, z decyzjami cyfrowych gigantów o blokowaniu lub usuwaniu treści uznawanych przez nich za szkodliwe, a z drugiej strony naturalna u naukowca i prawnika potrzeba udzielenia odpowiedzi na pytanie o stałość (stabilność) standardu wolności wypowiedzi w zmieniającym się świecie nowych nawyków komunikacyjnych, zmian technologicznych, wszechpotężnego oddziaływania internetu oraz aktywności prawotwórczej w tych obszarach ze strony prawodawcy europejskiego oraz ustawodawców krajowych. Zasadniczym, ogólnym, ale niezmiernie fascynującym oraz, co należy podkreślić, obarczonym różnego rodzaju ryzykiem było pytanie o to, jaki jest obecnie standard wolności wypowiedzi. Jakie są zatem granice wolności wypowiedzi i jak są one ustalane? A przede wszystkim: czy rozwój jednolitego rynku cyfrowego i przeniesienie debaty publicznej do internetu rodzi potrzebę zmiany modelu wolności wypowiedzi, w którym na nowo oznaczone zostają jej granice? Czy na jednolitym rynku cyfrowym istnieje potrzeba budowania standardu wolności wypowiedzi, a jeśli tak, czy jest to standard wspólny dla wszystkich? Czy standard wolności wypowiedzi ma charakter intuicyjny czy – przeciwnie – stanowi konstrukcję mozolnie budowaną na przestrzeni długich okresów historycznych, a jego treść odzwierciedla doświadczenia jednostek i narodów? O ile jeszcze dekadę

temu odpowiedź na te pytania mogła stanowić zbiór truizmów niepodlegających dowodzeniu, raczej należących do stwierdzeń o charakterze notoryjnym, o tyle obecnie w związku z cyfrowym przyspieszeniem (cyfrową rewolucją) pojawia się na nowo potrzeba postawienia ogólnego pytania o standard wolności wypowiedzi, z tym jednak zastrzeżeniem, że jego ustalenie musi uwzględniać nową, cyfrową rzeczywistość. O ile zatem w pozainternetowej rzeczywistości (offline) wolność wypowiedzi stanowiła wartość autoteliczną, niekiedy absolutyzowaną (nadwartościowaną) przez Europejski Trybunał Praw Człowieka (dalej: ETPC), o tyle o wolności wypowiedzi w cyfrowej rzeczywistości można powiedzieć metaforycznie, że spowszedniała – z wysublimowanego, rzadkiego dobra, gdzie informację ujmowano jako „zanikające dobro” (fr. *le bien perissable*) zasługujące na intensywną ochronę, stała się dobrem o charakterze nadmiarowym. Zbyt intensywne, nieogłędne, nieroztropne korzystanie z wolności wypowiedzi poza wszelką kontrolą, a nadto bez jakichkolwiek mechanizmów różnicowania wartości, prawdziwości lub adekwatności wypowiedzi spowodowało obniżenie nie tylko jakości debaty publicznej, lecz także wartość samej wolności wypowiedzi. Wolność wypowiedzi została niejako spauperyzowana.

W powyżej opisanych realiach, które, jak się wydaje, nie muszą być dowodzone, albowiem wynikają z powszechnie znanych faktów i doświadczenia życiowego (dowód ze stanu powszechnej wiedzy), badawczo interesujące i konieczne stało się postawienie na nowo pytania o istnienie, a także o potrzebę istnienia standardu wolności wypowiedzi.

Celem badawczym pracy było, w pierwszej kolejności, ustalenie istnienia (albo zaprzeczenie istnieniu) standardu wolności wypowiedzi na gruncie prawa europejskiego, a zatem przede wszystkim w obszarze objętym jurysdykcją państw członkowskich UE oraz państw stron europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności (dalej: EKPC lub Konwencja)¹, a następnie – o ile taki standard istnieje – ustalenie jego treści, konstrukcji oraz zakresu zastosowania.

¹ Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5, 8, 15 oraz uzupełniona Protokołem nr 2 (Dz.U. z 1993 r. Nr 61, poz. 284 z późn. zm.).

Zakres terytorialny pracy został ograniczony do kontynentu europejskiego i regulacji regionalnych, co znajduje uzasadnienie nie tylko w prawnomiędzynarodowym statusie Polski wynikającym z przynależności naszego państwa do struktur UE oraz Rady Europy, ale przede wszystkim jest związany z rezultatem wstępnego ustalenia dotyczącego strategii i poziomu zaawansowania Europy w jej dążeniach do uregulowania i ustabilizowania stosunków prawnych na jednolitym rynku cyfrowym rozumianym jako obszar bez granic terytorialnych², który ze względu na jego usytuowanie w cyberprzestrzeni³ oraz specyfikę środków informacyjno-komunikacyjnych (ICT)⁴ wykorzystywanych przez jego użytkowników (usługobiorców i usługodawców)

² Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Strategia jednolitego rynku cyfrowego dla Europy*, pkt 3.3.1, <https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=celex%3A52015DC0192> (dostęp: 13.03.2023).

³ Przez pojęcie cyberprzestrzeni, zgodnie z przyjętą na gruncie ustaw o stanach nadzwyczajnych definicją, ustawodawca rozumie przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2019 r., poz. 700 z późn. zm.), wraz z powiązaniem pomiędzy nimi oraz relacjami z użytkownikami. W treści definicji obecne jest zarówno pojęcie informacji, jak i pojęcie systemów teleinformatycznych, które to pojęcia – jak się wydaje – stanowią jądro definicji cyberprzestrzeni (J. Taczowska-Olszewska, *Cyberprzestrzeń jako przestrzeń przetwarzania i wymiany informacji w systemach teleinformatycznych*, [w:] J. Taczowska-Olszewska, K. Chałubińska-Jentkiewicz, M. Nowikowska, *Retencja, migracja i przepływy danych w cyberprzestrzeni. Ochrona danych osobowych w systemie bezpieczeństwa państwa*, Warszawa 2019, s. 5). Ustawodawca zdecydował się na umieszczenie i zdefiniowanie pojęcia cyberprzestrzeni w treści ustaw o stanach nadzwyczajnych, tj. art. 2 ust. 1b ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (t.j. Dz.U. z 2017 r., poz. 1932), a art. 2 ust. 1a ustawy z dnia 21 czerwca 2002 r. o stanie wyjątkowym (t.j. Dz.U. z 2017 r., poz. 1928) oraz art. 3 ust. 1 pkt 4 ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (t.j. Dz.U. z 2017 r., poz. 1897).

⁴ R. Seweryn wyjaśnia, że termin „technologie informacyjno-komunikacyjne” (w skrócie TIK lub z ang. ICT – od słów: *information and communication technologies*) został po raz pierwszy użyty w 1997 r. w sprawozdaniu sporządzonym przez D. Stevena dla rządu Wielkiej Brytanii i upowszechnił się w 2000 r. za sprawą dokumentów dotyczących nowego krajowego programu nauczania w tym kraju. TIK (zamiennie określane jako technologie informacyjno-telekomunikacyjne, teleinformatyczne lub techniki informacyjne) obejmuje wszelkie działania, jakie wiążą się produkcją i wykorzystaniem urządzeń informatycznych i telekomunikacyjnych oraz wszelkie usługi, które tej produkcji i wykorzystaniu towarzyszą. Ogólnie rzecz biorąc, technologie informacyjno-komunikacyjne to rodzina technologii gromadzących, przetwarzających i przesyłających informacje w formie elektronicznej (zob. R. Seweryn, *Technologie informacyjne*

do świadczenia usług społeczeństwa informacyjnego⁵, tworzy nieograniczone w znaczeniu faktycznym możliwości przesyłania i odbierania informacji. Unia Europejska jawi się jako organizacja międzynarodowa zaangażowana w porządkowanie i regulowanie przestrzeni cyfrowej. Dowodem na zaawansowanie struktur europejskich w dziedzinie zarządzania treścią w internecie są uchwalone przez Parlament Europejski w 2022 r. dwa rozporządzenia PE i Rady, które weszły w życie w lutym 2024 r.: 1) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych – dalej: AUC)⁶ oraz 2) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828 (akt o rynkach cyfrowych – dalej: ARC)⁷ nazywane pakietem cyfrowym⁸.

Wejście w życie rozporządzeń oznaczało uchylenie zawartych w dyrektywie 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym)⁹ regulacji adresowanych do podmiotów świadczących usługi pośrednictwa internetowego w zakresie, w jakim pozwalały im one na uchylenie się od odpowiedzialności za naruszenia prawa spowodowane rozpowszechnieniem nielegalnych (szkodliwych)

i komunikacyjne – wprowadzenie w problematykę, [w:] *Technologie informacyjne i komunikacyjne na rynku turystycznym*, J. Berbeka, K. Borodako (red.), Warszawa 2017, s. 14).

⁵ Usługa społeczeństwa informacyjnego to zgodnie z art. 1 ust. 1 lit. a dyrektywy (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiającej procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (t.j. Dz.U. UE L Nr 241, s. 1) – dalej: dyrektywa w sprawie usług społeczeństwa informacyjnego lub dyrektywa 2015/1535 – każda usługa normalnie świadczona za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy.

⁶ Dz.U. L Nr 277, s. 1–102.

⁷ Dz.U. L Nr 265, s. 1–66.

⁸ Komisja Europejska (dalej: KE) używa terminu „pakiet cyfrowy”, przedstawiając na swoich stronach założenia, cele i zakres stosowania ww. rozporządzeń, <https://eur-lex.europa.eu/PL/legal-content/summary/digital-services-act.html> (dostęp: 13.09.2023).

⁹ Dz.U. L Nr 178, s. 1–16 – dalej: dyrektywa 2000/31 albo dyrektywa o handlu elektronicznym.

treści. Mechanizmy zawarte w art. 12–15 dyrektywy o handlu elektronicznym zostały częściowo przeniesione, a częściowo zastąpione narzędziami, które – oparte na mechanizmie oceny starannego działania dostawców cyfrowych, w tym platform i wyszukiwarek internetowych – pozwalają im, a niekiedy obligują do wdrażania instrumentów istotnie ingerujących w wolność wypowiedzi użytkowników internetu takich jak w szczególności monitorowanie, filtrowanie i usuwanie treści oraz blokowanie dostępu do nich.

Komisja Europejska, która wniosowała do Parlamentu Europejskiego o przyjęcie pakietu cyfrowego w proponowanym przez nią kształcie¹⁰, wskazała, że rozporządzenia cyfrowe „regulują działanie pośredników internetowych i platform internetowych, takich jak platformy handlowe, sieci społecznościowe, platformy udostępniania treści, sklepy z aplikacjami oraz portale z ofertami podróży i zakwaterowania. Akty mają na celu przede wszystkim zwalczanie dezinformacji oraz nielegalnych i szkodliwych działań w internecie. Zapewniają one użytkownikom bezpieczeństwo, chronią ich podstawowe prawa oraz tworzą sprawiedliwe i otwarte środowisko platform internetowych”¹¹. Wskazywano ponadto, że „Akt o usługach cyfrowych zapewnia ochronę praw podstawowych internautów”¹², a także, że „pod względem ambicji i charakteru regulowanych podmiotów akt o usługach cyfrowych jest bezprecedensowy wśród regulacji cyfrowych w skali globalnej. Akt ten wprowadza także innowacyjny mechanizm nadzoru”¹³.

¹⁰ Wniosek: rozporządzenie Parlamentu Europejskiego i Rady w sprawie jednolitego rynku usług cyfrowych (akt o usługach cyfrowych) i zmieniające dyrektywę 2000/31/WE, 15.12.2020 r., <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020PC0825> (dostęp: 13.09.2023).

¹¹ *Unijny akt o usługach cyfrowych: Bezpieczeństwo i odpowiedzialność uczestników interakcji w internecie*, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_pl (dostęp: 13.09.2023).

¹² *Akt o usługach cyfrowych: Rada zatwierdza przepisy o ochronie praw użytkowników internetu*, Komunikaty prasowe Rady Unii Europejskiej, 4.10.2022 r., <https://www.consilium.europa.eu/pl/press/press-releases/2022/10/04/dsa-council-gives-final-approval-to-the-protection-of-users-rights-online/> (dostęp: 13.09.2023).

¹³ *Akt o usługach cyfrowych: wstępne porozumienie Rady i Parlamentu Europejskiego uczyni internet bezpieczniejszym dla europejskich obywateli*, Komunikaty prasowe Rady Unii Europejskiej, 23.04.2022 r., <https://www.consilium.europa.eu/pl/press/press-releases/2022/04/23/digital-services-act-council-and-european-parliament-reach-deal-on-a-safer-online-space/> (dostęp: 13.09.2023).

Podkreślano, że „nowym przepisom przyświeca zasada, że co jest nielegalne offline, powinno też być nielegalne online”¹⁴.

Bezsporne jest, że pakiet cyfrowy (rozporządzenia cyfrowe) zarówno ze względu na wypowiedziane w nim *explicite* cele¹⁵, jak i ze względu na ustanowione mechanizmy i narzędzia oddziaływania na stosunki i zachowania w internecie, nie tylko wywołuje skutek polegający na ingerowaniu w wolność wypowiedzi użytkowników internetu, ale legalizuje podejmowane wobec nich działania przez dostawców platform i wyszukiwarek internetowych. To podmioty prywatne, w tym giganci cyfrowi nazywani na gruncie pakietu cyfrowego „strażnikami dostępu”¹⁶, zostały upoważnione, a zarazem zobowiązane do ustalania, wykrywania i usuwania nielegalnych treści, przy czym sposób definiowania terminu „nielegalne treści” pozostał prerogatywą Komisji Europejskiej. W konsekwencji podmiot publiczny, co wydaje się zaskakujące na gruncie przedinternetowego standardu wolności wypowiedzi, uzyskał kompetencje do kształtowania granic wolności wypowiedzi.

Powyższe spostrzeżenia stanowiły zachętę do tego, by określić tematykę badawczą, sformułować na tej podstawie tezy i hipotezy badawcze oraz ustalić metody badań, które pozwolą doprowadzić do potwierdzenia lub falsyfikacji przyjętych założeń.

Jako główne założenie badawcze (teza główna) przyjęto, że **nowe podejście prawodawcy europejskiego do problematyki regulowania wolności**

¹⁴ Tamże.

¹⁵ W art. 1 AUC wskazano, że celem przyjęcia i wdrożenia rozporządzenia jest „przyczynienie się do właściwego funkcjonowania rynku wewnętrznego usług pośrednich poprzez ustanowienie zharmonizowanych przepisów dotyczących bezpiecznego, przewidywalnego i budzącego zaufanie środowiska internetowego [...]”.

¹⁶ „Strażnik dostępu” oznacza przedsiębiorstwo świadczące podstawowe usługi platformowe, przy czym przedsiębiorstwo wskazuje się jako strażnika dostępu, jeżeli: a) wywiera znaczący wpływ na rynek wewnętrzny; b) świadczy podstawową usługę platformową będącą ważnym punktem dostępu, za pośrednictwem którego użytkownicy biznesowi docierają do użytkowników końcowych; oraz c) zajmuje ugruntowaną i trwałą pozycję w zakresie prowadzonej przez siebie działalności lub można przewidzieć, że zajmie taką pozycję w niedalekiej przyszłości (art. 3 ust. 1 AUC). Domniemywa się, że przedsiębiorstwo wywiera znaczący wpływ, jeżeli uzyskało roczny obrót w Unii wynoszący co najmniej 7,5 mld EUR w każdym z ostatnich trzech lat obrotowych oraz świadczy podstawową usługę platformową, z której w ostatnim roku obrotowym korzystało miesięcznie co najmniej 45 mln aktywnych użytkowników końcowych mających siedzibę lub miejsce pobytu w Unii (art. 3 ust. 2 lit. a i lit. b AUC).

wypowiedzi w internecie, w szczególności podyktowane potrzebą zwalczania nielegalnych treści, ma wpływ na kształt wolności wypowiedzi zarówno w środowisku cyfrowym (online), jak i poza internetem (offline). W założeniu tym tkwi zarazem presupozycja, która sprowadza się do stwierdzenia, że skoro następuje zmiana standardu (albo standardów) wolności wypowiedzi, to przyjąć należy, że takie standardy istniały także przed uchwaleniem i wejściem w życie rozporządzeń cyfrowych. Założenie to jest w niniejszej dysertacji obszernie rozwijane i uzasadniane, w szczególności poprzez omówienie w rozdziale I zatytułowanym „Standard wolności wypowiedzi – konstrukcja i zakres terminu” trzech, jak starano się wykazać, współistniejących ze sobą, niesprzecznych standardów wolności wypowiedzi, tj. standardu normatywnego, standardu orzeczniczego i standardu etycznego. W ramach głównego założenia badawczego rozstrzygane jest także zagadnienie dotyczące – jak przyjęto w pracy – „nowego podejścia prawodawcy europejskiego do regulowania wolności wypowiedzi”. Przy nakreślaniu zakresu badawczego pracy konieczne wydawało się bowiem ustalenie, czy w ogóle, a jeśli tak, to w jakim zakresie ujawnia się „nowe podejście”, a nadto czy rzutuje ono ostatecznie na kształt wolności wypowiedzi.

W celu rozstrzygnięcia głównego problemu badawczego, a w konsekwencji zweryfikowania podstawowej tezy badawczej, przyjęto szereg hipotez badawczych i towarzyszących im pytań szczegółowych. Podjęto zatem próbę udzielenia odpowiedzi na pytania dotyczące:

1. zakresu kompetencji i zadań przypisanych organom publicznym, w szczególności prawodawczym (Parlament Europejski, parlamenty krajowe) i wykonawczym (Komisja Europejska) w dziedzinie wolności wypowiedzi, w tym zakresu obowiązków pozytywnych i zmianę ich roli w odniesieniu do kształtu wolności wypowiedzi realizowanej na jednolitym rynku cyfrowym;
2. charakteru relacji pomiędzy podmiotami publicznymi a dostawcami usług cyfrowych, w tym pośrednikami internetowymi pełniącymi funkcje „strażników dostępu”;
3. przesłanek, których uwzględnienie determinuje, na gruncie pakietu cyfrowego, ocenę legalności lub nielegalności treści, a także ich źródeł oraz ich stabilności;

4. mechanizmów warunkujących wkroczenie w sferę wolności wypowiedzi jednostki, ich nazwanie oraz odniesienie do wcześniej stosowanych przesłanek legalizujących;
5. stosowania klauzul limitujących ingerencję w prawa i wolności, w tym przydatności trójelementowego testu (testu szkodliwości) do ustalania granic wolności wypowiedzi na rynku cyfrowym;
6. znaczenia i zasad stosowania kryterium starannego działania do usług świadczonych przez pośredników internetowych oraz rodzaju tych usług i okoliczności uchylających bezprawność działania dostawcy usług;
7. istnienia (albo nieistnienia) różnic w odniesieniu do sposobu, terminu i podmiotu stosującego ingerencję w wolność wypowiedzi oraz mechanizmów legalizowania tych ingerencji w porównaniu z tymi, jakie były stosowane poza środowiskiem internetowym;
8. roli sądów w procesie ustalania charakteru wypowiedzi, jej legalności oraz kontroli aktów ingerowania w wolność wypowiedzi internautów;
9. dopuszczalności prewencyjnego ograniczania wolności wypowiedzi;
10. rodzaju i celu ustanowienia nowych instytucji prawnych takich jak w szczególności: instytucja dobrego samarytanina, zaufanych podmiotów, strażników dostępu, nielegalnych treści.

Udzielenie odpowiedzi na powyżej postawione pytania służyło rozstrzygnięciu przyjętych hipotez badawczych wspierających główne założenie pracy. Skoro jako główne założenie badawcze przyjęto, że pakiet cyfrowy wywiera wpływ na kształt wolności wypowiedzi na jednolitym rynku cyfrowym, a zawarte w nim mechanizmy regulacyjne i instytucje odnoszą taki skutek, że nastąpiła zmiana standardu wolności wypowiedzi, to założeniu temu towarzyszyły hipotezy, których potwierdzenia lub falsyfikacji poszukiwano w uzyskaniu odpowiedzi na powyżej postawione pytania szczegółowe. Przyjęto zatem jako szczegółowe założenie (pierwsza hipoteza badawcza), że **prawodawca europejski powierzył organom publicznym, w szczególności Komisji Europejskiej, nowe kompetencje (regulacyjne, prawotwórcze, nadzorcze, kontrolne) w dziedzinie wolności wypowiedzi oraz nakreślił zadania, których realizacja oznacza zmianę podejścia do sposobu regulowania wolności wypowiedzi oraz obowiązków państwa w tym obszarze, co przesądza – w konsekwencji – o zmianie standardu wypowiedzi.** Ustalenie zasadności powyższego założenia ma fundamentalne znaczenie dla rozstrzygnięcia

głównej tezy badawczej z tego powodu, że w klasycznym (pozainternetowym) standardzie wolności wypowiedzi rola podmiotów publicznych (rola państwa) była, w świetle głównego nurtu orzecznictwa i wypowiedzi doktryny, ograniczona do wypełniania obowiązków negatywnych, a zatem powstrzymywania się przed podejmowaniem działań, których skutkiem mogłaby być ingerencja w wolność wypowiedzi jednostek. Przyjęcie pakietu cyfrowego odwraca tę linię w ten sposób, że nakłada na podmioty publiczne, przede wszystkim na Komisję Europejską, obowiązek sprawowania kontroli i nadzoru oraz przeciwdziałania rozpowszechnianiu nielegalnych treści.

Drugą hipotezę badawczą stanowi założenie, zgodnie z którym kształt wolności wypowiedzi (standard) zależy od sposobu definiowania terminu „nielegalne treści”, a następnie klasyfikowania wypowiedzi, w szczególności przy zastosowaniu klauzuli przepadku (art. 17 EKPC) do tych kategorii wypowiedzi, które zostały uznane za nielegalne, przy czym upoważnienie do dokonywania takiej oceny powierzono podmiotom prywatnym (strażnikom dostępu), legalizując w ten sposób dokonywane przez te podmioty ingerencje w wolność wypowiedzi jednostek (filtrowanie, moderowanie, monitorowanie, usuwanie treści, blokowanie dostępu, depozycjonowanie, demonetyzacja) oraz konstruując domniemanie o prawnej dopuszczalności takiej ingerencji nawet bez nakazu sądowego. Hipotezę tę uzasadnia spostrzeżenie dotyczące zawartego w pakiecie usług cyfrowych mechanizmu uchylania się dostawców usług pośrednich (dostawców platform i wyszukiwarek internetowych) od odpowiedzialności za naruszenia prawa spowodowane rozpowszechnioną treścią. Szczególne znaczenie prawodawca europejski przypisuje wykazaniu przez dostawców, że świadcząc usługi, działali z należytą starannością. Przesłanką, której powołanie przez dostawców może przesądzać o dochowaniu wymogów staranności, jest wypowiedziana wprost w art. 7 AUC „klauzula dobrego samarytanina”. Na gruncie tego przepisu okolicznością potwierdzającą dochowanie wymaganego poziomu staranności mogą stanowić dobrowolnie podjęte przez niego wobec użytkowników internetu czynności sprawdzające polegające w szczególności na monitorowaniu i filtrowaniu treści pod kątem jej legalności.

Kolejną, trzecią hipotezę badawczą stanowi założenie o nieadekwatności oraz niewystarczalności wzorców oceny, tak normatywnych, jak i orzeczniczych, które znajdowały zastosowanie do wypowiedzi rozpowszechnionych

poza internetem, jeśli miałyby być one odnoszone do realiów jednolitego rynku cyfrowego, nakładających na organy sądowe obowiązek zbadania dopuszczalności ograniczenia wolności wypowiedzi poprzez zastosowanie przesłanek wypracowanych na podstawie art. 10 ust. 2 EKPC, tj. proporcjonalności, niezbędności oraz istnienia ustawowej podstawy ograniczenia (trójelementowy test). O ile wskazane powyżej przesłanki są nadal stosowane w orzecznictwie ETPC, to jednak, co należy podkreślić, Trybunał posługuje się nimi dopiero na etapie kontroli sądowej, a zatem tylko w odniesieniu do tych wypowiedzi, które, przy wstępnej ocenie Trybunału dokonywanej przed merytorycznym rozpoznaniem skargi, zostały uznane za legalne. Przesłanki te nie mają zatem znaczenia i w żaden sposób nie oddziałują na rodzaj i zakres podejmowanych czynności w odniesieniu do wypowiedzi uznanych za nielegalne. Wzorzec wolności wypowiedzi powstaje zatem, co nie było dotychczas zauważane, na etapie wcześniejszym niż ocena sądowa. Nadto wzorzec ten jest rezultatem oceny dokonywanej przez podmioty prywatne przy wykorzystaniu innych niż ustalone na gruncie art. 10 ust. 2 przesłanek. Punktem odniesienia dla dokonywanej na tym etapie oceny są inne podstawy normatywne, do których nawiązanie pozwala rozstrzygnąć o legalności albo nielegalności wypowiedzi.

Zakresem przedmiotowym pracy objęte zostały zagadnienia dotyczące rozpowszechnia wypowiedzi w internecie w szerokim rozumieniu, tj. niezależnie od autora, formy i treści wypowiedzi oraz forum, na którym wypowiedź została udostępniona. Szczególną wagę przypisano dostawcom usług pośrednich jako tym podmiotom, które sprawują faktyczne władztwo nad rozpowszechnianymi w internecie treściami, ich rozliczalnością i integralnością oraz szybkością dostępu do nich. Założono bowiem, podobnie jak uczynił to prawodawca europejski w rozporządzeniach cyfrowych, że szczególnie istotne znaczenia dla realizacji wolności wypowiedzi na jednolitym rynku cyfrowym mają usługi pośrednictwa internetowego (hosting, mere conduit, caching), w tym przede wszystkim usługi dostawców bardzo dużych platform i wyszukiwarek internetowych klasyfikowanych przez prawodawcę europejskiego jako „strażników dostępu”. Zakres przedmiotowy pracy został zatem określony szeroko, zarazem jednak ze względu na przedstawiony temat badawczy oraz cele i założenia badawcze ramy analizy zostały ograniczone do tych zagadnień, które dotyczyły swobody wypowiedzi na jednolitym rynku

cyfrowym oraz statusu podmiotów będących uczestnikami tego rynku. Cel badań mógł zostać osiągnięty jednak tylko wówczas, gdy ustalenia dotyczące wolności wypowiedzi w internecie zostały odniesione do uwarunkowań korzystania z wolności wypowiedzi poza internetem, a zatem do kanonu zasad oraz stanów faktycznych stanowiących podstawę ustalenia standardów wolności wypowiedzi przez sądy krajowe i europejskie. Ustalenia te stanowiły punkt odniesienia niezbędny do stwierdzenia podobieństw i różnic w obszarze ochrony wolności wypowiedzi i gwarancji jej realizacji.

Cezury czasowe prowadzonych badań zostały wyznaczone odpowiednio do obowiązywania aktów prawnych poddanych analizie. Zważywszy, że z racji podjętej tematyki konieczne było sięgnięcie do dokumentów konstytuujących system gwarancji wolności i praw człowieka i obywatela w ujęciu uniwersalnym, a skończywszy na dokumentach i aktach prawnych oczekujących na wejście w życie, jak w szczególności akt o wolności mediów¹, badania obejmowały okres od 1948 r., w którym przyjęta została przez Zgromadzenie Ogólne ONZ Powszechna deklaracja praw człowieka (dalej: PDPC), do dnia złożenia niniejszej pracy do druku przy określeniu stanu prawnego na 2024 r.

Zakres terytorialny pracy został ograniczony do kontynentu europejskiego, a precyzyjnie do obszaru objętego jurysdykcją sądów i trybunałów europejskich (ETPC i TSUE) rozstrzygających w przedmiocie przestrzegania gwarancji wolnościowych zawartych w europejskiej Konwencji o ochronie praw człowieka i obywatela oraz Karcie praw podstawowych (dalej: KPP lub Karta).

Rozprawa składa się z pięciu rozdziałów. Na decyzję o podziale treści i konstrukcji pracy wpłynęło przekonanie o potrzebie omówienia terminu „standard wolności wypowiedzi” zarówno w nowej perspektywie badawczej ze względu na nowe uwarunkowania korzystania z wolności wypowiedzi istniejące na jednolitym rynku cyfrowym, jak i w odniesieniu do znanych modeli i wzorców wypracowanych na gruncie europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności, Karty praw podstawowych oraz innych dokumentów i aktów prawnych zawierających gwarancje wolności wypowiedzi. Konstrukcja pracy stanowi rozwinięcie przyjętych założeń

¹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1083 z dnia 11 kwietnia 2024 r. w sprawie ustanowienia wspólnych ram dla usług medialnych na rynku wewnętrznym i zmiany dyrektywy 2010/13/UE (europejski akt o wolności mediów) (Dz.U. UE L, poz. 1083) – dalej: AWM.

badawczych, co znajduje także odzwierciedlenie w zakresie i sposobie formułowania tytułów rozdziałów i sygnalizowaniu zawartych w nich zagadnień. Rozprawa dzieli się zatem na dwie części, co nie zostało wprost wypowiedziane, ale jest widoczne ze względu na zakresy przedmiotowe rozdziałów. Pierwsze dwa rozdziały mają w istocie charakter przeglądowy, a zarazem podsumowujący dorobek prawodawczy i orzecznicy z zakresu wolności wypowiedzi, bez czego nie byłoby możliwe przeprowadzenie analizy i dostrzeżenie zaistnienia zmiany zarówno koncepcji, jak i sposobu normowania wolności wypowiedzi, co stanowiło przedmiot ustaleń poczynionych w drugiej części pracy zawierających się w rozdziałach od III do V.

Pierwszy rozdział zatytułowany „Standard wolności wypowiedzi – konstrukcja i zakres terminu” obejmuje próbę ustalenia i uzasadnienia źródła ochrony wolności wypowiedzi oraz uchwycenia ewolucji jej ochrony. Wskazano na niejednorodność i brak stanowczości w kreowaniu wzorca wolności wypowiedzi, wbrew wyrażanemu często w doktrynie stanowisku. To właśnie próba „przymierzenia” tzw. klasycznego (konwencyjnego) standardu wolności wypowiedzi wypracowanego na gruncie art. 10 EKPC i art. 11 KPP do realiów korzystania z wolności wypowiedzi w internecie ujawniła *de facto* brak jednolitego standardu i skłoniła do podjęcia próby zrekonstruowania normatywnych, orzecznich i zwyczajowych (etycznych) standardów wolności wypowiedzi. Uwzględniono zatem w pierwszej kolejności treść aktów prawnych (standardy normatywne) oraz w dalszej kolejności wypowiedzi orzecznictwa (standard orzecznicy), a także – wyrażane w różnorodnych dokumentach i materiałach – stanowisko podmiotów prywatnych, w tym dziennikarzy (standard etyczny). W tej części pracy opisana została zatem ewolucja realizowanych modeli wolności wypowiedzi ze wskazaniem na nowy trend, w którym odchodzi się od definiowania wolności wypowiedzi wyłącznie jako fundamentu systemu demokratycznego i prawa człowieka na rzecz zrównania wolności wypowiedzi z innymi prawami i wolnościami, a w konsekwencji scedowania na podmioty publiczne upoważnienia do kształtowania jej treści.

Rozdział drugi odpowiada na potrzebę przeprowadzenia kategoryzacji wypowiedzi z uwzględnieniem kryterium treści, formy, autora wypowiedzi, a także okoliczności jej rozgłoszenia (prywatne, publiczne) oraz forum, na jakim wypowiedź zostaje udostępniona oraz znaczenie (funkcja), jakie wypowiedź posiada dla debaty publicznej. W literaturze i piśmiennictwie

prawniczym, pomimo że autorzy odwołują się do różnych kategorii wypowiedzi, to jednak brak jest szczegółowego ich omówienia. Wskazane powyżej kryteria, którymi posłużono się w pracy dla rozróżnienia i opisu kategorii wypowiedzi, zostały przejęte z orzecznictwa. Zarówno w orzecznictwie sądów krajowych, jak i trybunałów międzynarodowych klasyfikacja wypowiedzi ma istotne znaczenie dla ustalenia zakresu jej ochrony i dopuszczalności ingerencji. W ostatnim podrozdziale zatytułowanym „Graniczne formy wolności wypowiedzi” odniesiono się w szczególności do terminu „mowa nienawiści” stanowiącego na gruncie pakietu cyfrowego wypowiedź kwalifikowaną jako nielegalna. Zarazem jednak, na co Autorka zwraca uwagę w niniejszej dysertacji, istnieje poważna, a nawet – w ocenie Autorki – nieusuwalna trudność (przeszkoda) w ustalaniu prawnej kwalifikacji terminu „mowa nienawiści”. W konsekwencji pojęcie to zawsze będzie definiowane intuicyjnie, przy czym rozstrzygające pozostawać będą okoliczności konkretnej sprawy.

Rozdział trzeci zawiera analizę wzorców normatywnych odnoszonych do nowych sytuacji komunikacyjnych występujących na jednolitym rynku cyfrowym oraz sytuacji prawnej podmiotów występujących na tym rynku w charakterze usługodawców (dostawcy usług pośrednich nazywani także pośrednikami internetowymi) oraz usługobiorców (użytkownicy internetu). Zmiana wzorca normatywnego opartego na art. 10 EKPC i art. 11 KPP, a także przepisach konstytucyjnych państw członkowskich UE (standard negocjowany), który nakazywał uwzględnienie zasady subsydiarności oraz marginesu oceny państwa (doktryna marginesu oceny państwa), nastąpiła w związku z uchwaleniem przez Parlament Europejski rozporządzeń cyfrowych (AUC i ARC). Standard negocjowany został – na rynku usług cyfrowych – zastąpiony standardem kontraktowym. Przez standard kontraktowy należy rozumieć wzorzec pożądanych zachowań w obszarze wolności wypowiedzi, którego źródłem przestały być normy prawa powszechnie obowiązującego, a stało się porozumienie przypominające umowę kontraktową zawarte pomiędzy organem wykonawczym odpowiedzialnym za bezpieczeństwo przepływu usług na jednolitym rynku cyfrowym, tj. Komisją Europejską, a dostawcami usług pośrednictwa internetowego świadczącymi usługi bardzo dużych platform i wyszukiwarek internetowych („strażnicy dostępu”).

Rozdział czwarty został w całości poświęcony ustaleniu i omówieniu statusu dostawców usług pośrednictwa internetowego oraz rodzajom tych

usług, a także zasadom ustalania i wyłączenia odpowiedzialności pośredników za naruszenia prawa spowodowane rozpowszechnieniem wypowiedzi. Pośrednicy internetowi nie są, co do zasady, dostawcami treści cyfrowych, nie generują tych treści ani nie inicjują ich rozpowszechnienia z wykorzystaniem internetu. Podmioty te świadczą jednak usługi tego rodzaju, że bez ich pośrednictwa nie byłoby możliwe ani umieszczenie, ani przechowywanie, ani rozpowszechnienie i dostarczenie treści jej potencjalnym adresatom. Władztwo pośredników internetowych polega na tym, że sprawują oni faktyczną kontrolę nad skutecznością, szybkością, integralnością i rozliczalnością umieszczanych w internecie treści, pomimo że sami tych treści nie tworzą. Czynności techniczne wykonywane przez pośredników w ramach świadczonych przez nich usług (hosting, *mere conduit*, caching) powalają im jednak na zapoznanie się z treścią rozpowszechnianych wypowiedzi, a co za tym idzie, jeszcze przed ich publicznym udostępnieniem w internecie możliwe jest dokonywanie oceny z jednej strony pod kątem zgodności wypowiedzi z warunkami świadczonych przez nich usług, z drugiej strony pod kątem zgodności z innymi – pochodzącymi w szczególności od podmiotów publicznych – kryteriami, a w konsekwencji przeprowadzenia oceny – jak życzy sobie tego Komisja Europejska – pod kątem legalności wypowiedzi i eliminowanie z obiegu publicznego treści uznanych za nielegalne. Na jednolitym rynku cyfrowym standard wolności wypowiedzi stanowi zatem wypadkową porozumień zawieranych między pośrednikami a Komisją Europejską. Standard ten nie jest ani dziełem orzecznictwa, ani prawodawcy.

W rozdziale piątym podjęto próbę skonkretyzowania standardu wolności wypowiedzi obecnego na jednolitym rynku cyfrowym poprzez wskazanie i opisanie elementów konstruujących ten model wolności wypowiedzi. Do elementów konstytuujących standard wolności wypowiedzi na jednolitym rynku cyfrowym zaliczono, znajdujące podstawę w przepisach prawa formalnego i materialnego, zawarte w rozporządzeniach cyfrowych instytucje prawne i instrumenty uprawniające podmioty prywatne do oceny legalności wypowiedzi i rozstrzygania o dopuszczalności jej rozpowszechnienia, jak w szczególności zawarte w AUC i ARC domniemania prawne usprawiedliwiające monitorowanie, filtrowanie, blokowanie i usuwanie treści, w tym poprzez wykorzystanie zautomatyzowanych systemów kontroli treści („dobry samarytanin”). Nowy standard wolności wypowiedzi konstruują także dozwolone

na gruncie pakietu cyfrowego mechanizmy nakazujące współpracę z zaufanymi podmiotami sygnalizującymi oraz przeciwdziałania powstawaniu i minimalizowanie ryzyka systemowego. Na standard ten składa się także system kontratypów oraz ich konstrukcja, umożliwiające uchylenie się przez pośrednika internetowego od odpowiedzialności prawnej za naruszenia wywołujące szkodę lub krzywdę po stronie zarówno usługobiorcy (wówczas, gdy blokowanie lub usunięcie treści stanowiło nadmiarowe zachowanie pośrednika i miało charakter bezprawny), jak i podmiotu, którego wypowiedź dotyczyła. Na gruncie rozporządzeń cyfrowych zbudowany został system zachęt (kontratypy) i kar (kary finansowe nakładane przez Komisję Europejską za naruszenie przepisów AUC lub ARC) adresowanych do pośredników internetowych, którego uruchomienie lub wstrzymanie należy do wyłącznych kompetencji Komisji Europejskiej. Organy publiczne zyskały w ten sposób sprzymierzeńców w walce z nielegalnymi treściami.

Badania zmierzające do rozwiązania stawianych problemów badawczych i potwierdzenia hipotez były prowadzone z wykorzystaniem metody analizy i krytyki piśmiennictwa (źródeł) oraz metody badania dokumentów. Metodą badania dokumentów przemiennie z metodą analizy źródeł posłużono się także w centralnych dla prowadzonych badań partiach pracy, a zwłaszcza w tych częściach, w których konieczna stała się analiza aktów prawnych oraz orzecznictwa. W celu ustalenia odpowiedzi na zasadnicze pytania badawcze stosowano metody i reguły wykładni przepisów prawa. Przyjęto bowiem, że badanie problematyki z obszaru wolności wypowiedzi powinno obejmować analizę treści przepisów zawartych w różnej rangi aktach prawotwórczych i dokumentach należących do różnych gałęzi prawa. Do dokonania ich interpretacji posłużono się, w pierwszej kolejności, metodą wykładni językowej, a następnie historycznej, systemowej i funkcjonalnej. Przeprowadzając badania związane z tytułem rozprawy, zastosowano strukturę pracy o charakterze problemowym. W następujących po sobie kolejno rozdziałach pracy Autorka stara się rozstrzygać zasadnicze dla głównego celu badawczego zagadnienia. Dysertacja składa się z pięciu rozdziałów, z których każdy stanowi logiczne rozwinięcie i pogłębienie badań podejmowanych we wcześniejszych partiach pracy.

W ramach prowadzonych badań posiłkowano się wszystkimi rodzajami źródeł pisanych. Korzystano zarówno z bardzo bogatej literatury przedmiotu, jak i z wypowiedzi doktryny, komentarzy do treści aktów normatywnych

oraz orzecznictwa sądów, w tym sądów międzynarodowych (ETPC, TSUE). Konieczne było dokonanie selekcji na poziomie tak doboru opracowań z zakresu literatury przedmiotu, jak również analizowanych aktów normatywnych oraz orzeczeń sądowych. Celem pracy nie było bowiem, co Autorka uznała za usprawiedliwione ze względu na sposób sformułowania problemu badawczego i jego zakres, przeprowadzenie analizy treści wszystkich odnoszących się do wolności wypowiedzi obowiązujących aktów prawotwórczych i, wypowiedzianych na ich tle w piśmiennictwie i doktrynie, opinii. Szczegółowej analizie poddane zostały natomiast wypowiedzi ETPC i TSUE, a także Trybunału Konstytucyjnego RP, sprawujących kontrolę nad przestrzeganiem konwencyjnego i krajowego standardu wolności wypowiedzi. Szczególnie pomocne były wypowiedzi doktryny, w tym także komentarze oraz zbiory orzeczeń i ich omówienia. W szerokim zakresie wykorzystane zostały również prace monograficzne oraz publikacje zbiorowe i serie artykułów odnoszących się do zasadniczej dla tematu pracy problematyki.

I. Standard wolności wypowiedzi – konstrukcja i zakres terminu

1. Uzasadnienie i źródła ochrony wolności wypowiedzi

Wolność wypowiedzi stanowi jeden z zasadniczych fundamentów społeczeństwa demokratycznego i jeden z podstawowych warunków jego rozwoju oraz samorealizacji każdej jednostki¹. Europejski Trybunał Praw Człowieka już w 1976 r. sformułował fundamentalne stanowisko, w myśl którego swoboda wypowiedzi stanowi jeden z zasadniczych filarów społeczeństwa demokratycznego oraz podstawowych warunków jego postępu i rozwoju każdej osoby. Swoboda wypowiedzi nie może być przy tym ograniczana do informacji i poglądów, które są odbierane przychylnie, uważane za nieobraźliwe lub neutralne, lecz odnosi się także do tych, które obrażają, oburzają lub wprowadzają niepokój w państwie lub części społeczeństwa. Takie są wymagania pluralizmu, tolerancji, otwartości na inne poglądy, bez których nie istnieje demokratyczne społeczeństwo².

¹ Wyroki ETPC: z dnia 8 lipca 1986 r. w sprawie Lingens przeciwko Austrii, skarga nr 9815/82 (dalej: Wyrok ETPC w sprawie Lingens przeciwko Austrii), § 41; podobnie z dnia 8 listopada 2022 r. w sprawie Magdalena Bajer i in. przeciwko Polsce, skarga nr 55212/15 (dalej: Wyrok ETPC w sprawie Bajer przeciwko Polsce); wszystkie powołane w tekście wyroki ETPC dostępne są w bazie HUDOC.

² Wyroki ETPC: z dnia 7 grudnia 1976 r. w sprawie Handyside przeciwko Wielkiej Brytanii, skarga nr 5493/72, § 49 (dalej: Wyrok ETPC w sprawie Handyside przeciwko Wielkiej Brytanii); w sprawie Lingens przeciwko Austrii, skarga nr 9815/82; z dnia 23 kwietnia 1992 r. w sprawie Castells przeciwko Hiszpanii, skarga nr 11798/85 (dalej: Wyrok ETPC w sprawie Castells przeciwko Hiszpanii); z dnia 1 lipca 1997 r. w sprawie Oberschlick przeciwko Austrii, skarga nr 20834/92 (dalej: Wyrok w sprawie Oberschlick przeciwko Austrii (nr 2)).

Na istotę wolności wypowiedzi jako wartości fundamentalnej zarówno ze względu na prawo człowieka do samorozwoju i ochrony godności, jak i ze względu na jej znaczenie dla realizacji innych wolności i praw, a w konsekwencji jako wartość istotną dla całego społeczeństwa³ zwrócił uwagę Trybunał Konstytucyjny w wykładni art. 54 ust. 1 Konstytucji RP wyroku z 12.05.2008 r.⁴ Trybunał wskazał, że zarówno na gruncie filozofii, jak i w nauce prawa od lat poszukuje się uzasadnienia dla przyznawania wolności słowa ochrony szczególnej i silniejszej w porównaniu z innymi wolnościami oraz prawami. Wśród podstawowych rodzajów argumentacji wysuwanych w obronie wolności słowa wyodrębnić należy przede wszystkim takie, które odwołują się do roli tej wolności:

- a) w poszukiwaniu prawdy – niedopuszczanie do krytyki przyjmowanych w społeczeństwie opinii powoduje, że opinie te są aprobowane bez głębszego zrozumienia, przyjmowane zaś doktryny zamieniają się w martwe dogmaty tamujące rozwój myśli; tłumienie wolności słowa jest więc złem, bo pozbawia człowieka sposobności dojścia do prawdy;
- b) w funkcjonowaniu demokratycznego państwa – po pierwsze: wolność słowa zapewnia obywatelom informacje niezbędne do brania udziału w społecznych debatach i w sprawowaniu demokratycznych rządów, po drugie: wolność krytyki umożliwia poddanie osób sprawujących władzę kontroli w celu wyeliminowania korupcji oraz arbitralności i po trzecie: wolność słowa sprzyja procesowi identyfikacji interesów przez obywateli oraz ich reprezentantów, a także wspieraniu kształtowania prawidłowych relacji pomiędzy rządzonymi i rządzącymi;

³ Problem wolności w ogólności, a wolności słowa w szczególności, mieści się, jak zauważa J. Sobczak, w polu rozważań wielu dyscyplin naukowych, stając się przedmiotem analizy zarówno prawników, jak i filozofów, teologów, psychologów, socjologów w szczególności: J. Sobczak, *Prawo prasowe. Komentarz*, Warszawa 2008, s. 25–31, omówienie i odwołanie się do podstawowych tekstów. Wywody te zostały powtórzone w: W. Lis, P. Wiśniewski, Z. Husak, *Prawo prasowe. Komentarz*, Warszawa 2012, s. 7–15. W przedmiocie filozoficznych i doktrynalnych podstaw wolności prasy por. także J. Sobczak, *U podstaw liberalnej koncepcji prasy*, [w:] *Czy istnieje IV władza? Wolność prasy w teorii i praktyce*, T. Gardocka, J. Sobczak (red.), Warszawa 2010, s. 36–55; J. Waclawczyk, *Idea wolności słowa Johna Milтона*, Toruń 2008, s. 230; tenże, *Swoboda wypowiedzi politycznej w USA do roku 1918*, Toruń 2011, s. 270; M. Urbańczyk, *Liberalna doktryna wolności słowa a swoboda wypowiedzi historycznej*, Poznań 2009, s. 105.

⁴ Wyrok TK z dnia 12 maja 2008 r., SK 43/05, OSNP A 2008, nr 4, poz. 57.

- d) w promocji tolerancji – życie w społeczeństwie, w którym chroniona jest wolność słowa, uczy tolerancji dla różnych opinii oraz zachowań odmiennych od naszych własnych, co jest niezbędne dla normalnego funkcjonowania społeczeństwa pluralistycznego;
- d) jako integralnej części pewnych wartości uznawanych za fundamentalne – wolność słowa stanowi m.in. nieodzowny warunek samo-realizacji jednostki⁵.

Osiągnięcie przez człowieka szczęścia jest determinowane pełnym rozwinięciem sił jego umysłu, do czego niezbędne jest właśnie komunikowanie się, dostarczanie obywatelom informacji oraz opinii, co umożliwia im kształtowanie własnych przekonań⁶.

Trybunał Konstytucyjny podkreślił, że choć zatem jądro wolności słowa powiązane jest w pierwszej kolejności ze sferą praw osobistych, to w praktyce ta wolność jest realizowana głównie w sferze publicznej⁷, przy czym powyższe rozróżnienie jest istotne z perspektywy interpretacji treści i znaczenia art. 14 Konstytucji ustanawiającego zasadę wolności prasy jako fundamentalną zasadę ustrojową Rzeczypospolitej Polskiej⁸. W doktrynie podkreśla się, że z wolnością wypowiedzi (wolnością wyrażania poglądów) łączy się wolność komunikowania i wolność pozyskiwania i rozpowszechniania informacji. Jak zauważa J. Sobczak, obie te wolności są z jednej strony pochodną wolności wypowiedzi, z drugiej – jej sensem i zasadą. Bez wolności komunikowania się wolność wypowiedzi pozbawiona jest racji i doniosłości społecznej⁹.

⁵ Wyrok TK z dnia 12 maja 2008 r., SK 43/05, OSNP A 2008, nr 4, poz. 57.

⁶ A. Wiśniewski, *Znaczenie wolności słowa w państwie demokratycznym*, „Gdańskie Studia Prawnicze” 2000, t. 7, s. 645–658, podobnie: A. Sajó, *Freedom of expression*, Warszawa 2004, s. 17–25, szeroko na temat „funkcji mediów masowych w systemie demokratycznym” także: A. Jaskiernia, *Media masowe w demokratycznych procesach wyborczych. Standardy europejskie i uwarunkowania ich realizacji*, Warszawa 2008, s. 42–105.

⁷ L. Garlicki, *Polskie prawo konstytucyjne. Zarys wykładu*, Warszawa 2007, s. 108.

⁸ Wyrok TK z dnia 12 maja 2008 r., SK 43/05, OSNP A 2008, nr 4, poz. 57.

⁹ J. Sobczak zauważa, że przekaz wypowiedzi, który nie może być w sposób wolny odebrany przez inny podmiot oraz nie umożliwia porozumienia się co najmniej dwóch podmiotów, nie pozwala na wymianę myśli, opinii i poglądów, nie realizuje wolności wypowiedzi, może co najwyżej być przejawem wolności myśli. Zasadą wolności komunikowania jest wymiana opinii i informacji, możliwa tylko w kontaktach interpersonalnych o charakterze dwustronnym lub wielostronnym. Podkreślić jednak należy, iż „informacja” i „komunikacja” to, wbrew utartym przekonaniom, pojęcia o różnych zakresach, przy czym informacja jest tylko fragmentem komunikacji (J. Sobczak, *Komentarz do art. 11 KPP*,

W konsekwencji wskazuje się, że fundamentalne znaczenie swobody posiadania oraz wyrażania własnych przekonań i opinii sprawia, że niemożliwe byłoby obecnie skonstruowanie jakiegokolwiek katalogu praw człowieka, który pomijałby tę wolność¹⁰. Wolność wypowiedzi jest niekiedy ujmowana jako warunek korzystania z innych praw i wolności, uzyskując prymat ochrony nad tymi wartościami¹¹.

O ile akty prawne potwierdzające treść i znaczenie wolności wypowiedzi nie uległy zmianie ani co do ich treści, ani rangi, o tyle zmienił się model korzystania z wolności wypowiedzi, a także pojawiły się nowe środki komunikacji, metody i technologie komunikacyjne, a w konsekwencji zmieniły się metody i cele eksploatacji danych i informacji. Dobra te stały się przedmiotem obrotu gospodarczego, podlegają monetyzacji dokonywanej bez ograniczeń czasowych i przestrzennych poprzez kreowanie nowych zachowań komunikacyjnych, charakterystycznych dla cyberprzestrzeni. Okoliczności te wpływają także na przedmiot i charakter celów realizowanych przez organizacje międzynarodowe, w tym UE i Radę Europy. Wszystkie te zmiany, zarówno dotyczące modelu i warunków korzystania z wolności wypowiedzi, jak i funkcji, jaka jest przepisywana wolności wypowiedzi realizowanej przez nowy typ społeczeństwa intensywnie eksploatującego informacje i dane, rzutują na kształt europejskiego standardu wolności wypowiedzi.

A. Standard normatywny

Standard normatywny oznacza konstrukcję teoretyczną zawierającą zobiektywizowany i pozbawiony odniesień do stanów faktycznych oraz odporny na wypowiedzi orzecznictwa model pożądanego przez normodawcę (prawodawcę) zachowania opisanego w treści aktu prawnego, przy czym celem

[w:] *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, A. Wróbel (red.), Warszawa 2020, pkt 10).

¹⁰ A. Gliszczyńska-Grabias, *Międzynarodowy pakt praw obywatelskich (osobistych) i politycznych. Komentarz*, R. Wieruszewski (red. nauk.), Warszawa 2012, art. 19.

¹¹ I.C. Kamiński przytacza wypowiedź prezesa ETPC J.P. Costy, który w 2001 r. na Uniwersytecie Navarra stwierdził, że nadwartościowanie wolności wypowiedzi zbliża standard europejski do wypracowanego przez Sąd Najwyższy Stanów Zjednoczonych. Zob. I.C. Kamiński, *Ograniczenia swobody wypowiedzi dopuszczalne w Europejskiej Konwencji Praw Człowieka. Analiza krytyczna*, Warszawa 2010, s. 89.

zdekodowania standardu jest potrzeba zapewnienia ochrony wartości, którą normodawca uznaje za zasługującą na ochronę. Standard normatywny jest rezultatem wykładni dokonywanej w sposób najbardziej zbliżony do tego, w jaki dokonywałby jej normodawca (wykładnia autentyczna). Ustalenie standardu normatywnego wymaga zatem zastosowania reguł i metody wykładni, które w najbardziej zbliżony (autentyczny) sposób odwzorowują stanowisko historycznego prawodawcy. Wobec powyższego zasadne jest założenie, że najwłaściwsza dla ustalenia standardu normatywnego jest wykładnia autentyczna. Wykładnia autentyczna może przybierać dwie postaci:

- a) wykładni, do której prawodawca został upoważniony w konstytucji, ustawie lub innym wiążącym akcie prawnym albo
- b) wykładni, w której intencji prawodawcy poznajemy na podstawie różnego rodzaju materiałów, deklaracji lub oświadczeń, które formalnie nie mają mocy wiążącej¹².

Jak spostrzegł L. Morawski,

przypadki oficjalnej wykładni autentycznej, która miałaby formalnie moc wiążącą, są niezmiernie rzadkie, ponieważ w krajach demokratycznych, zgodnie z zasadą podziału władzy inne organy prawo stanowią, a inne stosują, natomiast zgodnie z powszechnym poglądem wykładnia wchodzi w zakres stosowania, a nie tworzenia prawa¹³.

Wykładnia autentyczna ma charakter abstrakcyjny i nie wiąże się z rozstrzyganiem indywidualnych spraw. Uważa się zarazem, że wykładnia autentyczna ma moc równą mocy interpretowanego aktu prawnego¹⁴.

Ustalenie standardu normatywnego wolności wypowiedzi przy odniesieniu się do pierwotnego znaczenia regulacji i jej źródeł wymaga zastosowania

¹² Tamże, s. 35

¹³ L. Morawski, *Zasady wykładni prawa*, Toruń 2010, s. 36.

¹⁴ L. Morawski zwraca jednak uwagę, powołując się na stanowisko Sądu Najwyższego (Zob. Uchwała SN(7) z dnia 11 lutego 2004 r., III PZP 12/03, OSNP 2004, nr 11, poz. 187), że podejście to jest nieprawidłowe, albowiem moc wiążąca wynika zawsze z treści aktu prawnego, a nie z samego faktu, kto dokonał interpretacji danego przepisu prawa (Zob. L. Morawski, *Zasady wykładni...*, s. 35).

wykładni językowej i udzielenia jej pierwszeństwa przed pozostałymi metodami interpretowania tekstu prawnego. Wykładnia, której rezultat pokrywa się z wykładnią językową, to wykładnia literalna¹⁵, przy czym powszechnie zastosowanie znajduje do tej wykładni dyrektywa języka potocznego, zgodnie z którą „normie należy przypisać takie znaczenie, jakie ma ona w języku potocznym, chyba że ważne względy przemawiają za odstępniem od tego znaczenia”¹⁶.

Standard normatywny może być pochodną ustaleń dokonywanych na gruncie jednego aktu prawnego albo systemu rozwiązań i regulacji ustanowionych przez tego samego prawodawcę i adresowanych do podmiotów objętych jego jurysdykcją. W odniesieniu do wolności wypowiedzi, która – co do zasady – jest ujmowana w prawie międzynarodowym jako prawo człowieka, stała się ona przedmiotem udzielenia gwarancji ochronnych w wymiarze uniwersalnym, tj. na gruncie Organizacji Narodów Zjednoczonych (PDPC¹⁷, Międzynarodowy pakt praw obywatelskich i politycznych – dalej: MPPOiP¹⁸), a także na płaszczyźnie regulacji regionalnych – w naszym położeniu geograficznym będą to dokumenty Rady Europy (europejska Konwencja o ochronie praw człowieka i podstawowych wolności¹⁹) oraz Unii Europejskiej (Karta praw podstawowych²⁰). Poszukiwanie normatywnego standardu wolności wypowiedzi, zważywszy, że nie stanowi zasadniczego przedmiotu dociekań w niniejszej pracy, zostanie ograniczone do podstawowych spostrzeżeń odnoszących się do wskazanych powyżej porządków prawnych przy jednoczesnym nawiązaniu do regulacji krajowych, które nie mogłyby zostać pominięte.

Gwarancje wolności wypowiedzi zostały potwierdzone w wielu aktach prawa ponadnarodowego, w szczególności w art. 10 europejskiej Konwencji

¹⁵ L. Morawski, *Zasady wykładni...*, s. 191.

¹⁶ Wyrok SN z dnia 8 maja 1998 r., I CKN 664/97, OSNC 1999, nr 1, poz. 7, podobnie: Uchwała SN(7) z dnia 9 września 2008 r., III CZP 31/08, OSNC 2009, nr 3, poz. 36.

¹⁷ Powszechna deklaracja praw człowieka (przyjęta i proklamowana rezolucja Zgromadzenia Ogólnego ONZ 217 A (III) w dniu 10 grudnia 1948 r.), <http://www.un-documents.net/a3r217.htm> (dostęp: 13.09.2023).

¹⁸ Międzynarodowy pakt praw obywatelskich i politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (Dz.U. z 1977 r. Nr 38, poz. 167).

¹⁹ EKPC została przyjęta przez Komitet Ministrów 4 listopada 1950 r. w Rzymie.

²⁰ Karta praw podstawowych Unii Europejskiej (Dz.U. UE C z 2007 r., Nr 303, s. 1 z późn. zm.).

o ochronie praw człowieka i podstawowych wolności²¹, a także art. 11 Karty praw podstawowych²² oraz w art. 19 Międzynarodowego paktu praw obywatelskich i politycznych²³ i w art. 19 Powszechnej deklaracji praw człowieka²⁴. Na gruncie prawa krajowego wolność wypowiedzi została zagwarantowana w art. 54 i art. 14 Konstytucji, przy czym zasadne wydaje się podkreślenie, że niektóre jej aspekty i charakterystyczne przejawy zostały poddane ochronie w odrębnych postanowieniach Konstytucji, a więc w art. 73 (wolność twórczości artystycznej, badań naukowych, nauczania i korzystania z dóbr kultury), art. 61 (dostęp do informacji publicznej), art. 74 ust. 3 (dostęp do informacji o środowisku), art. 53 ust. 2 (wolność uzewnętrzniania religii)²⁵.

²¹ Art. 10 EKPC ma następujące brzmienie: „1. Każdy ma prawo do wolności wyrażania opinii. Prawo to obejmuje wolność posiadania poglądów oraz otrzymywania i przekazywania informacji i idei bez ingerencji władz publicznych i bez względu na granice państwowe. Niniejszy przepis nie wyklucza prawa państw do poddania procedurze zezwoleń przedsiębiorstw radiowych, telewizyjnych lub kinematograficznych. 2. Korzystanie z tych wolności pociągających za sobą obowiązki i odpowiedzialność może podlegać takim wymogom formalnym, warunkom, ograniczeniom i sankcjom, jakie są przewidziane przez ustawę i niezbędne w społeczeństwie demokratycznym w interesie bezpieczeństwa państwowego, integralności terytorialnej lub bezpieczeństwa publicznego ze względu na konieczność zapobieżenia zakłóceniu porządku lub przestępstwu, z uwagi na ochronę zdrowia i moralności, ochronę dobrego imienia i praw innych osób oraz ze względu na zapobieżenie ujawnieniu informacji poufnych lub na zagwarantowanie powagi i bezstronności władzy sądowej”.

²² Art. 11 KPP ma następujące brzmienie: „1. Każdy ma prawo do wolności wypowiedzi. Prawo to obejmuje wolność posiadania poglądów oraz otrzymywania i przekazywania informacji i idei bez ingerencji władz publicznych i bez względu na granice państwowe. 2. Szanuje się wolność i pluralizm mediów”.

²³ Art. 19 ma następujące brzmienie: „1. Każdy człowiek ma prawo do posiadania bez przeszkód własnych poglądów. 2. Każdy człowiek ma prawo do swobodnego wyrażania opinii; prawo to obejmuje swobodę poszukiwania, otrzymywania i rozpowszechniania wszelkich informacji i poglądów, bez względu na granice państwowe, ustnie, pismem lub drukiem, w postaci dzieła sztuki bądź w jakiegokolwiek inny sposób według własnego wyboru. 3. Realizacja praw przewidzianych w ustępie 2 niniejszego artykułu pociąga za sobą specjalne obowiązki i specjalną odpowiedzialność. Może ona w konsekwencji podlegać pewnym ograniczeniom, które powinny być jednak wyraźnie przewidziane przez ustawę, i które są niezbędne w celu: a) poszanowania praw i dobrego imienia innych; b) ochrony bezpieczeństwa państwowego lub porządku publicznego albo zdrowia lub moralności publicznej”.

²⁴ Art. 19 PDPC ma następujące brzmienie: „Każdy człowiek ma prawo wolności opinii i wyrażania jej; prawo to obejmuje swobodę posiadania niezależnej opinii, poszukiwania, otrzymywania i rozpowszechniania informacji i poglądów wszelkimi środkami, bez względu na granice”.

²⁵ Zauważono, że podobny sposób ochrony polegający na uwzględnieniu w konstytucji jako akcie prawnym najwyższej rangi wielu aspektów wolności wypowiedzi, przyznając

Każdy z powyżej wskazanych aktów prawnych może stanowić odrębny wzorzec normatywny, na podstawie którego jest możliwe konstruowanie standardów wolności wypowiedzi, przy czym standardy te na gruncie wykładni językowej są niesprzeczne. Jednakże, ze względu na odmienne usytuowanie źródeł ochrony wartości, jaką jest wolność wypowiedzi, oraz zawarte we wskazanych powyżej aktach normatywnych zakres i metody ochrony, a także moment historyczny, w którym powstały, dopuszczalne wydaje się założenie, że generują one zbliżone, aczkolwiek nie tożsame wzorce normatywne. Prawodawca, zważywszy na cele, jakie chce osiągnąć, ustanawia odmienny standard wolności wypowiedzi, co rzutuje z jednej strony na status państwa jako adresata pozytywnych i negatywnych obowiązków względem tej wolności, a z drugiej strony na status jednostki ze względu na granice, w jakich mieścić się winno korzystanie przez nią z wolności wypowiedzi, by nie spotkała się z negatywną reakcją ze strony państwa.

Najbardziej lakoniczne i najmniej kazuistyczne gwarancje wolności wypowiedzi zawiera Powszechna Deklaracja Praw Człowieka. Zgodnie z art. 19 Deklaracji „Każdy człowiek ma prawo wolności opinii i wyrażania jej; prawo to obejmuje swobodę posiadania niezależnej opinii, poszukiwania, otrzymywania i rozpowszechniania informacji i poglądów wszelkimi środkami, bez względu na granice”. Prawa człowieka sformułowane w tym akcie są normami zwyczajowymi, a w konsekwencji – co ma fundamentalne znaczenie dla oceny ich rangi w hierarchii praw i wolności, w tym tzw. wolności drugiej i kolejnej generacji²⁶, oznacza, że „prawa sformułowane w tym dokumencie wiążą

im samoistną ochronę prawną, występuje w niektórych krajowych systemach prawnych, np. w Szwajcarii. W Szwajcarii, od czasu wejścia w życie nowej konstytucji federalnej w dniu 1 stycznia 2000 r., wolność słowa jest częścią wielu gwarancji konstytucyjnych, z których wszystkie mają na celu ochronę wolności wyrażania opinii, swobodnego rozpowszechniania i swobodnego przyjmowania opinii. Konstytucja Federalna świadczy o tej różnorodności, grupując pod płaszczykiem wolności komunikacji wolność opinii i informacji (art. 16), wolność mediów (prasy, radia i telewizji, a także „inne formy rozpowszechniania produkcji i informacji wchodzące w zakres telekomunikacji publicznej”, art. 17), wolność nauki (art. 20) i wolność sztuki (art. 21). Oprócz tego wachlarza istnieją inne gwarancje, które odgrywają główną rolę w zakresie rozpowszechniania idei, takie jak wolność języka (art. 18), wolność zgromadzeń (art. 22) i zrzeszania się (art. 23) lub prawo do składania petycji (art. 33); zob. M. Hottelier, E. McGregor, *La liberté d'expression: regards croisés sur ses sources, son contenu et ses fonctions*, „Cahiers de la recherche sur les droits fondamentaux” 2010, nr 8, DOI: <https://doi.org/10.4000/crdf.6122>, s. 13.

²⁶ H. Izdebski, *Fundamenty współczesnych państw*, Warszawa 2007, s. 43.

wszystkie państwa, niezależnie od stopnia ratyfikacji i przystąpienia do poszczególnych (tak powszechnych, jak i regionalnych) umów dotyczących praw człowieka”²⁷. Jak zauważa J. Sobczak, „Powszechna Deklaracja Praw Człowieka zdała się stać na gruncie absolutnych, czyli naturalnych praw człowieka”²⁸.

Powszechna deklaracja praw człowieka oraz MPPOiP „stanowią podstawowe ramy wolności słowa. Współgrają z nimi inne dokumenty ONZ i tzw. organizacji wyspecjalizowanych, wśród nich zaś: Międzynarodowa konwencja prawa sprostowań z 1952 r. (mająca gwarantować przedstawianie faktów bez dyskryminacji, we właściwym kontekście, z poszanowaniem praw człowieka, w duchu międzynarodowego zrozumienia i współpracy, dająca prawo przedstawienia zainteresowanemu swojej wersji, jeśli uznaje on relacje za fałszywe lub niepełne), Międzynarodowa konwencja w sprawie likwidacji wszelkich form dyskryminacji rasowej z 1969 r. (deklarująca potrzebę zniesienia barier rasowych w przekazie informacji) oraz Deklaracja UNESCO w sprawie podstawowych zasad dotyczących udziału organów informacji w umacnianiu pokoju i zrozumienia międzynarodowego w popieraniu praw człowieka i w walce przeciwko rasizmowi i podżeganiu do wojny wydana w Paryżu 22.11.1978 r.”²⁹.

Standard normatywny w ujęciu Powszechnej deklaracji praw człowieka i Międzynarodowego paktu praw obywatelskich i politycznych oraz przyjętych na łonie ONZ aktów prawnych o zasięgu uniwersalnym odwołuje się do prawnonaturalnych koncepcji wolności wypowiedzi jako przyrodzonej wolności, której źródłem jest fakt bycia człowiekiem i jego podobieństwo do osobowego Boga oraz, co się z tym wiąże, posiadanie niezbywalnej godności. W teorii prawa naturalnego koncepcja przyrodzonych praw i wolności znajdowała uzasadnienie w potrzebie ochrony godności jako wartości fundamentalnej i niezależnej od woli państwa. Rolą państwa było zatem potwierdzenie

²⁷ J. Symonides, *Powszechna Deklaracja Praw Człowieka (po 60 latach od jej przyjęcia)*, „Państwo i Prawo” 2008, nr 12, s. 3–16.

²⁸ J. Sobczak, *Komentarz...*, wraz z cytowaną tam literaturą, a w szczególności: H. Andrzejczak, *Filozoficzne podstawy Powszechnej Deklaracji Praw Człowieka*, „Roczniki Filozoficzne” 1966, nr 14, s. 88; K. Motyka, *50 lat minęło. Powszechna Deklaracja Praw Człowieka i jej credo*, „Prawo i Życie” 1998, nr 39; K. Motyka, *Wprowadzenie. O prawach człowieka i ich ochronie*, [w:] *Prawa człowieka. Wprowadzenie, wybór źródeł*, Lublin 2004, s. 41–44.

²⁹ *Biuletyn: Przegląd Polskiego Komitetu do spraw UNESCO*, I. Morżoł (red.), Warszawa 2014, s. 47.

i gwarantowanie wolności wypowiedzi, a nie jej kształtowanie, odbieranie lub nadawanie. W konsekwencji udział państwa w ochronie wolności polegał na powstrzymaniu się od ingerowania w tę wartość (obowiązek negatywny), a tylko w rzadkich przypadkach za dopuszczalne uznawano angażowanie się państwa w jej ochronę poprzez wytyczanie granic tej wolności.

Wobec niezmienionego, statycznego, zawartego w art. 19 Powszechnej deklaracji praw człowieka i art. 19 MPPOiP wzorca wolności wypowiedzi oraz stabilnej, odnoszonej do praw człowieka koncepcji jego realizacji nie kwestionowano źródeł tej wolności i znaczenia prawa naturalnego w uniwersalnym systemie praw człowieka. Obecnie pojawiają się jednak stanowiska, których autorzy nie tyle negują treść określonych w PDPC i MPPOiP wolności, co kwestionują termin „prawa człowieka”. Termin ten uznają za anachroniczny³⁰.

Termin „prawa człowieka” zaczął być, pod wpływem nauki niemieckiej³¹, interpretowany w połączeniu z pojęciem skutecznego środka ochrony. Wskazuje się zatem na jego przydatność wówczas, gdy istnieją instrumenty służące egzekwowaniu praw człowieka, przy czym rolą państwa jest zapewnienie skutecznego środka ochrony. W ten sposób pod pozorem ochrony praw człowieka następuje wzmocnienie roli państwa jako – w rezultacie – kształtującego zakres wolności i praw.

Zważywszy na regionalny kontekst prawa, w szczególności zakres jego terytorialnego obowiązywania, a w konsekwencji zasadność odwoływania się przez państwa strony – do wspólnych tradycji historycznych, kulturowych i – szerzej – cywilizacyjnych, szczególne znaczenie na gruncie europejskim ma europejska Konwencja o ochronie praw człowieka i podstawowych wolności. Ustanowione na gruncie EKPC i KPP wzorce normatywne odchodzą od odwołań do koncepcji prawa naturalnego, upatrując źródła ochrony

³⁰ G. Koubi, *Droits de l'homme et droits de la personne: réflexion sur l'imprudence d'une distinction*, „International Journal of Psychology” 2000, t. 6, nr 15, s. 38; cyt. za: S. Etoa, *La terminologie des „droits fondamentaux” dans la jurisprudence du Conseil constitutionnel*, „Cahiers de la recherche sur les droits fondamentaux” 2011, nr 9, DOI: <https://doi.org/10.4000/crdf.5390>, s. 29.

³¹ Prawa człowieka są rozumiane przede wszystkim jako szczególna kategoria konstytucyjnych praw podmiotowych i jako takie kwalifikowane przez ustawę zasadniczą. Zauważa się, że „Ta transformacja sposobu pojmowania przedmiotu nie pozostaje bez wpływu na to pojęcie, ponieważ dąży do uwypuklenia strukturyzującego charakteru praw podstawowych”; zob. S. Etoa, *La terminologie...*, s. 25.

wolności wypowiedzi w prawie pozytywnym i roli państwa³². Zauważa się, że w dokumentach wspólnot europejskich pojęcie „prawa człowieka” było używane wyjątkowo rzadko. W jego miejsce posilkowano się wypracowanym w orzecznictwie TSUE (dawniej TS) terminem „**prawa podstawowe**”. Określenie to znalazło się także w art. 6 ust. 2 TUE oraz w samym tytule KPP. Jednak ani TSUE w swoich judykatach, ani żaden z aktów normatywnych nie definiują pojęcia „prawa podstawowe”³³. Podkreślono ponadto, że sformułowane w Karcie prawa podstawowe „zostały powiązane z sześcioma wartościami ogólniejszymi (godność, wolność, równość, solidarność, obywatelstwo UE, sprawiedliwość) i podzielone na tyleż grup praw”³⁴.

Polska ratyfikowała Konwencję o ochronie praw człowieka i podstawowych wolności dopiero 19 stycznia 1993 r. i z tą datą weszła w życie na terytorium RP. Tekst Konwencji uzupełniony został o 15 protokołów (1–14 oraz pozostający w mocy przez kilkanaście miesięcy Protokół 14bis), z których sześć uzupełnia katalog praw jednostki, a pozostałe mają charakter instytucjonalny i proceduralny. Do ostatniej kategorii aktów zaliczyć należy także protokoły stanowiące ostatni, jak dotąd, etap reformy Trybunału: Protokół 15 i Protokół 16. Pierwszy z aktów przewiduje m.in. wpisanie doktryny marginesu swobody uznania (marginesu oceny) i zasady subsydiarności do preambuły Konwencji³⁵. Zmiany te, ze względu na wzmocnienie roli Trybunału, nie pozostają bez wpływu na kształt normatywny wolności wypowiedzi.

³² Zgodnie z orzecznictwem Europejskiego Trybunału Praw Człowieka, oprócz negatywnych obowiązków związanych z wolnościami, państwo ma obowiązki pozytywne, co pociąga za sobą nakaz interwencji ze strony władz publicznych. Obowiązek poszanowania swobód jest zatem połączony z obowiązkiem aktywnej ochrony tych gwarancji, aby zapewnić im pełną skuteczność. Wolność słowa nie jest wyjątkiem od tej innowacyjnej wizji; zob. M. Hottelier, E. McGregor, *La liberté d'expression...*, s. 21. Na pozytywne obowiązki państwa wynikające z art. 10 EKPC Trybunał zwrócił uwagę w szczególności w wyrokach: z dnia 6 maja 2003 r. w sprawie Appleby przeciwko Wielkiej Brytanii, skarga nr 44306/98, § 39 (dalej: Wyrok ETPC w sprawie Appleby przeciwko Wielkiej Brytanii); z dnia 16 grudnia 2008 r. w sprawie Khurshid Mustafa i Tarzibachi przeciwko Szwecji, skarga nr 23883/06, § 31.

³³ J. Sobczak, *Komentarz...*

³⁴ C. Mik, *Europejskie prawo wspólnotowe. Zagadnienia teorii i praktyki*, Warszawa 2000, s. 85; cyt. za: J. Sobczak, *Komentarz...*

³⁵ Z. Kotuła, *Protokół 15 do europejskiej konwencji praw człowieka: doktryna marginesu swobody uznania i zasada subsydiarności w kontekście reformy ETPCz*, „Studenckie Prace Prawnicze, Administratywistyczne i Ekonomiczne” 2017, s. 86.

Polska ratyfikowała Protokół nr 15 w drodze ustawy z dnia 9 kwietnia 2015 r.³⁶ W uzasadnieniu do projektu ustawy zauważono, że Protokół nr 15 dodaje do preambuły Konwencji nowy ustęp, zawierający odwołania do zasady subsydiarności, mechanizmu ochronnego Konwencji i do doktryny marginesu oceny państwa oraz podkreślający obowiązek zapewnienia przez państwo pełnej skuteczności praw i wolności określonych w Konwencji. Przedmiotowe zasady – jak wskazano w uzasadnieniu – zostały wypracowane w toku rozwoju orzecznictwa Trybunału i z uwagi na swą doniosłość nie są kwestionowane przez strony Konwencji. Odzwierciedlają one obowiązek ciążyący na państwach, tj. obowiązek skutecznego zapewnienia praw i wolności określonych w Konwencji każdej osobie podlegającej ich jurysdykcji oraz zagwarantowania skutecznego krajowego środka odwoławczego każdemu, kogo prawa i wolności zostały naruszone.

Ratyfikacja Protokołu nr 15 oznacza zatwierdzenie prawotwórczej aktywności ETPC i potwierdza siłę, z jaką orzecznictwo ETPC oddziałuje na treść norm prawa konwencyjnego. W orzecznictwie Trybunału podkreślano bowiem, że państwa cieszą się pewnym marginesem oceny co do sposobu zagwarantowania praw i wolności zawartych w Konwencji, co jest zgodne z subsydiarnym charakterem ochrony zapewnianej przez Konwencję, jednakże realizacja tych zasad również powinna pozostać pod kontrolą Trybunału. Zostały one bowiem powiązane z jednej strony z odpowiedzialnością państw za zapewnienie praw i wolności określonych w Konwencji i jej Protokołach, z drugiej zaś strony z nadzorczą rolą Trybunału, który bada, czy decyzje podjęte przez władze krajowe są zgodne z Konwencją³⁷. Wskazując na przewidywane skutki ratyfikacji Protokołu nr 15, ustawodawca krajowy założył, że wzmocnienie pozycji Trybunału nastąpiło poprzez „uwzględnienie w preambule Konwencji dwóch najdonioślejszych zasad interpretacyjnych wypracowanych w orzecznictwie Trybunału – zasady subsydiarności mechanizmu ochronnego

³⁶ Ustawa z dnia 9 kwietnia 2015 r. o ratyfikacji Protokołu nr 15 zmieniającego Konwencję o ochronie praw człowieka i podstawowych wolności, sporządzonego w Strasburgu dnia 24 czerwca 2013 r. (Dz.U., poz. 763).

³⁷ Rządowy projekt ustawy o ratyfikacji Protokołu nr 15 zmieniającego Konwencję o ochronie praw człowieka i podstawowych wolności, sporządzoną w Rzymie dnia 4 listopada 1950 r., Druk Sejmowy nr 3056, <https://www.sejm.gov.pl/Sejm7.nsf/PrzebiegProc.xsp?nr=3056> (dostęp: 23.02.2024).

Konwencji oraz doktryny marginesu oceny państwa – nadając im dzięki temu zwiększoną rangę³⁸. Jak zauważono,

z uwagi na dużą popularność i zaufanie, jakim cieszy się Trybunał wśród obywateli polskich, będzie to miało pozytywne skutki w postaci szybszego rozpatrywania spraw obywateli polskich, toczących się przed Trybunałem³⁹.

Struktura i treść art. 10 ust. 1 EKPC jest w dużej mierze zbieżna z tekstem art. 11 KPP⁴⁰. Zbieżność regulacji gwarantujących – jak deklaruje prawodawca europejski – ten sam poziom ochrony wolności wypowiedzi na płaszczyźnie dwóch systemów, tj. systemu Rady Europy (systemu konwencyjnego) i systemu Unii Europejskiej (systemu traktatowego), potwierdza treść art. 52 ust. 3 KPP. Zgodnie z tym przepisem „w zakresie, w jakim niniejsza Karta zawiera prawa, które odpowiadają prawom zagwarantowanym w europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności, ich znaczenie i zakres są takie same jak praw przyznanych przez tę konwencję”. Artykuł 52 ust. 3 KPP, nazywany niekiedy klauzulą „transferową”, reguluje relacje między postanowieniami Karty i (materialnoprawnymi) postanowieniami EKPC oraz zasady wykładni odnośnych postanowień Karty (zdanie pierwsze), a także pozwala uznać standard ochronny, gwarantowany postanowieniami konwencji, za standard minimalny (zdanie drugie)⁴¹. Zgodnie z art. 52 ust. 1 Karty wszystkie ograniczenia w korzystaniu z praw i wolności uznanych w Karcie muszą być przewidziane ustawą i szanować istotę tych praw i wolności. Z zastrzeżeniem zasady proporcjonalności ograniczenia mogą być wprowadzone wyłącznie wtedy, gdy są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób.

³⁸ Tamże, pkt 1.

³⁹ Tamże, pkt 3.

⁴⁰ J. Sobczak zwraca uwagę, że w art. 11 ust. 2 KPP zawarto treść, która nie znalazła się w tekście art. 10 EKPC, a mianowicie, że szanowana jest wolność mediów i ich pluralizm. Z objaśnień Sekretariatu Konwencji wynika, że tekst ten wyraża skutki w sferze wolności mediów, które wynikają w szczególności z „orzecznictwa Trybunału Sprawiedliwości”; zob. J. Sobczak, *Komentarz...*

⁴¹ A. Wróbel, *Komentarz do art. 52 KPP*, [w:] *Karta Praw...*, pkt 44.

KPP⁴² została włączona na podstawie art. 4 Traktatu o Unii Europejskiej⁴³ do prawa pierwotnego UE, co oznacza, że wobec adresatów zawartych w niej postanowień wywołuje bezpośredni skutek prawny, ingerując w system prawa wewnętrznego związanych nimi państw członkowskich UE. W literaturze często pomijana jest kwestia obowiązywania, w ścisłym rozumieniu tego terminu, Karty praw podstawowych na gruncie prawa polskiego. Ograniczano się bowiem często do wskazywania zakresu jej stosowania ze względu na treść art. 51–53 KPP, co *de facto* prowadziło do odrzucenia tezy, zgodnie z którą złożony przez Polskę i Wielką Brytanię w 2008 r. Protokół nr 30 w sprawie stosowania Karty praw podstawowych Unii Europejskiej do Polski i Wielkiej Brytanii⁴⁴ skutecznie wyłączył stosowanie Karty w stosunkach pomiędzy Polską a Unią Europejską (skutek opt-out). Tymczasem Protokół polsko-brytyjski zarówno ze względu na jego treść, jak i charakter prawny jako umowy międzynarodowej, a także okoliczności jego złożenia, motywy oraz argument wskazujący na niezmienność stanowiska Polski, która nigdy z jego postanowień się nie wycofała, nakłada obowiązek dokonywania wykładni prawa europejskiego przy uwzględnieniu zmian zachodzących w prawie europejskim, a także zdarzeń i faktów prawnych oddziałujących na sytuację Polski w strukturach UE. Przyjąć bowiem trzeba, że ewentualne zastosowanie KPP w stosunkach z UE wymaga nie tylko uwzględnienia – zarówno w polskim, jak i europejskim orzecznictwie – wskazanych w art. 51–53 ograniczeń zastosowania, ale przede wszystkim dokonania ustalenia opartego na Protokole nr 30 zakresu, w jakim stosowanie KPP zostało wyłączone.

Artykuł 10 Konwencji nie gwarantuje całkowicie nieograniczonej wolności wypowiedzi. Zgodnie z ust. 2 tego przepisu wolność wypowiedzi pociąga za sobą „obowiązki i odpowiedzialność” nawet w odniesieniu do spraw budzących poważne zaniepokojenie opinii publicznej. Ingerencja jest dopuszczalna wówczas, gdy jest przewidziana w ustawie, a nadto jest uzasadniona

⁴² Karta praw podstawowych z dnia 7 grudnia 2000 r., w brzmieniu dostosowanym 12 grudnia 2007 r. w Strasburgu (Dz.U. UE C z 2012 r. Nr 326, s. 391).

⁴³ Traktat o Unii Europejskiej i Traktat o funkcjonowaniu Unii Europejskiej (Dz.U. UE C z 2008 r. Nr 115/01), <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:C2008/115/01&from=PL> (dostęp: 22.03.2024).

⁴⁴ Protokół (nr 30) w sprawie stosowania Karty praw podstawowych Unii Europejskiej do Polski i Zjednoczonego Królestwa stanowiący załącznik do Traktatu o Unii Europejskiej i Traktatu o funkcjonowaniu Unii Europejskiej.

realizacją ważnego celu społecznego, jednakże tylko wtedy, gdy wkroczenie w wolność wypowiedzi nie narusza istoty tej wolności, a zastosowana sankcja jest proporcjonalna w stosunku do uprawnionego celu⁴⁵. Z innego punktu widzenia, ktokolwiek korzysta z wolności wypowiedzi, podejmuje się „obowiązków i odpowiedzialności”, których zakres zależy od jego sytuacji i środków technicznych, którymi się posługuje. Trybunał nie może pominąć „obowiązków” i „odpowiedzialności” takiej osoby, gdy bada, czy „ograniczenia” lub „kary” sprzyjały ochronie innej konwencyjnej wartości, co czyniło je „koniecznymi” w „społeczeństwie demokratycznym”⁴⁶.

Nie ulega wątpliwości, że na płaszczyźnie prawa europejskiego istnieją dwa wzorce normatywne tj. pierwszy wynikający z treści art. 10 EKPC oraz drugi ustanowiony w art. 11 KPP. Kwestią podstawowej wagi jest ustalenie, w jakim zakresie wzorce te są tożsame albo stwierdzenie, że konkurują ze sobą bądź są sprzeczne. Ewentualnej niespójności lub sprzeczności tych wzorców nie może usuwać zawarta w art. 52 ust. 3 KPP dyrektywa interpretacyjna (klauzula transferowa). Wydaje się zarazem, że wołą prawodawcy europejskiego nie było odwzorowywanie standardu konwencyjnego, lecz jego modyfikacja. Za takim stanowiskiem przemawia treść art. 52 ust. 3 zdanie drugie. Wskazano w nim, że chociaż Karta zawiera prawa, które odpowiadają prawom zagwarantowanym w EKPC, to jednak „Niniejsze postanowienie nie stanowi przeszkody, aby prawo Unii przyznawało szerszą ochronę”. Zgodnie z wykładnią art. 11 KPP zawartą w dokumencie towarzyszącym uchwaleniu KPP zatytułowanym „Wyjaśnienia dotyczące Karty praw podstawowych”⁴⁷ ma ona charakter blankietowy i została ograniczona przez prawodawcę unijnego do odesłania do treści art. 10 EKPC. W wyjaśnieniach wskazano, że art. 11 KPP „odpowiada” art. 10 EKPC.

Karta zawiera prawa, które nie zostały przyznane wyraźnymi postanowieniami EKPC, lecz co najwyżej zostały uznane za mieszczące się w zakresie innego prawa, przyznanego wprost w EKPC, np. określone w art. 3 KPP prawo

⁴⁵ Wyroki ETPC: z dnia 26 kwietnia 1979 r. w sprawie *The Sunday Times* przeciwko Wielkiej Brytanii, skarga nr 6538/74, § 62 (dalej: Wyrok ETPC w sprawie *The Sunday Times* przeciwko Wielkiej Brytanii (nr 1)); z dnia 27 maja 2003 r. w sprawie *Skalka* przeciwko Polsce, skarga nr 43425/98, § 35 (dalej: Wyrok ETPC w sprawie *Skalka* przeciwko Polsce).

⁴⁶ Wyrok ETPC w sprawie *Handyside* przeciwko Wielkiej Brytanii.

⁴⁷ Wyjaśnienia dotyczące Karty praw podstawowych.

do integralności, które nie ma swojego literalnego odpowiednika w przepisach EKPC⁴⁸. A. Wróbel zauważa, że brzmienie odnośnych przepisów nie jest miarodajnym kryterium ustalania, czy prawa przyznane tymi przepisami odpowiadają sobie w rozumieniu art. 52 ust. 3 KPP. Zarazem ustalenie, czy prawa są podobne, wymaga porównywania przedmiotu regulacji przepisów gwarantujących dane prawo i zakresu ochrony gwarantowanej tymi przepisami. Z tej perspektywy wydaje się nie być oczywiste, że prawo gwarantowane art. 11 KPP odpowiada prawu gwarantowanemu art. 10 EKPC, pomimo że w obu przypadkach dobrem chronionym jest wolność wypowiedzi.

Lakoniczność regulacji zawartej w art. 11 KPP nie wydaje się przypadkowa. Przepis ten potwierdza istnienie wolności wypowiedzi w hierarchii wartości prawnie chronionych i gwarantuje jej ochronę. Nie zawiera jednak żadnych wskazówek dotyczących zakresu udzielenia ochrony oraz dopuszczalności zasad ograniczania tej wolności. Skoro w odniesieniu do innych wolności wypowiedzianych w KPP prawodawca unijny sformułował je w sposób jednobrzmiący z treścią przepisów EPKC⁴⁹, to musi zastanawiać, dlaczego nie uczynił tego w odniesieniu do wolności wypowiedzi. W celu ustalenia wzorca normatywnego wolności wypowiedzi na gruncie KPP należy mieć na uwadze z jednej strony generalne odesłanie do treści art. 10 EKPC, ale także, z drugiej strony, okoliczność, że w KPP przewidziano wprost ochronę takich wartości, które nie zostały wymienione w EKPC. Zważywszy na treść art. 53 KPP⁵⁰ zapewniającego zrównanie poziomu ochrony wolności wypowiedzi, w szczególności z takimi prawami i wolnościami jak równość, niedyskryminacja, równe prawa kobiet i mężczyzn, solidarność, konieczne jest ustalenie standardu normatywnego przy uwzględnieniu ważenia tych praw. W konsekwencji wolność wypowiedzi może doznawać ograniczeń ze względu na potrzebę

⁴⁸ A. Wróbel, *Komentarz...*

⁴⁹ A. Wróbel spostrzega, że takie samo brzmienie mają art. 4 KPP, odpowiadający brzmieniem art. 3 EKPC, art. 5 KPP, odpowiadający brzmieniem art. 4 EKPC czy art. 6 KPP, odpowiadający brzmieniem art. 5 ust. 1 zdanie 1 EKPC; zob. A. Wróbel, *Komentarz...*

⁵⁰ Zgodnie z brzmieniem art. 53 KPP „Żadne z postanowień niniejszej Karty nie będzie interpretowane jako ograniczające lub naruszające prawa człowieka i podstawowe wolności uznane, we właściwych im obszarach zastosowania, przez prawo Unii i prawo międzynarodowe oraz konwencje międzynarodowe, których Unia lub wszystkie Państwa Członkowskie są stronami, w szczególności przez europejską Konwencję o ochronie praw człowieka i podstawowych wolności oraz przez konstytucje Państw Członkowskich”.

ochrony wartości, które uznane zostały w KPP za wymagające równorzędnej ochrony, a które nie zostały objęte konwekcyjną ochroną. Lakoniczność art. 11 KPP daje pole rozszerzającej interpretacji i skłania do dokonywania wykładni celowościowej. Osiągnięcie zakładanego w art. 11 celu (ochrona wolności wypowiedzi) i adekwatnego skutku wymaga jednakże ustalenia granic wolności wypowiedzi, co na gruncie art. 11 KPP może następować na podstawie szerokich ram wykładni dokonywanej przez kompetentny organ sądowniczy. Przy dokonywaniu wykładni konieczne jest odniesienie się przez interpretatora do poziomu ochrony (art. 53) oraz klauzul limitacyjnych (art. 54). W konsekwencji rzeczywistym wykonawcą normy, a zatem także jej adresatem, staje się organ sądowniczy. W nowy standard normatywny wolności wypowiedzi wpisana zostaje rola dla organu orzeczniczego jako podmiotu uprawnionego do wydania wiążącej interpretacji. Słusznie zatem spostrzega się w doktrynie prawa, że możliwość orzekania przez sędziów na podstawie ogólnych i abstrakcyjnych stwierdzeń nieuchronnie prowadzi do przesunięcia władzy na ich korzyść⁵¹, a następnie do rozdzwięku między prawami człowieka a prawem na rzecz sądowej realizacji praw człowieka⁵².

W prawie krajowym gwarancje wolności słowa zostały potwierdzone w art. 54 ust. 1 Konstytucji, stanowiącym, iż „Każdemu zapewnia się wolność wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji”. Wyrażone zostały tam trzy odrębne, acz powiązane i uzależnione od siebie wolności jednostki. Są to: wolność wyrażania swoich poglądów, wolność pozyskiwania informacji oraz wolność rozpowszechniania informacji⁵³. Użyte w jego treści słowo „pogląd”, zgodnie z przyjętym w orzecznictwie Trybunału Konstytucyjnego oraz doktrynie stanowiskiem, powinno być interpretowane jak najszerzej, nie tylko jako wyrażenie osobistych ocen co do faktów, lecz także przypuszczeń oraz opinii⁵⁴. Nie jest przy tym istotna forma wyrażanych poglądów, a więc może to być wypowiedź ustna lub pisemna albo za pomocą

⁵¹ C. Roulhac, *Les droits de l'homme sans la loi?*, „La Revue des droits de l'homme” 2014, nr 5, DOI: <https://doi.org/10.4000/revdh.741>, s. 2.

⁵² Tamże, s. 4.

⁵³ Wyrok TK z dnia 12 maja 2008 r., SK 43/05, OSNP A 2008, nr 4, poz. 57.

⁵⁴ Wyroki TK: z dnia 5 maja 2004 r., P 2/03, OSNP ZU nr 5/A/2004, poz. 39 oraz z 23 marca 2006 r., sygn. K 4/06, OSNP ZU nr 3/A/2006, poz. 32; zob. też. P. Sarnecki, *Uwaga 5 do art. 54, [w:] Konstytucja Rzeczypospolitej Polskiej, Komentarz*, t. 3, L. Garlicki (red.), Warszawa 2003.

obrazu, dźwięku, jak również otwarcie manifestowanej postawy (np. noszenie określonego stroju w określonej sytuacji)⁵⁵. Artykuł 54 ustęp 1 Konstytucji chroni wszelkie zgodne z prawem formy ekspresji, które umożliwiają jednostce uzewnętrznianie i eksponowanie własnego stanowiska.

Ustawodawca konstytucyjny, umieszczając art. 54 ust. 1 Konstytucji w rozdziale II, zaliczył wolność wypowiedzi do wolności i praw osobistych człowieka i obywatela⁵⁶. Wskazuje to, iż celem udzielanej konstytucyjnie ochrony jest możliwość realizacji jednostki w sferze osobistej. Doniosłe znaczenie wolności wypowiedzi w tej sferze, jako jednego z podstawowych praw człowieka przysługujących w naturalny sposób jednostce, dostrzegł Trybunał Konstytucyjny jeszcze przed wejściem w życie obowiązującej Konstytucji⁵⁷. Wolność słowa zapewnia więc w pierwszej kolejności samodzielność podejmowania decyzji oraz autonomię działania, którą stanowi możność swobodnego poszukiwania, otrzymywania, wyrażania oraz rozpowszechniania informacji⁵⁸.

Trybunał Konstytucyjny zwrócił uwagę, że zapewnienie w art. 54 Konstytucji realizacji wolności wypowiedzi na dwóch płaszczyznach, tj. wolności pozyskiwania i wolności rozpowszechniania informacji, nie oznacza automatycznego powiązania obu elementów, albowiem pozyskiwanie informacji nie musi implikować ich rozpowszechniania, które łączy się z partycypacją w przestrzeni społecznej. Tym samym zagwarantowano jednostce wolność wyboru w zakresie „głębokości” (intensywności) partycypacji w życiu społecznym. Korzystanie z wolności zagwarantowanej w art. 54 ust. 1 Konstytucji ma więc w tym znaczeniu ściśle osobisty wymiar⁵⁹.

Znaczenie art. 54 ust. 1 Konstytucji polega zatem na zabezpieczeniu możliwości prawidłowego rozwoju jednostki w demokratycznym państwie prawa. Treść tego przepisu obejmuje wszelkie płaszczyzny aktywności, w których dana osoba postanowiła wyrazić swój pogląd. Wolność słowa nie może być bowiem podporządkowana wyłącznie uczestnictwu w jednym z możliwych

⁵⁵ Wyrok TK z dnia 12 maja 2008 r., SK 43/05, OSNP A 2008, nr 4, poz. 57.

⁵⁶ J. Sobczak, *Prawo Prasowe...*, s. 28.

⁵⁷ Uchwała TK z dnia 2 marca 1994 r., W 3/93, OSNP 1994, cz. I, s. 154–164.

⁵⁸ A. Frankiewicz, *Regulacja wolności wypowiedzi w polskim porządku prawnym*, [w:] *Prawa i wolności obywatelskie w Konstytucji RP*, B. Banaszak, A. Preisner (red.), Warszawa 2002, s. 362 i n.

⁵⁹ Wyrok TK z dnia 12 maja 2008 r., SK 43/05, OSNP A 2008, nr 4, poz. 57.

w społeczeństwie dyskursów (np. politycznym)⁶⁰. Za powyższym przemawia, wynikająca z poszanowania przyrodzonej godności (art. 30 Konstytucji), najszersza ochrona autonomii jednostki, stwarzająca możliwość pełnego rozwoju osobowości w otaczającym ją środowisku kulturowym, cywilizacyjnym⁶¹.

W demokratycznym państwie prawnym szczególną rolę w gwarantowaniu wolności słowa odgrywa wolna i niezależna prasa, co zostało podkreślone w Konstytucji poprzez uznanie wolności prasy za jedną z zasad ogólnych ustroju Rzeczypospolitej Polskiej (art. 14). Władza publiczna powinna więc z jednej strony powstrzymywać się od ingerencji w sferę wolności słowa, z drugiej – tworzyć mechanizmy zapewniające wolność prasy⁶². Na wolność prasy i innych środków społecznego przekazu, zwaną również (zamiennie) wolnością mediów, składają się: wolność zakładania i prowadzenia działalności wydawniczej oraz wolność działalności dziennikarskiej. Treścią wolności mediów są więc przede wszystkim: swoboda zakładania środków społecznego przekazu (tj. swoboda tworzenia odpowiednich prawnie i materialnie struktur nakierowanych na upowszechnianie określonych treści) oraz swoboda wyrażania opinii i pozyskiwania informacji. Konstytucyjne gwarancje realizacji wolności mediów w tym zakresie polegają głównie na ograniczeniu możliwości koncesjonowania działalności radiowej i telewizyjnej (art. 54 ust. 2 zdanie drugie Konstytucji) oraz bezwzględnym zakazie cenzury prewencyjnej środków społecznego przekazu oraz koncesjonowania prasy (art. 54 ust. 2 zdanie pierwsze Konstytucji).

Wolność mediów nie sprowadza się jedynie do wolności upowszechniania własnych poglądów przez dziennikarzy za pomocą mediów, ale umożliwia obieg informacji i krytykę społeczną oraz utrudnia manipulację, w tym także prawem. W tym sensie wolność wyrażania poglądów na łamach prasy i innych środków społecznego przekazu stanowi istotny element zasady zwierzchnictwa narodu (art. 4 ust. 1 Konstytucji), albowiem pozwala obywatelom na świadomy i czynny udział w realizacji władzy państwowej⁶³. Wolność ta ma wymiar

⁶⁰ Tamże.

⁶¹ Wyrok z dnia 4 kwietnia 2001 r., sygn. K. 11/00, OSNP ZU nr 3/2001, poz. 54.

⁶² Wyrok TK z dnia 12 maja 2008 r., SK 43/05, OSNP A 2008, nr 4, poz. 57.

⁶³ W. Skrzydło, *Konstytucja Rzeczypospolitej Polskiej*, Warszawa 2007, s. 22 oraz P. Winczorek, *Komentarz do Konstytucji Rzeczypospolitej Polskiej*, Warszawa 2000, s. 17.

społeczny i jest wolnością pro publico bono, zapewniającą przede wszystkim jawność i pluralizm życia społecznego w demokratycznym państwie prawa⁶⁴.

Znaczenie standardów normatywnych i ich wpływ na realizację praw człowieka może się różnić w zależności od modelu gwarancji praw człowieka osiągniętego w danym kraju i w danym czasie⁶⁵. Tam, gdzie prawa konstytucyjne są wynikiem zasadniczo narodowej ich wizji i kultury, prawa człowieka potwierdzają świadomość ich ponadnarodowego znaczenia oraz dążenia państw do zapewnienia harmonizacji i minimalnej ochrony najbardziej podstawowych gwarancji dla tych wolności, których wysoki stopień podatności na naruszenia jest klasyfikowany jako zagrożenie dla systemu demokratycznego⁶⁶. Zważywszy na kierunek zmian w kształtowaniu normatywnego modelu wolności wypowiedzi, którego symptomem jest lakoniczność regulacji i towarzyszące jej przeniesienie kompetencji do ustalania wiążącej ich interpretacji z normodawcy na władzę sądowniczą oraz inkorporowanie rozwiązań, które poszerzają władzę Trybunałów kosztem władztwa państwa (Protokół nr 15 do EKPC), prowadzi to do marginalizacji znaczenia krajowych standardów wolności wypowiedzi oraz osłabienia roli państw – stron konwencji w definiowaniu normatywnych standardów wolności i praw, w tym wolności wypowiedzi.

Zważywszy na pojawiające się różnice nie tylko w treści regulacji zawierających gwarancje wolności wypowiedzi, ale także ze względu na zróżnicowane podejście do źródeł ochrony tej wolności oraz niejednorodność stanowisk dotyczących samego terminu „prawa człowieka”, nie można zaakceptować poglądu o istnieniu jednolitego normatywnego standardu wolności wypowiedzi. Zawarte w omówionych powyżej aktach prawnych wzorce normatywne zawierają wspólne elementy, w szczególności:

1. założenie o potrzebie ochrony wolności wypowiedzi;
2. potwierdzenie, że wolność wypowiedzi przysługuje każdej jednostce ludzkiej;
3. wolność wypowiedzi obejmuje poglądy i opinie, a także informacje (twierdzenia o faktach);

⁶⁴ J. Szymanek, *Konstytucyjna zasada wolności słowa w radiofonii i telewizji*, „Państwo i Prawo” 2007, nr 8, s. 21.

⁶⁵ C. Roulhac, *Les droits...*

⁶⁶ M. Hottelier, E. McGregor, *La liberté d'expression...*, s. 13.

4. korzystanie z wolności wypowiedzi może następować na wielu płaszczyznach: otrzymywania, posiadania lub przekazywania wypowiedzi;
5. realizacja wolności wypowiedzi powinna następować niezależnie od granic terytorialnych państw.

Odmienne jednak, jak wynika z powyżej przeprowadzonej analizy, mogą kształtować się wzorce dotyczące:

1. aktywności państwa;
2. roli i zadań państwa w ujęciu, tak pozytywnych, jak i negatywnych jego obowiązków;
3. relacji pomiędzy wolnością wypowiedzi a innymi wartościami prawnie chronionymi;
4. harmonizacji standardu i jego obowiązywania;
5. egzekwowalności standardu;
6. definiowania wolności wypowiedzi i jej statusu w katalogu praw człowieka (praw podstawowych).

B. Standard jurydyczny

Zarówno państwa strony europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności, jak i państwa członkowskie UE, podpisując Traktat z Lizbony, do którego załącznik stanowiła KPP⁶⁷, potwierdziły fundamentalne

⁶⁷ Karta praw podstawowych została włączona na podstawie art. 4 Traktatu o Unii Europejskiej – Traktatu o Unii Europejskiej i Traktatu o funkcjonowaniu Unii Europejskiej – do prawa pierwotnego UE, co oznacza, że wobec adresatów zawartych w niej postanowień wywołuje bezpośredni skutek prawny, ingerując w system prawa wewnętrznego związanych nimi państw członkowskich UE. W większości opracowań i analiz autorzy pomijali kwestię obowiązywania, w ścisłym rozumieniu tego terminu, Karty praw podstawowych, skupiając uwagę na zakresie jej stosowania ze względu na treść art. 51–53 KPP, co *de facto* wskazywało na odrzucenie tezy, zgodnie z którą złożony przez Polskę i Wielką Brytanię w 2008 r. Protokół nr 30 w sprawie stosowania Karty praw podstawowych Unii Europejskiej do Polski i Zjednoczonego Królestwa – stanowiący załącznik do Traktatu o Unii Europejskiej i Traktatu o funkcjonowaniu Unii Europejskiej – wyłącza stosowanie Karty w stosunkach pomiędzy Polską a Unią Europejską (skutek opt-out). Tymczasem Protokół polsko-brytyjski zarówno ze względu na jego treść, jak i charakter prawny jako umowy międzynarodowej, a także okoliczności jego złożenia, motywy oraz argument wskazujący na niezmiennność stanowiska Polski, która nigdy z jego postanowień się nie wycofała, nakazuje dokonywanie wykładni art. 51–53 KPP z uwzględnieniem, nie zaś przy

znaczenie wolności wypowiedzi jako wartości, której ochrona jest nieodzowna dla ukonstytuowania i utrzymania demokratycznego systemu sprawowania rządów. Pod kontrolą niezawisłych trybunałów powinna pozostawać zatem aktywność podmiotów publicznych i prywatnych, w tym organów państwowych, organizacji i instytucji, której skutkiem mogłoby być ograniczenie wolności wypowiedzi. Międzynarodowym trybunałom oddano sprawowanie kontroli nad przestrzeganiem przez państwa wolności wypowiedzi. Wyinterpretowane przez TSUE i ETPC na gruncie art. 10 ust. 2 EKPC przesłanki składające się na tzw. trójstopniowy test szkodliwości stanowiły bufor chroniący istotę i jądro wolności wypowiedzi, której źródła upatrywano w prawie przyrodzonym człowieka, w tym w prawie do ochrony jego godności.

Zgodnie z orzecznictwem Europejskiego Trybunału Praw Człowieka art. 10 EKPC gwarantuje każdemu wolność wypowiedzi i informacji i dotyczy nie tylko treści informacji, lecz także środków ich rozpowszechniania, a wszelkie ograniczenia tych środków wpływają na prawo do otrzymywania i przekazywania informacji. Trybunał zauważył, że internet jest obecnie jednym z głównych środków, za pomocą których jednostki korzystają z prawa do wolności wypowiedzi i informacji. Strony internetowe, a zwłaszcza platformy udostępniania treści online, dzięki ich dostępności oraz zdolności do przechowywania i rozpowszechniania dużej ilości danych, przyczyniają się w dużej mierze do zwiększania dostępu społeczeństwa do aktualnych wiadomości i w sposób ogólny do ułatwiania przekazywania informacji, gdyż możliwość wypowiadania się przez jednostki w internecie stanowi bezprecedensowe narzędzie umożliwiające korzystanie z wolności wypowiedzi⁶⁸. Udostępnienie treści, w tym także treści online – niezależnie od tego, czy chodzi o materiały wideo, fotografie, teksty itp. – wchodzi zatem w zakres wykonywania prawa do wolności wypowiedzi i informacji⁶⁹. Takie udostępnienie online

pominięciu, treści Protokołu nr 30. W konsekwencji uprawnione jest także stanowisko, zgodnie z którym KPP nie znajduje zastosowania do Polski.

⁶⁸ Wyroki ETPC: z dnia 1 grudnia 2015 r. w sprawie Cengiz i in. przeciwko Turcji, skargi nr 48226/10 i 14027/11, § 52 (dalej: Wyrok ETPC w sprawie Cengiz przeciwko Turcji); z dnia 23 czerwca 2020 r. w sprawie Vladimir Kharitonov przeciwko Rosji, skarga 10795/14, § 33 (dalej: Wyrok w sprawie Kharitonov przeciwko Rosji) i przytoczone tam orzecznictwo.

⁶⁹ Wyroki ETPC: z dnia 19 lutego 2013 r. w sprawie Neij i Sunde Kolmisoppi przeciwko Szwecji, skarga 40397/12, s. 9–10; z dnia 10 kwietnia 2013 r. w sprawie Ashby

może również dotyczyć innych pokrewnych wolności. W szczególności, jeżeli rozpatrywane treści stanowią wypowiedź artystyczną użytkowników, którzy je zamieszczają, ich udostępnienie online jest objęte zakresem korzystania z wolności sztuki zagwarantowanej w art. 13 Karty oraz w art. 10 EKPC⁷⁰.

Wolność wypowiedzi, jeśli wywodzi się z prawa naturalnego, była kwalifikowana, co stanowiło powszechnie stosowaną praktykę orzecniczą i niekwestionowaną zasadę, do podstawowych praw człowieka, uzyskując często prymat nad innymi prawami i wolnościami prawnie chronionymi. Zmiana normatywnego standardu wolności wypowiedzi otworzyła pole do redefiniowania granic wolności wypowiedzi, a nawet jej zakwestionowania jako wolności przyrodzonej i niezależnej od woli państwa. Nowy, międzynarodowy standard normatywny inspirowany niekiedy, jak dzieje się to w doktrynie prawa francuskiego, do postawienia pytania o:

charakter relacji między wolnością wypowiedzi, która jest tradycyjnie chroniona przez krajowe prawo konstytucyjne, a jej nowszym uznaniem na szczeblu międzynarodowym. Czy jest to ta sama wolność, czy też odrębne, komplementarne lub, w zależności od przypadku, antagonistyczne formy praw jednostki? Czy prawa konstytucyjne o randze państwowej są całkowicie zbieżne z ich kuzynami określonymi w instrumentach ochrony praw człowieka?⁷¹

Zauważono zarazem, że zmiana orzeczniczego wzorca wolności wypowiedzi następuje poprzez zastosowanie przez sędziów europejskich art. 17 EKPC, co prowadzi do uzyskania „efektu tasaka” lub „efektu gilotyny” zgodnie z terminologią użytą przez Jeana-François Flaussa⁷², a w doktrynie prawa

Donald i in. przeciwko Francji, skarga nr 36769/08 – dalej: Wyrok ETPC w sprawie Ashby Donald i in. przeciwko Francji § 34; a także opinia rzecznika generalnego N. Jääskinen w sprawie L'Oréal i in., C-324/09, pkt 49, 157.

⁷⁰ O ile bowiem EKPC nie zawiera takiej wolności jako autonomicznego prawa, o tyle „wolność wypowiedzi artystycznej” jest objęta art. 10 tej konwencji. Zob. w szczególności wyroki ETPC: z dnia 24 maja 1988 r. w sprawie Müller i in. przeciwko Szwajcarii, skarga nr 10737/84, § 27; a także z dnia 8 lipca 1999 r. w sprawie Karatábór przeciwko Turcji, skarga nr 23657/94, § 49.

⁷¹ M. Hottelier, E. McGregor, *La liberté d'expression...*

⁷² J.F. Flauss, *Labus de droit dans le cadre de la CEDH*, „Revue Universelle des Droits de l'Homme” 1992, s. 464. Inni mówią o „mieczu utraty konwencjonalnej ochrony w czystej

polskiego wypowiedzianego przez I.C. Kamińskiego. Artykuł 17 EKPC bywa także trafnie nazywany „klauzulą przypadku”⁷³.

Zgodnie z art. 17 EKPC „Żadne z postanowień niniejszej konwencji nie może być interpretowane jako przyznanie jakiegokolwiek państwu, grupie lub osobie prawa do podjęcia działań lub dokonania aktu zmierzającego do zniweczenia praw i wolności wymienionych w niniejszej konwencji albo ich ograniczenia w większym stopniu, niż to przewiduje konwencja”. Zawarta w tym przepisie dyspozycja skierowana *de facto*, w związku z treścią art. 19 EKPC⁷⁴, do Trybunału, zobowiązuje sędziów do dokonywania oceny skutku, jaki mógłby powstać dla skuteczności ochrony innej niż wolność wypowiedzi wartości konwencyjnych, gdyby na gruncie rozstrzygnięcia konkretnej indywidualnej sprawy Trybunał uznał za dopuszczalne korzystanie z wolności wypowiedzi. ETPC dokonując wstępnej oceny skargi na naruszenie art. 10 Konwencji, ustala zatem, czy treść, forma wypowiedzi i intencje jej autora nie są sprzeczne z wartościami Konwencji. Zasadnicze znaczenie dla ustalenia standardu orzeczniczego ma zatem nie tylko sposób dokonywania przez Trybunał wykładni art. 10 EKPC, ale także, a nawet – jak uważam – przede wszystkim przesłanki, które Trybunał bierze pod uwagę, rozstrzygając o odmowie przyjęcia skargi do rozpoznania. Standard orzeczniczy wyznacza więc nie tylko sposób ustalenia i zastosowania przesłanek ograniczania wolności wypowiedzi na podstawie art. 10 EKPC, ale też kryteria, jakie Trybunał stosuje, w ogóle odmawiając oceny wskazanego w skardze ograniczenia, uznając zachowanie skarżącego za nielegalne, a w konsekwencji niezaskługujące na ochronę. Linia podziału biegnie zatem obecnie pomiędzy wypowiedziami, które ETPC uznaje za nielegalne, a tymi wypowiedziami, do których znajdować

postaci” (S. Van Drooghenbroeck, *Czy artykuł 17 Europejskiej Konwencji Praw Człowieka jest niezbędny?*, „Revue trimestrielle des droits de l’homme” 2001, s. 541–566, zwłaszcza s. 565; cyt. za: M. Levinet, *La clause d’interdiction de l’abus de droit de l’article 17 de la CEDH. Un instrument légitime de l’ordre public européen?*, 20.03.2023, Confluence des droits_La revue, <https://confluencedesdroits-larevue.com/?p=2322>, s. 4 (dostęp: 23.02.2024)).

⁷³ W oryginalnym brzmieniu: „la clause de déchéance”; zob. M. Levinet, *La clause...*, s. 5.

⁷⁴ Trybunał został ustanowiony, by czuwać nad wykonywaniem praw konwencyjnych. Zgodnie z brzmieniem art. 19: „W celu zapewnienia przestrzegania zobowiązań wynikających dla Wysokich Układających się Stron z Konwencji i jej protokołów tworzy się Europejski Trybunał Praw Człowieka, zwany dalej »Trybunałem« Działa on w sposób stały”.

będą zastosowanie wypracowane przez Trybunał na gruncie art. 10 ust. 2 EKPC wzorce oceny, w szczególności trójstopniowy test (test szkodliwości).

Jak podkreśla M. Levinet,

możliwość skorzystania z klauzuli zawartej w art. 17 jest bardzo często przedstawiana jako ilustracja formuły „Brak wolności dla wrogów wolności”, która odnosi się do jednego z przywódców Rewolucji Francuskiej: Saint-Justa. Jeśli jednak wyrażenie to zostało użyte 10 października 1793 r. w jego Raporcie o konieczności ogłoszenia rządu rewolucyjnego do czasu pokoju, nie powinno być odczytywane ahistorycznie, tracąc z oczu kontekst, w którym pojawia się takie stwierdzenie, kiedy zastosowano w stosunku do współrewolucjonistów terror i ustanowiono dyktaturę w celu zapewnienia bezpieczeństwa publicznego⁷⁵.

W istocie sformułowanie to było u niego nierozdzielnie związane z rozróżnieniem – obecnym również u Robespierre’a – między „rządem rewolucyjnym” (który zakłada odwołanie się do terroru) a „rządem konstytucyjnym”⁷⁶. Cytowana formuła nie była zatem odnoszona do rządów demokratycznych, które bronią się przed słowami lub czynami zmierzającymi do jego naruszenia. Formuła ta stanowiła uzasadnienie rewolucji, a zatem przewrotu na płaszczyźnie politycznej, społecznej i kulturowej. Zastosowanie art. 17 EKPC (mechanizm gilotyny) w warunkach pokoju w celu ochrony potencjalnie zagrożonego systemu, nie zaś jego zniesienia (dokonania przewrotu), przy zastosowaniu formuły wypowiedzianej przez Saint-Justa do uzasadniania decyzji odmawiających ochrony niektórym emanacjom wolności wypowiedzi powinno zatem także zostać poddane ocenie pod kątem legalności. Jak zauważa się w doktrynie francuskiej, także te decyzje, które zostały oparte na art. 17 EKPC, mogą być bowiem nielegalne⁷⁷. Wskazano zarazem, że art. 17 „dominuje nad całą Konwencją”⁷⁸, pozwalając oceniać sędziom strasburskim „normalność

⁷⁵ M. Levinet, *La clause...*, s. 4.

⁷⁶ Saint-Just twierdził, że „Niemożliwe jest wprowadzenie w życie praw rewolucyjnych, jeśli sam rząd nie zostanie ukonstytuowany w sposób rewolucyjny; zob. Archiwum Parlamentarne, seria 1, t. 76, s. 313 i 315; B. Manin, *Saint-Just, la logique de la Terreur*, Payot 1979, s. 165–231; cyt. za: M. Levinet, *La clause...*, s. 5.

⁷⁷ M. Levinet, *La clause...*, s. 2.

⁷⁸ Tamże, s. 3.

ograniczeń nałożonych na prawa i wolności, które ta konwencja określa”⁷⁹. Ma to zasadnicze znaczenie, jeśli weźmie się pod uwagę, że Europejski Trybunał Praw Człowieka określa Konwencję jako „konstytucyjny instrument europejskiej polityki publicznej”⁸⁰.

Zastosowanie przez sędziów Trybunału klauzuli przepadku jest pozbawione kontroli ze strony innych organów, a nadto nie jest konsekwentne, na co zwracają uwagę także sami sędziowie ETPC⁸¹. Typologię spraw, w których poczesne miejsce zajmują skargi na naruszenie wolności wypowiedzi, ale zostały one przez Trybunał odrzucone z powołaniem na art. 17 jako sprzeczne z konwencyjnymi wartościami, zawiera opracowywany systematycznie przez sekretariat Trybunału *Przewodnik po artykule 17*⁸². Wskazuje się w nim, że Trybunał nie przyjmował do rozpoznania spraw jako sprzecznych z Konwencją, wskazując jako przyczyny sprzeczność realizowanego przez skarżącego celu z wartościami konwencji, tj. ze względu na⁸³:

1. mowę nienawiści⁸⁴,
2. przemoc⁸⁵,

⁷⁹ W oryginalnym brzmieniu: „*permettant de juger de la normalité des limitations apportées aux droits et libertés qu'elle énonce*”.

⁸⁰ Wyrok ETPC z dnia 18 grudnia 1996 r. w sprawie Loizidou przeciwko Turcji, skarga nr 15318/89, § 75, w brzmieniu oryginalnym: „*a Convention en tant qu'instrument constitutionnel de l'ordre public européen*”.

⁸¹ A. Spielmann, wyrażając ubolewanie z powodu „podejścia opartego na orzecnictwie opartego na zmiennej geometrii praw”; zob. A. Spielmann, *Europejski Trybunał Praw Człowieka i Podstawowych Wolności*, [w]: tenże, *Au diapason des droits de l'homme: écrits choisis (1975–2003)*, Bruksela 2006, s. 390.

⁸² *Guide sur l'article 17 de la Convention européenne des droits de l'homme. Interdiction de l'abus de droit*, 29.02.2024, https://ks.echr.coe.int/documents/d/echr-ks/guide_art_17_fre (dostęp: 23.05.2024).

⁸³ Typologia wskazana w: tamże, s. 11.

⁸⁴ Wyroki ETPC: z dnia 15 października 2015 r. w sprawie Perinçek przeciwko Szwajcarii, skarga nr 27510/08, §§ 115–230 (dalej: Wyrok ETPC w sprawie Perinçek przeciwko Szwajcarii); z dnia 23 października 2012 r. w sprawie Molnar przeciwko Rumunii, skarga nr 16637/06; decyzja z dnia 27 czerwca 2017 r. w sprawie Belkacem przeciwko Belgii, skarga nr 34367/14 (dalej: Decyzja ETPC w sprawie Belkacem przeciwko Belgii); z dnia 12 maja 2020 r. w sprawie Lilliendahl przeciwko Islandii, skarga nr 29297/18, § 39; z dnia 27 czerwca 2023 r. w sprawie Lenis przeciwko Grecji, skarga nr 47833/20, § 56.

⁸⁵ Decyzja ETPC z dnia 12 czerwca 2012 r. w sprawie Hizb Ut-Tahrir i in. przeciwko Niemcom, skarga nr 31098/08; wyrok z dnia 14 marca 2013 r. w sprawie Kasymakhunov i Saybatalov przeciwko Rosji, skargi nr 26261/05 i 26377/06 (dalej: Wyrok ETPC w sprawie Kasymakhunov i Saybatalov przeciwko Rosji); wyrok ETPC w sprawie Belkacem przeciwko Belgii.

3. ksenofobię i dyskryminację rasową⁸⁶,
4. antysemityzm⁸⁷,
5. islamofobię⁸⁸,
6. terroryzm i przestępstwa wojenne⁸⁹,
7. negację holokaustu⁹⁰,
8. niechęć do ofiar holokaustu, reżimów wojennych i totalitaryzmu⁹¹,
9. pochwalanie ideologii totalitarnych i idei niezgodnych z Konwencją⁹².

⁸⁶ Wyroki ETPC: z dnia 23 września 1994 r. w sprawie Jersild przeciwko Danii, skarga nr 15890/89 (dalej: Wyrok ETPC w sprawie Jersild przeciwko Danii); z dnia 16 lipca 2009 r. w sprawie Feret przeciwko Belgii, skarga nr 15615/07; z dnia 8 października 2020 r. w sprawie Ayoub przeciwko Francji, skarga nr 77400/14.

⁸⁷ Decyzje ETPC: z dnia 27 sierpnia 2004 r. w sprawie Pavel Ivanov przeciwko Rosji, skarga nr 35222/04; z dnia 2 września 2004 r. w sprawie W.P. i inni przeciwko Polsce, skarga nr 42264/98 (dalej: Decyzja ETPC w sprawie W.P. przeciwko Polsce).

⁸⁸ Decyzje ETPC: z dnia 16 listopada 2004 r. w sprawie Norwood przeciwko Wielkiej Brytanii, skarga nr 23131/03 (dalej: Wyrok ETPC w sprawie Norwood przeciwko Wielkiej Brytanii); z dnia 18 maja 2004 r. w sprawie Seurot przeciwko Francji, skarga nr 57383/00 (dalej: Wyrok ETPC w sprawie Seurot przeciwko Francji); z dnia 10 lipca 2008 r. w sprawie Soulas i in. przeciwko Francji, skarga nr 15948/03 (dalej: Wyrok ETPC w sprawie Soulas przeciwko Francji); z dnia 20 grudnia 2022 r. w sprawie Zemmour przeciwko Francji, skarga nr 63539/19 (dalej: Wyrok ETPC w sprawie Zemmour przeciwko Francji).

⁸⁹ Wyroki ETPC: z dnia 15 stycznia 2009 r. w sprawie Orban i in. przeciwko Francji, skarga nr 20985/05, § 35; z dnia 2 października 2008 r. w sprawie Leroy przeciwko Francji, skarga nr 36109/03, § 27; z dnia 17 kwietnia 2018 r. w sprawie Roj TV A/S przeciwko Danii, skarga nr 24683/14, § 46–47.

⁹⁰ Wyroki ETPC: z dnia 23.09.1998 r. w sprawie Lehideux i in. przeciwko Francji, nr skargi 55/1997/839/1045, § 47 (dalej: Wyrok ETPC w sprawie Lehideux przeciwko Francji); z dnia 20 października 2015 r. w sprawie M'Bala M'Bala przeciwko Francji, skarga nr 25239/13 (dalej: Wyrok ETPC w sprawie M'Bala M'Bala przeciwko Francji); z dnia 24 czerwca 2003 r. w sprawie Garaudy przeciwko Francji, skarga nr 65831/01 (dalej: Wyrok ETPC w sprawie Garaudy przeciwko Francji); z dnia 13 grudnia 2005 r. w sprawie Witzsch przeciwko Niemcom, skarga nr 7485/03 (dalej: Wyrok ETPC w sprawie Witzsch przeciwko Niemcom).

⁹¹ Wyroki ETPC: z dnia 22 kwietnia 2010 r. w sprawie Fatullayev przeciwko Azerbejdżanowi, skarga nr 40984/07, § 81; z dnia 8 lipca 2008 r. w sprawie Vajnai przeciwko Węgrom, skarga nr 33629/06, § 25 (dalej: Wyrok ETPC w sprawie Vajnai przeciwko Węgrom); z dnia 24 lipca 2012 r. w sprawie Fáber przeciwko Węgrom, skarga nr 40721/08, § 58; z dnia 3 października 2019 r. w sprawie Pastör przeciwko Niemcom, skarga nr 55225/14, § 39.

⁹² Wyroki ETPC: w sprawie Lehideux przeciwko Francji, § 53; z dnia 9 lipca 2013 r. w sprawie Vona przeciwko Węgrom, skarga nr 35943/10, § 36; w sprawie Vajnai przeciwko Węgrom, § 25; w sprawie Kasymakhunov i Saybatalov przeciwko Rosji, §§ 108–113; z dnia 13 lutego 2003 r. w sprawie Refah Partisi (Partide la prospérité) i in. przeciwko Turcji, skargi nr 41340/98, 41342/98, 41343/98 i 41344/98, § 132; z dnia 1 lutego 2000 r. w sprawie

Jako wartości, które były nie do pogodzenia z celami działania skarżących i wymagały ochrony polegającej na zastosowaniu względem skarżących „klausuli przepadku”, ETPC wskazał:

1. pokój i sprawiedliwość,
2. prawdziwie demokratyczny ustrój i wolne wybory,
3. ochronę życia i pokojowego rozwiązywania konfliktów zbrojnych,
4. tolerancję, pokój społeczny i niedyskryminację,
5. równość kobiet i mężczyzn,
6. współegzystencję w społeczeństwie pozbawionym segregacji rasowej⁹³.

Korzystanie z wolności wypowiedzi w celu rozpowszechniania wiadomości podlegającej do nienawiści, przemocy, rasizmu, ksenofobii, antysemityzmu lub cechującej się islamofobią stanowi nadużycie, które nie może, w ocenie Trybunału, korzystać z ochrony systemu gwarancji prawa europejskiego. *Prima facie* zauważalne jest jednak, że wartości, w imię ochrony których Trybunał odmawiał przyjęcia skargi do rozpoznania jako sprzecznej z Konwencją, nie zostały w niej wprost wymienione. Nie oznacza to, że nie pozostają one pod ochroną Konwencji, jednakże ustalenie i nazwanie wartości jako zasługujących na konwencyjną ochronę nie jest dziełem normodawcy, tj. umawiających się stron – sygnatariuszy Konwencji, lecz pochodną stosowania Konwencji przez sędziów Trybunału.

Trybunał dokonując rozstrzygnięć, nie wdaje się w klasyczne pytanie o realność istnienia zarzucanej nadmiernej ingerencji w chronione w Konwencji wartości. Nie ocenia stopnia ich przewidywalności ani nie podejmuje próby legitymizacji celu. Uchyła się także od podjęcia zwykłej kontroli proporcjonalności ingerencji, która zakłada uzasadnione wyważenie między imperatywami obrony społeczeństwa demokratycznego a imperatywami ochrony praw jednostki. M. Levinet zauważa, że w tych przypadkach urząd sędziego europejskiego „zatrzymuje się na prostym etapie oceny dopuszczalności skargi poprzez ograniczenie się do sprawdzenia, czy kwestionowane stwierdzenie lub zachowanie ma na celu zniweczenie praw i wolności

Schimanek przeciwko Austrii, skarga 32307/96; z 1988 r. w sprawie Kühnen przeciwko Niemcom, [http://hudoc.echr.coe.int/fre#{%22itemid%22:\[%22001-81746%22\]}](http://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-81746%22]}) (dostęp: 23.05.2024); z dnia 17 sierpnia 1956 r. w sprawie Parti communiste (KPD) przeciwko Niemcom, skarga nr 250/57.

⁹³ *Guide sur l'article 17...*, s. 9–10.

chronionych przez EKPC. Trybunał ogranicza się zatem do ustalenia intencji skarżącego. Skutkuje to brutalnym stwierdzeniem niedopuszczalności korzystania z ochrony i natychmiastowego i ostatecznego ukarania nadużycia prawa – a nie w drodze wyroku rozstrzygającego w sprawie zasadności żądania skarżących”⁹⁴.

Dopiero przyjęcie skargi do rozpoznania przez Trybunał, co *de facto* oznacza, że sędziowie w drodze wstępnej kontroli ocenili jako dopuszczalny (legalny) sposób korzystania przez skarżącego z wolności wypowiedzi, umożliwia zastosowanie wynikających z art. 10 EKPC zasad ochrony wypowiedzi (nazywam dalej: klasycznym standardem).

Trzon standardu orzeczniczego ustanowionego przez ETPC na gruncie art. 10 EKPC stanowią ustalenia zawarte w wyroku z 7.12.1976 r. (wydanym w składzie plenarnym) w sprawie Handyside przeciwko Wielkiej Brytanii, kiedy to ETPC sformułował doniosły i wielokrotnie powtarzany w jego judykatach pogląd, że swoboda wypowiedzi stanowi jeden z zasadniczych filarów społeczeństwa demokratycznego, jeden z podstawowych warunków jego postępu i rozwoju każdej osoby. Swoboda wypowiedzi nie ma się przy tym – zdaniem ETPC – ograniczać do informacji i poglądów, które są odbierane przychylnie, uważane za nieobraźliwe lub neutralne, lecz odnosi się także do tych, które obrażają, oburzają lub wprowadzają niepokój w państwie lub części społeczeństwa. Takie są wymagania pluralizmu, tolerancji, otwartości na inne poglądy, bez których nie istnieje demokratyczne społeczeństwo⁹⁵. Stanowisko, że wolność słowa jest fundamentem społeczeństwa demokratycznego, znalazło potwierdzenie i ugruntowanie w późniejszej, rozwijającej tę linię orzeczniczą, działalności ETPC⁹⁶. Pojęcie społeczeństwa demokratycznego okazało się przy tym nie tylko pojęciem konstytuującym znaczenie prawa do swobody wypowiedzi, ale także określającym jego granice.

Wolność wypowiedzi – jako prawo materialne, a przy tym tylko jedno z praw zawartych w katalogu europejskiej Konwencji o ochronie praw człowieka

⁹⁴ M. Levinet, *La clause...*

⁹⁵ Wyrok ETPC w sprawie Handyside przeciwko Wielkiej Brytanii; por. I.C. Kamiński, *Swoboda wypowiedzi w orzeczeniach Europejskiego Trybunału Praw Człowieka w Strasburgu*, Kraków 2003, s. 27–41.

⁹⁶ Wyrok ETPC: w sprawie Lingens przeciwko Austrii; Castells przeciwko Hiszpanii czy Oberschlick przeciwko Austrii (nr 2).

i podstawowych wolności – może, co zostało dostrzeżone już w samym brzmieniu art. 10 ust. 2 EKPC, wchodzić w konflikt z innymi wartościami prawnie chronionymi, np. z prawem do poszanowania życia prywatnego, i z tego względu nie może być uznana za prawo absolutne. Jak zauważono w doktrynie „jest jednak ewidentne, że ETPC przyznaje znacznie szerszą swobodę korzystania z wolności słowa, gdy służy debacie publicznej uważanej za niezbędną w demokratycznym społeczeństwie”⁹⁷.

Zgodnie ze standardem orzecznictwem wypracowanym przez ETPC, swoboda wypowiedzi z art. 10 ust. 1 EKPC obejmuje nie tylko treść wypowiedzi, lecz także jej formę⁹⁸, a także sam środek przekazu⁹⁹.

Niemniej, co zgodnie potwierdzają także sądy krajowe, swoboda wypowiedzi nie ma charakteru absolutnego¹⁰⁰. Korzystanie z niej pociąga za sobą, także po stronie podmiotu tej wolności, pewne obowiązki i odpowiedzialność¹⁰¹. Dlatego swoboda ta może doznawać różnego rodzaju ograniczeń, aczkolwiek należy wyraźnie zaznaczyć, iż zgodnie z utrwalonym orzecznictwem ETPC wyjątki od art. 10 EKPC muszą być jednak konstruowane restrykcyjnie, a potrzeba ograniczenia swobody wypowiedzi przekonywająco uzasadniona¹⁰². Zgodność ograniczeń swobody wypowiedzi ze standardem konwencyjnym

⁹⁷ W. Waclawczyk, *Swoboda wypowiedzi jako fundamentalna zasada społeczeństwa demokratycznego. Kilka uwag o standardach Rady Europy i orzecznictwie Europejskiego Trybunału Praw Człowieka*, „Orzecznictwo Sądów Apelacyjnych” 2005, nr 12, s. 96.

⁹⁸ Wyroki ETPC: z dnia 23 maja 1991 r. w sprawie Oberschlick przeciwko Austrii (nr 1), skarga nr 11662/85, § 57 (dalej: Wyrok ETPC w sprawie Oberschlick przeciwko Austrii (nr 1)); w sprawie Oberschlick przeciwko Austrii (nr 2), § 34.

⁹⁹ Wyroki ETPC: z dnia 10 lipca 2003 r. w sprawie Murphy przeciwko Irlandii, skarga nr 44179/98, § 61 (dalej: Wyrok ETPC w sprawie Murphy przeciwko Irlandii); z dnia 28 czerwca 2001 r. w sprawie VgT Verein Gegen Tierfabriken przeciwko Szwajcarii, skarga nr 24699/94, § 66 (dalej: Wyrok ETPC w sprawie VgT Verein Gegen Tierfabriken przeciwko Szwajcarii); z dnia 8 listopada 2012 r. w sprawie Peta Deutschland przeciwko Niemcom, skarga nr 43481/09, § 47 (dalej: Wyrok ETPC w sprawie Peta Deutschland przeciwko Niemcom).

¹⁰⁰ Wyrok SN z dnia 14 stycznia 2010 r., III SK 15/09, LEX 578182.

¹⁰¹ Wyrok ETPC w sprawie Murphy przeciwko Irlandii, § 65.

¹⁰² Wyroki ETPC z dnia 28 grudnia 2000 r. w sprawie Lopes Gomes a Silva przeciwko Portugalii, skarga nr 37698/97, pkt 35; w sprawie VgT Verein Gegen Tierfabriken przeciwko Szwajcarii, § 66.

podlega zindywidualizowanej ocenie dokonywanej przez ETPC. W ramach tej oceny uwzględnia się okoliczności faktyczne konkretnej sprawy¹⁰³.

Sformułowany w orzecznictwie ETPC ogólny test oceny zgodności ograniczenia swobody wypowiedzi z art. 10 EKPC składa się z trzech podstawowych przesłanek. Po pierwsze, ograniczenie swobody wypowiedzi musi być przewidziane przez prawo (kryterium legalności). Po drugie, ograniczenie tego prawa podstawowego musi służyć ochronie jednej z wartości wymienionych w art. 10 ust. 2 EKPC (kryterium celowości). Po trzecie, zastosowane w konkretnej sprawie ograniczenie musi być konieczne w demokratycznym społeczeństwie (kryterium niezbędności).

Kryterium legalności jest spełnione, gdy ograniczenie swobody wypowiedzi ma oparcie w przepisach prawa krajowego oraz przepisy te są sformułowane w taki sposób, że jednostka samodzielnie lub po konsultacji z prawnikiem może racjonalnie przewidzieć konsekwencje prawne swojego zachowania¹⁰⁴. Nie jest przy tym konieczne, by konsekwencje te były „absolutnie pewne”¹⁰⁵, ponieważ od prawodawcy krajowego nie można oczekiwać stanowienia wyłącznie kazuistycznie sformułowanych przepisów. Dozwolone jest zatem posługiwanie się pojęciami nieostryimi, których ostateczna treść zostanie sprecyzowana dopiero w praktyce stosowania¹⁰⁶ przez organy administracji lub sądy krajowe. Przykładowo za „przewidziane prawem” ograniczenie swobody wypowiedzi uznano ustawowy zakaz reklamy politycznej i jego zastosowanie do reklamy stowarzyszenia zajmującego się ochroną zwierząt, która to reklama zachęcała do ograniczenia spożycia mięsa¹⁰⁷. Podobne stanowisko w odniesieniu do kryterium legalności zajmuje na gruncie KPP

¹⁰³ Wyroki ETPC: w sprawie Oberschlick przeciwko Austrii (nr 1), § 60; w sprawie Oberschlick przeciwko Austrii (nr 2), pkt 31; w sprawie Murphy przeciwko Irlandii, § 62–69; w sprawie VgT Verein Gegen Tierfabriken przeciwko Szwajcarii, § 68.

¹⁰⁴ Wyroki ETPC: w sprawie VgT Verein Gegen Tierfabriken przeciwko Szwajcarii, § 52 i 55; z dnia 21 lipca 2011 r. w sprawie Sigma Radio Television Ltd. przeciwko Cyprowi, skargi 32181/04 i 35122/05, § 194 (dalej: Wyrok ETPC w sprawie Sigma Radio Television Ltd. przeciwko Cyprowi).

¹⁰⁵ Wyrok ETPC w sprawie VgT Verein Gegen Tierfabriken przeciwko Szwajcarii, § 55.

¹⁰⁶ Wyrok ETPC w sprawie VgT Verein Gegen Tierfabriken przeciwko Szwajcarii, § 55; w sprawie Sigma Radio Television Ltd. przeciwko Cyprowi, § 194.

¹⁰⁷ Wyrok ETPC w sprawie VgT Verein Gegen Tierfabriken przeciwko Szwajcarii, § 57–58.

Trybunał Sprawiedliwości UE. Trybunał stwierdził, że wszelkie ograniczenia korzystania z praw podstawowych muszą być przewidziane ustawą. Zwraca zarazem uwagę, że akt, który pozwala na ingerencję w te prawa, musi sam określać zakres ograniczenia wykonywania danego prawa¹⁰⁸.

Kryterium celowości odnosi się z kolei do powodów ograniczenia swobody wypowiedzi. Wartościami najczęściej uwzględnianymi jako uzasadniające ingerencję w swobodę wypowiedzi jest ochrona praw innych osób oraz moralności publicznej¹⁰⁹.

Przy ocenie, czy istniała potrzeba ingerencji oraz w razie jej stwierdzenia decyzja, jakie środki należało podjąć, aby jej zaradzić, organom krajowym pozostawia się pewien margines uznania. To uprawnienie do samodzielnej oceny w ramach marginesu swobody państwa nie jest jednak nieograniczone, lecz idzie w parze z europejską kontrolą Trybunału, którego zadaniem jest ostateczne rozstrzygnięcie, czy ograniczenie jest zgodne z wolnością wypowiedzi chronioną przez art. 10. Zadaniem Trybunału, który wykonuje swoją funkcję kontrolną, nie jest zastępowanie organów krajowych, lecz kontrola na podstawie art. 10, w świetle całej sprawy, decyzji, które podjęły one w ramach przysługujących im uprawnień kontrolnych¹¹⁰.

Trybunał, który wraz z Komisją, jak zauważa I.C. Kamiński, jest odpowiedzialny za zapewnienie przestrzegania zobowiązań państw – stron konwencji (art. 19), jest uprawniony do oceny, czy działanie państwa mieściło się w granicach przyznanego mu na gruncie art. 10 ust. 2 marginesu swobody i wydania ostatecznego orzeczenia w sprawie tego, czy „ograniczenie” zastosowane na podstawie prawa krajowego obowiązującego w państwie członkowskim było zgodne z wolnością wypowiedzi chronioną przez art. 10¹¹¹. Krajowy margines uznania idzie zatem w parze z europejskim nadzorem. Nadzór ten dotyczy zarówno celu kwestionowanego środka, jak i jego „konieczności”. Obejmuje ona nie tylko podstawowe akty prawne, lecz także orzeczenie o ich

¹⁰⁸ Wyrok z dnia 16 lipca 2020 r. w sprawie Facebook Ireland i Schrems, C-311/18, EU:C:2020:559, pkt 175 i przytoczone tam orzecznictwo.

¹⁰⁹ Wyroki ETPC: w sprawie Sigma Radio Television Ltd. przeciwko Cyprowi, § 196; w sprawie Peta Deutschland przeciwko Niemcom, § 44.

¹¹⁰ Wyrok ETPC z dnia 21 stycznia 1999 r. w sprawie Fressoz i Roire przeciwko Francji, skarga nr 29183/95, § 45 (dalej: Wyrok ETPC w sprawie Fressoz i Roire przeciwko Francji).

¹¹¹ I.C. Kamiński, *Ograniczenia swobody wypowiedzi...*, Warszawa 2010, s. 206.

stosowaniu, nawet wydane przez niezawisły sąd. W tym zakresie Trybunał powołuje się na art. 50 Konwencji, jak również na własne orzecznictwo¹¹².

Kryterium konieczności wymaga zaś stwierdzenia, czy ingerencja w swobodę wypowiedzi uzasadniona była istnieniem pilnej potrzeby społecznej, czy interwencja była proporcjonalna do realizacji zgodnego z prawem celu oraz czy wskazane przez organy administracji lub sądy powody tej interwencji są właściwe i wystarczające¹¹³. Zasada proporcjonalności wymaga, by ograniczenia, które mogą być nałożone zwłaszcza przez akty prawa Unii na prawa i wolności ustanowione w Karcie, nie wykraczały poza granice tego, co jest odpowiednie i konieczne do realizacji uzasadnionych celów lub poza potrzeby ochrony praw i wolności innych osób, przy czym tam, gdzie istnieje możliwość wyboru spośród większej liczby odpowiednich rozwiązań, należy stosować rozwiązania najmniej dotkliwe, a wynikające z tego niedogodności nie mogą być nadmierne w stosunku do zamierzonych celów¹¹⁴. W przypadku, gdy sprawa dotyczy różnych praw podstawowych i zasad ustanowionych w traktatach, ocena poszanowania zasady proporcjonalności powinna być dokonywana z należytym uwzględnieniem koniecznego pogodzenia wymogów dotyczących ochrony poszczególnych praw i zasad, o których mowa, oraz odpowiedniej równowagi między tymi prawami i zasadami¹¹⁵. Ponadto, aby spełnić wymóg proporcjonalności, uregulowanie prowadzące do ingerencji w prawa podstawowe powinno zawierać jasne i precyzyjne reguły dotyczące zakresu i stosowania rozpatrywanego środka oraz ustanawiać minimalne wymagania służące temu, aby osoby, których korzystanie z tych praw jest ograniczone, były zaopatrzone w wystarczające zabezpieczenia umożliwiające ich rzeczywistą ochronę przed ryzykiem nadużyć. Uregulowanie to powinno w szczególności wskazywać, w jakich okolicznościach i pod jakimi warunkami

¹¹² Wyrok ETPC z dnia 8 czerwca 1976 r. w sprawie Engel i in. przeciwko Holandii, Seria A, nr 22, s. 41–42, pkt 100.

¹¹³ Wyroki ETPC: w sprawie Sigma Radio Television Ltd. przeciwko Cyprowi, § 199; Peta Deutschland przeciwko Niemcom, § 45.

¹¹⁴ Wyrok z dnia 13 marca 2019 r. w sprawie Polska/Parlament i Rada, C-128/17, EU:C:2019:194, pkt 94 i przytoczone tam orzecznictwo; wyrok z dnia 17 grudnia 2020 r. w sprawie Centraal Israëlitisch Consistorie van België i in., C-336/19, EU:C:2020:1031, pkt 64 i przytoczone tam orzecznictwo.

¹¹⁵ Wyrok z dnia 17 grudnia 2020 r. w sprawie Centraal Israëlitisch Consistorie van België i in., C-336/19, EU:C:2020:1031, pkt 65 i przytoczone tam orzecznictwo.

taki środek może zostać przyjęty, gwarantując w ten sposób, że ingerencja będzie ograniczona do tego, co ściśle konieczne. Konieczność zapewnienia takich gwarancji ma tym większe znaczenie, gdy ingerencja jest wynikiem zautomatyzowanego procesu¹¹⁶.

Sąd Najwyższy zauważył, że chociaż w piśmiennictwie konstytucyjnym wskazuje się na węższy zakres wolności wypowiedzi z art. 54 Konstytucji RP w porównaniu ze swobodą wypowiedzi z art. 10 EKPC, to standardy krajowy i międzynarodowy w zakresie tego prawa podstawowego są zbliżone, czego dowodzą m.in. liczne odwołania Trybunału Konstytucyjnego do wyroków ETPC, czy posiłkowanie się przez komentatorów Konstytucji RP orzecznictwem strasburskim¹¹⁷. Przepis art. 54 ust. 1 Konstytucji dotyczy wolności wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji jako prawa jednostki¹¹⁸. Mimo szerokiej konstytucyjnej ochrony wolności wypowiedzi, wzmocnionej dodatkowo przez art. 14 Konstytucji RP, ustawa zasadnicza pozwala na wprowadzenie ograniczeń w korzystaniu z tej wolności. W przekonaniu Sądu Najwyższego i polskiego sądu konstytucyjnego dopuszczalne jest, co do zasady, ograniczenie wolności wypowiedzi, nawet gdyby, w skrajnych wypadkach, miało przybrać postać sankcji karnej¹¹⁹, jak również kary finansowej¹²⁰, o ile w okolicznościach konkretnej sprawy zastosowanie przepisów przewidujących taką sankcję będzie znajdowało oparcie w przesłankach art. 31 ust. 3 Konstytucji RP¹²¹.

O ile na płaszczyźnie prawa krajowego klauzulę limitacyjną, w oparciu na której sądy krajowe, w tym sąd konstytucyjny, ustalają granice wolności wypowiedzi, stanowi art. 31 ust. 3 Konstytucji, a ocena dokonywana na podstawie zawartych w tym przepisie przesłanek ma charakter bezwarunkowy i nie jest uzależniona od wstępnego, przedsądowego ustalania dopuszczalności powoływania się przez jednostkę na zagwarantowaną w Konstytucji „każdemu” wolność wypowiedzi, o tyle na gruncie EKPC i KPP (wobec treści art. 52

¹¹⁶ Wyrok z dnia 16 lipca 2020 r. w sprawie Facebook Ireland i Schrems, C-311/18, EU:C:2020:559, pkt 176 i przytoczone tam orzecznictwo.

¹¹⁷ Wyrok SN z dnia 2 lipca 2013 r., III SK 42/12, OSNP 2014, nr 11, poz. 163.

¹¹⁸ Wyroki TK: z dnia 20 lutego 2007 r., P 1/06, OSNP A z 2007 r., nr 2, poz. 11; z dnia 9 listopada 2010 r., K 13/07, OSNP A z 2010 r., nr 9, poz. 98.

¹¹⁹ Wyrok TK z dnia 30 października 2006 r., P 10/06, OSNP A 2006, nr 9, poz. 128.

¹²⁰ Wyrok SN z dnia 2 lipca 2013 r., III SK 42/12, OSNP 2014, nr 11, poz. 163.

¹²¹ Wyrok SN z dnia 2 lipca 2013 r., III SK 42/12, OSNP 2014, nr 11, poz. 163.

ust. 3 KK), swoboda wypowiedzi przybrała postać wolności o charakterze warunkowym. Jeśli zatem polski sąd konstytucyjny i sądy powszechne wskazują na podobieństwo standardu europejskiego do standardów krajowych¹²², to jednak, zważywszy na znaczenie, jakie ETPC przywiązuje do zawartej w art. 17 EKPC klauzuli przypadku, co w rezultacie prowadzi do pozbawienia jednostek w ogóle możliwości powołania się na ochronę wolności wypowiedzi ze względu na uznanie przez ETPC danego zachowania komunikacyjnego za nielegalne, trzeba stwierdzić, że krajowy standard orzeczniczy gwarantuje bardziej intensywną, dalej idącą i pewniejszą ochronę wolności wypowiedzi niż ma to miejsce na gruncie prawa europejskiego.

C. Standard etyczny (zawodowy, korporacyjny)

Użycie terminu „standard etyczny” wskazuje, że założono, iż możliwe jest ustalenie pozaprawnych, opartych na dobrym obyczaju, tradycji i odnoszących się do wspólnie uznawanych wartości i akceptowanym wzorcu moralności, zasad korzystania z wolności wypowiedzi.

W nauce ścierają się dwa podejścia w odniesieniu do celowości i skuteczności stosowania kodeksów etyki i rozwiązań opartych na samoregulacji. Jedno, którego zwolennicy uważają, że kodeksy etyki oraz inicjatywy podejmowane na zasadzie samoregulacji są nieskuteczne, nieefektywne i z góry skazane na niepowodzenie¹²³ oraz drugie, którego przedstawiciele przykładają dużą wagę do rozwiązań pozaprawnych polegających na dobrowolnym samowiązaniu się osób korzystających z wolności wypowiedzi do przestrzegania zasad i reguł ograniczających dowolność form komunikowania i przyjęcie rygorystycznych zasad regulujących korzystanie z wolności wypowiedzi oraz ponoszenie odpowiedzialności za naruszenia spowodowane nadużyciem

¹²² Wyrok TK z dnia 12 maja 2008 r., SK 43/05, OSNP A 2008, nr 4, poz. 57.

¹²³ M. Drózdź zauważa, że „wielu współczesnych twórców koncepcji medialnych nie uważa sfery etycznej za ważną, nie uwzględniając jej jako podstawy kształtowania się i samoregulacji całości działań medialnych człowieka lub eliminując ją na margines refleksji medialnej jako sferę włączoną wprawdzie integralnie w teoretyczny zamysł nad mediami, ale niemającą zasadniczo większego znaczenia tak dla samej teorii medialnej, jak i dla jej praktycznego zastosowania”; zob. M. Drózdź, *Etyka mediów. W obronie wartości*, Kraków 2019, s. 22.

wolności wypowiedzi. Zwolennicy drugiego stanowiska dowodzą, że prawo miękkie, ze względu na jego funkcję polegającą na oddziaływaniu na sposób interpretacji skomplikowanych przepisów prawa:

jest powoływane przez wiele wyznaczonych podmiotów lub organów i często odgrywa rolę praktycznie nie do odróżnienia od twardego prawa, takiego jak ustawodawstwo i orzecznictwo. Dzieje się tak nie tylko w środowisku internetowym, jednak w odniesieniu do internetu stanowisko to jest szczególnie częste¹²⁴.

Zbiory postulatów i reguł pozaprawnych, których wdrożenia, stosowania i przestrzegania oczekuje się od podmiotów korzystających z wolności wypowiedzi, w szczególności w mediach, w tym na platformach internetowych, nie są jednolicie nazywane. O ile skodyfikowane wzory oczekiwanego zachowania odnoszone do osób profesjonalnie zajmujących się rozpowszechnianiem informacji, przede wszystkim dziennikarzy, nazywane były – co do zasady – kodeksami etyki, o tyle w odniesieniu do innych środowisk adresowane do nich skodyfikowane, pozaprawne reguły postępowania są nazywane kodeksami postępowania, co może wskazywać, że ich twórcy, inaczej niż adresaci kodeksów etycznych, w większym stopniu przywiązują wagę do samego aktu uzgodnienia tych warunków (umowy) niż do wartości, które miałyby być źródłem tych uzgodnień i przedmiotem ochrony.

Pomimo dążenia różnorodnych środowisk, a również organów europejskich, do wzmocnienia mechanizmów samoregulacji i dobrowolnie przyjmowanych – także w środowisku cyfrowym – praktyk, ostatecznie prawodawca europejski uznał te rozwiązania za niewystarczające rozwiązania miękkie i skorzystał z narzędzi prawnych, posługując się najbardziej ingerującym w prawa i wolności oraz suwerenność państw instrumentem prawnym, jakim jest rozporządzenie, a nadto, przesądzając w nim o pełnej harmonizacji prawa w zakresie kształtowania wzorca wolności wypowiedzi, w szczególności na rynku cyfrowym.

¹²⁴ D. Jerker, B. Svantesson, *Global status report 2019*, 3.06.2019 r., Internet & Jurisdiction Policy Network, s. 51, <https://www.internetjurisdiction.net/work/data-jurisdiction> (dostęp: 23.05.2024).

Rozwijane są zarazem dwa kierunki regulacji, pierwszy zmierza do ochrony na nowo „wolności mediów”¹²⁵ jako wartości posiadającej samodzielne, samoistne znaczenie, która obejmuje aktywność dziennikarzy, nadawców oraz wydawców prasy, a także drugi kierunek, zmierzający do ochrony użytkowników internetu przed nielegalnymi treściami. Oba kierunki stanowią obszar działania europejskiego prawodawcy, który z jednej strony stanowi prawo w tych obszarach, a zarazem, z drugiej strony, koordynuje inicjatywy samoregulacyjne.

Przejawem aktywności prawodawcy europejskiego w pierwszym obszarze jest uchwalenie przez Parlament Europejski rozporządzenia „Europejski akt o wolności mediów” (*European Media Freedom Act*, AWM)¹²⁶, który wszedł w życie 7 maja 2024 r., a od 8 sierpnia 2025 r. będzie musiał być w pełni stosowany¹²⁷. W akcie tym uznaje się znaczenie mechanizmów samoregulacji w kontekście świadczenia usług medialnych na bardzo dużych

¹²⁵ AWM zostało uchwalone dnia 7.05.2024 r. przez Parlament Europejski, a wejdzie w życie i zacznie być stosowane począwszy od 8.08.2025 r. Co prawda w akcie tym przyjęto jako metodę regulacji harmonizację minimalną, jak bowiem wskazano w motywie 7, chodzi o „harmonizację niektórych aspektów przepisów krajowych związanych z pluralizmem mediów i niezależnością redakcyjną”, niemniej akt ten redefiniuje pozycję prasy na rynku usług cyfrowych, a w konsekwencji „wolność mediów”. O ile wskazuje się w motywach AWM, że państwa członkowskie mają możliwość przyjmowania bardziej szczególnych lub surowszych przepisów w konkretnych dziedzinach (motyw 8), to jednak warunkiem wykonywania tych kompetencji jest osiągnięcie „wyższego poziomu ochrony pluralizmu mediów lub niezależności redakcyjnej” (tamże), przy czym sposób rozumienia pojęcia „pluralizmu” i „niezależności redakcyjnej” powinien być zgodny z polityką UE, rozporządzeniem AWM oraz – ogólniej – z prawem Unii oraz z tym, że państwa członkowskie nie ograniczą swobodnego przepływu z innych państw członkowskich usług medialnych zgodnych z przepisami ustanowionymi w tych dziedzinach (motyw 7). Pojęcie pluralizmu występuje w AWM we wszystkich możliwych kontekstach (jako pluralizm treści, formy, mediów) i zostało użyte w tym akcie prawnym 55 razy. Pomimo wielokrotnego wykorzystania tego terminu, który służy – co należy podkreślić – do definiowania modelu „wolności mediów”, ustawodawca europejski go nie definiuje. Pojęcie pluralizmu staje się formułą, z jednej strony pustą, z drugiej jednak, na tyle istotną, że od wypełnienia jej treścią zależeć będzie ustalenie, czy podmioty publiczne, a także prywatne, zapewniają „wolność mediów” oraz czy nie dochodzi do jej naruszenia. W konsekwencji następuje przededefiniowanie „wolności mediów”, gdzie przesłanką *sine qua non*, swego rodzaju filtrem stosowanym do ustalenia poziomu wolności mediów, jest ich pluralizm.

¹²⁶ *Europejski akt o wolności mediów*, Komisja Europejska, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy/european-media-freedom-act_pl?etran=pl (dostęp: 23.05.2024).

¹²⁷ AWM.

platformach internetowych. Mechanizmy te – w ujęciu AWM – stanowią rodzaj dobrowolnych inicjatyw, np. w formie kodeksów postępowania, które umożliwiają dostawcom usług medialnych lub ich przedstawicielom przyjęcie między sobą i dla siebie wspólnych wytycznych, w tym dotyczących norm etycznych, korygowania błędów lub rozpatrywania skarg. Solidna, inkluzywna i powszechnie uznawana samoregulacja mediów stanowi – jak wskazano w uzasadnieniu wniosku KE¹²⁸ – skuteczną gwarancję jakości i profesjonalizmu usług medialnych i ma kluczowe znaczenie dla ochrony rzetelności redakcyjne.

W obszarze zapewnienia bezpieczeństwa użytkowników internetu przejawem aktywności prawotwórczej UE są rozporządzenia cyfrowe (AUC i ARC). Prawodawca europejski uznał za niezbędne dla zagwarantowania „bezpiecznego i godnego zaufania internetu”, wolnego od nielegalnych treści, skorzystanie z regulacji prawnych, co stanowi zarazem dowód na to, że miękkie rozwiązania, w tym kodeksy etyczne, zostały uznane za niewystarczająco skuteczne.

Nadal jednak prawodawca europejski zakłada, że istnieją obszary, które powinny być objęte współregulacją albo samoregulacją, a rolą Komisji Europejskiej jest wspieranie tych inicjatyw oraz „zapraszanie do wzięcia udziału w stosowaniu kodeksu postępowania (motyw 104 AUC). W AUC wskazuje się jednak także na potrzebę przyznania Komisji Europejskiej szerszych kompetencji niż inicjowanie i inspirowanie aktywności samoregulacyjnej. W motywie 107 AUC wskazano bowiem, że do kompetencji Komisji należy ocena stosowanych w kodeksach mechanizmów: „Aby zapewnić skuteczność kodeksów postępowania, Komisja powinna przewidzieć mechanizmy oceny przy opracowywaniu kodeksów postępowania. W stosownych przypadkach Komisja może zwrócić się do Agencji Praw Podstawowych lub Europejskiego Inspektora Ochrony Danych o wyrażenie opinii na temat danego kodeksu postępowania”.

W AUC postuluje się, by przedmiotem porozumień samoregulacyjnych i współregulacyjnych były obszary:

1. dotyczące stosowania środków zmniejszających ryzyko związane z określonymi rodzajami nielegalnych treści;
2. dezinformacji lub działań manipulacyjnych oraz nadużyć lub wszelkich negatywnych skutków dla małoletnich;

¹²⁸ AWM.

3. wykorzystania botów i zautomatyzowanego przetwarzania informacji (motyw 104 AUC), które rzutują, zdaniem prawodawcy europejskiego, na poziom ryzyka systemowego (motyw 104);
4. bezpieczeństwa produktów (*Product Safety Pledge* – motyw 106);
5. sprzedaży podrobionych towarów w internecie;
6. mowy nienawiści oraz
7. zwalczania dezinformacji (motyw 106).

W Akcie o wolności mediów do obszarów, które miałyby zostać objęte samoregulacją, należy świadczenie usług medialnych na bardzo dużych platformach internetowych (motyw 34). Mechanizmy samoregulacyjne, zgodnie z dyspozycjami zawartymi w AWM, powinny obejmować relacje istniejące pomiędzy prasą a platformami internetowymi. Powinny mieć charakter „dobrowolnych inicjatyw, np. w formie kodeksów postępowania, które umożliwiają dostawcom usług medialnych lub ich przedstawicielom przyjęcie między sobą i dla siebie wspólnych wytycznych, w tym dotyczących norm etycznych, korygowania błędów lub rozpatrywania skarg. Solidna, inkluzywna i powszechnie uznawana samoregulacja mediów stanowi skuteczną gwarancję jakości i profesjonalizmu usług medialnych i ma kluczowe znaczenie dla ochrony rzetelności redakcyjnej” (motyw 34 AWM).

Dostawcy bardzo dużych platform internetowych powinni nawiązać kontakt z dostawcami usług medialnych, którzy przestrzegają norm dotyczących wiarygodności i przejrzystości i którzy uważają, że dostawcy bardzo dużych platform internetowych często nakładają ograniczenia na ich treści bez wystarczających podstaw w celu znalezienia polubownego rozwiązania pozwalającego na zniesienie wszelkich nieuzasadnionych ograniczeń i uniknięcia ich w przyszłości. Dostawcy bardzo dużych platform internetowych powinni prowadzić taką wymianę w dobrej wierze, zwracając szczególną uwagę na ochronę wolności mediów i swobodny dostęp do informacji (motyw 35 AWM). Kodeksy postępowania powinny także powstawać w obszarze dokonywania pomiarów oglądalności. Kodeksy opracowane przez dostawców systemów pomiaru oglądalności usług miałyby służyć propagowaniu wysokich norm jakościowych w obszarze pomiaru oglądalności. Wskazano w motywie 47 AWM, że „dalszy rozwój samoregulacji można uznać za skuteczne narzędzie uzgadniania przez branżę praktycznych rozwiązań koniecznych do zapewnienia, aby systemy pomiaru oglądalności i stosowane w ich

ramach metody były zgodne z zasadami przejrzystości, bezstronności, inkluzywności, proporcjonalności, niedyskryminacji i możliwości sprawdzenia”.

Aktywność Komisji Europejskiej, stającej się *de facto* stroną tzw. kodeksów postępowań, oznacza, że prawodawca europejski chętnie włącza się w normowanie także tych rodzajów aktywności, których regulowanie było prerogatywą członków organizacji pozarządowych oraz korporacji zawodowych. Udział Komisji Europejskiej, która występuje w charakterze strony przy przyjmowaniu kodeksów postępowania, czyni te regulacje quasi-prawnymi. Do aktów tego typu należy w szczególności kodeks postępowania w zakresie zwalczania dezinformacji zgodnie z wytycznymi Komisji z maja 2021 r.¹²⁹, a także, uzgodniony w maju 2016 r. z Facebookiem, Microsoftem, Twitterem i YouTube’em, „Kodeks postępowania w zakresie zwalczania nielegalnego nawoływania do nienawiści w internecie”¹³⁰.

Komisja włącza się także w regulowanie działalności prasy i dziennikarzy, w szczególności poprzez „wsparcie finansowe dziennikarzy i innych pracowników sektora mediów” (motyw 7 Zalecenia w sprawie udzielenia ochrony); „ustanowienie punktów wsparcia, kontaktu i szybkiego reagowania oraz mechanizmów wczesnego ostrzegania” (motyw 15 Zalecenia w sprawie udzielenia ochrony), podnosząc jako argument przemawiający za tego rodzaju aktywnością zagrożenie bezpieczeństwa mediów i dziennikarzy¹³¹. Tworząc ramy dla wzmocnienia bezpieczeństwa prasy i dziennikarzy, KE odwołuje się

¹²⁹ Wzmocniony kodeks postępowania w zakresie zwalczania dezinformacji z 2022 r., <https://digital-strategy.ec.europa.eu/pl/library/2022-strengthened-code-practice-disinformation> (dostęp: 23.05.2024).

¹³⁰ The EU Code of conduct on countering illegal hate speech online, https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en?prefLang=pl&etrans=pl (dostęp: 23.05.2024).

¹³¹ KE zauważyła, że w ostatnich latach rośnie liczba gróźb fizycznych, prawnych i stosowanych za pośrednictwem internetu oraz ataków o takim charakterze skierowanych przeciwko dziennikarzom i innym pracownikom sektora mediów, udokumentowanych m.in. w sprawozdaniach Komisji na temat praworządności z lat 2020 i 2021 (4), co stanowi jednak niepokojącą tendencję; zob. Zalecenie Komisji (UE) 2021/1534 z dnia 16 września 2021 r. w sprawie zapewnienia ochrony i bezpieczeństwa dziennikarzom i innym pracownikom sektora mediów oraz wzmocnienia ich pozycji w Unii Europejskiej, motyw 3, https://commission.europa.eu/document/download/a5c92394-8e76-434a-9f3a-3a4977d399bb_en?filename=assessment_of_the_code_of_conduct_on_hate_speech_on_line_-_state_of_play_.pdf&prefLang=pl (dostęp: 23.05.2024).

także do celów realizowanych przez UE w strategii UE w zakresie praw ofiar na lata 2020–2025¹³² i strategii UE na rzecz równouprawnienia płci na lata 2020–2025¹³³, działania Komisji w obszarze szerzej rozumianej równości, szczególnie w ramach strategii na rzecz równości osób LGBTIQ na lata 2020–2025¹³⁴, unijny plan działania przeciwko rasizmowi na lata 2020–2025¹³⁵, plan działania na rzecz integracji i włączenia społecznego¹³⁶, unijne ramy strategiczne na rzecz równouprawnienia, włączenia społecznego i udziału Romów na lata 2020–2030¹³⁷ oraz strategię na rzecz praw osób z niepełnosprawnościami¹³⁸. Komisja wskazuje także na zgodność inicjatyw na rzecz bezpieczeństwa i wolności mediów z dokumentami programowymi dotyczącymi działań zewnętrznych, takich jak Plan działania UE dotyczący praw człowieka i demokracji na lata 2020–2024¹³⁹. Za pomocą zalecenia Komisja zmierza do „wzmocnienia wolności i pluralizmu mediów w UE dzięki wspieraniu wspólnych i skoordynowanych starań ze strony państw członkowskich w dążeniu do zwiększenia ochrony i bezpieczeństwa dziennikarzy i innych pracowników sektora mediów i wzmocnienia ich pozycji” (Motyw 11. Zalecenia w sprawie udzielenia ochrony).

¹³² Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 24 czerwca 2024 r.: Strategia UE w zakresie praw ofiar (2020–2025).

¹³³ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 5 marca 2020 r.: Unia równości: strategia na rzecz równouprawnienia płci na lata 2020–2025.

¹³⁴ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 12 listopada 2020 r.: Unia równości: strategia na rzecz równości osób LGBTIQ na lata 2020–2025.

¹³⁵ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 18 września 2020 r.: Unia równości: Unijny plan działania przeciwko rasizmowi na lata 2020–2025.

¹³⁶ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 24 listopada 2020 r.: Plan działania na rzecz integracji i włączenia społecznego na lata 2021–2027.

¹³⁷ Komunikat Komisji do Parlamentu Europejskiego i Rady z dnia 7 października 2020 r.: Unia równości: unijne ramy strategiczne na rzecz równouprawnienia, włączenia społecznego i udziału Romów.

¹³⁸ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 3 marca 2021 r.: Unia równości: Strategia na rzecz praw osób z niepełnosprawnościami na lata 2021–2030.

¹³⁹ Projekt konkluzji Rady w sprawie Planu działania UE dotyczącego praw człowieka i demokracji na lata 2020–2024, <https://data.consilium.europa.eu/doc/document/ST-12848-2020-INIT/pl/pdf> (dostęp: 23.05.2024).

Prawodawca unijny wyraża przekonanie, że „siła działań zewnętrznych UE w dziedzinie praw podstawowych zasadza się na sposobie, w jaki wspierane są i wzmacniane demokratyczne podstawy w Unii”¹⁴⁰. Kodeks postępowania w zakresie dezinformacji, jak zauważa Komisja Europejska na swojej stronie internetowej¹⁴¹, jest pierwszym tego rodzaju narzędziem, poprzez które istotne podmioty z branży uzgodniły – po raz pierwszy w 2018 roku – samoregulacyjne standardy walki z dezinformacją. Proces jego rewizji został rozpoczęty w czerwcu 2021 r., a jego zwieńczeniem było podpisanie i przedstawienie go 16 czerwca 2022 r. przez 34 sygnatariuszy¹⁴². Spełnia on założenia Wytycznych Komisji przedstawionych w maju 2021 r.¹⁴³. Przyjęcie kodeksu było poprzedzone wydaniem przez KE komunikatu, w którym KE zalecała zwalczanie nielegalnych treści w internecie, oczekując od platform internetowych większej odpowiedzialności¹⁴⁴. W dokumencie tym zaproponowano narzędzia samoregulacyjne do walki z dezinformacją w internecie, w tym:

1. Kodeks postępowania w sprawie dezinformacji online;
2. wsparcie dla niezależnej sieci weryfikacji faktów;
3. narzędzia do stymulowania dziennikarstwa wysokiej jakości.

¹⁴⁰ Zalecenie Komisji (UE) 2021/1534 z dnia 16 września 2021 r. w sprawie zapewnienia ochrony i bezpieczeństwa dziennikarzom i innym pracownikom sektora mediów oraz wzmocnienia ich pozycji w Unii Europejskiej, motyw 6.

¹⁴¹ Wprowadzenie do Kodeksu postępowania w zakresie zwalczania dezinformacji, <https://disinfocode.eu/pl/wprowadzenie-do-kodeksu/> (dostęp: 23.05.2024).

¹⁴² Tamże.

¹⁴³ Wytyczne UE w sprawie praw człowieka dotyczące wolności wypowiedzi w internecie i poza nim z dnia 12 maja 2014 r., Rada do spraw zagranicznych, <https://www.consilium.europa.eu/media/28348/142549.pdf> (dostęp: 23.05.2024).

¹⁴⁴ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 28 września 2017 r.: Zwalczanie nielegalnych treści w internecie. W kierunku większej odpowiedzialności platform internetowych, <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52017DC0555> (dostęp: 23.05.2024). W komunikacie przedstawiono zestawienie wytycznych i zasad, w ramach których wzywa się platformy internetowe do intensyfikacji zwalczania nielegalnych treści w internecie we współpracy z organami krajowymi, państwami członkowskimi i innymi odpowiednimi zainteresowanymi stronami. Celem komunikatu jest ułatwienie i intensyfikacja wdrażania dobrych praktyk w zakresie zapobiegania umieszczaniu nielegalnych treści, ich wykrywania, usuwania i uniemożliwiania dostępu do tego rodzaju treści, aby zapewnić skuteczne usuwanie nielegalnych treści, większą przejrzystość i ochronę praw podstawowych w internecie. Ponadto celem komunikatu jest dostarczenie platformom internetowym wyjaśnień na temat odpowiedzialności, jaką ponoszą, gdy podejmują aktywne działania w celu wykrycia nielegalnych treści, ich usunięcia lub uniemożliwienia dostępu do nich (tzw. działania dobrego samarytanina).

Tym samym zarysowane zostały propozycje konkretnych działań, jakie zdaniem Komisji można podjąć w krajach członkowskich¹⁴⁵. W odpowiedzi na Komunikat, Parlament Europejski wydał miesiąc później Rezolucję¹⁴⁶ w sprawie pluralizmu mediów i wolności mediów w Unii Europejskiej. Również ten dokument podkreśla znaczenie skutecznych systemów samoregulacji mediów społecznościowych i platform internetowych.

Biorąc za punkt wyjścia status umawiających się stron, wskazuje się w piśmiennictwie na kilka rodzajów regulacji dotyczących korzystania z wolności wypowiedzi:

1. regulacje prywatnoprawne;
2. regulacje publicznoprawne;
3. uzgodnienia prywatno-publiczne;
4. samoregulacje;
5. Kodeks techniczny lub *lex informatica*¹⁴⁷.

Pierwsze cztery (ale zwykle nie piąty) mogą być specyficzne dla danego kraju i różnić się od siebie.

Różne inicjatywy regulacyjne mogą:

1. prowadzić do fundamentalnych starć;
2. powodować drobne starcia;
3. współistnieć bez interakcji;
4. być ze sobą powiązane; lub
5. być współzależne¹⁴⁸.

Ostatecznie, niezależnie od rodzaju regulacji, normowanie zasad korzystania z wolności wypowiedzi, w szczególności w środowisku internetowym, wymaga z jednej strony determinacji, ale z drugiej strony także konsensusu¹⁴⁹.

¹⁴⁵ A. Ogrodowczyk, M. Borkowska, E. Murawska-Najmiec, K. Twardowska, *Fake news – dezinformacja online, próby przeciwdziałania tym zjawiskom z perspektywy instytucji międzynarodowych oraz wybranych państw UE, w tym Polski*, Warszawa 2018, s. 13; <https://www.gov.pl/attachment/e1eddda2-1304-45b6-84b7-141e5bd550c1> (dostęp: 25.05.2024).

¹⁴⁶ Rezolucja Parlamentu Europejskiego z dnia 3 maja 2018 r. w sprawie pluralizmu mediów i wolności mediów w Unii Europejskiej (2017/2209(INI)). Więcej informacji: patrz Załącznik, pkt 6, <https://eur-lex.europa.eu/legal-content/pl/TXT/PDF/?uri=CELEX:52018IP0204&from=GA> (dostęp: 23.05.2024).

¹⁴⁷ D. Jerker, B. Svantesson, *Global status...*

¹⁴⁸ Tamże, s. 52.

¹⁴⁹ Tamże.

Ze strony prawodawcy europejskiego następuje przewłaszczanie kompetencji¹⁵⁰ w dziedzinie samoregulacji mediów. Organy UE podtrzymują więc, a nawet wzmacniają stanowisko, zgodnie z którym kodeksy postępowania (kodeksy etyki) mają istotne znaczenie dla zapewnienia wolności wypowiedzi i wolności mediów, jednakże równolegle podejmują działania polegające na koordynowaniu, ocenianiu, udzielaniu wiążących wytycznych, a nawet podpisywaniu (sygnowaniu) kodeksów, które to działania – *de facto* – naruszają istotę samoregulacji.

Na wysoką rangę kodeksów etyki przy wykonywaniu obowiązków zawodowych przez dziennikarzy zwracał także nieustannie uwagę ETPC. Wydaje się jednak, że ETPC postulując działania zgodne z zasadami etyki, miał na myśli wypracowane przez środowisko zawodowe, bez udziału prawodawcy europejskiego, normy obyczajowe i ich skodyfikowane wzorce zawarte w aktach deontologii dziennikarskiej. Do uwolnienia się od odpowiedzialności przez dziennikarzy za nadużycie wolności wypowiedzi nie wystarcza, jak zwraca uwagę I.C. Kamiński, powołanie się na status prasy i działanie w granicach interesu publicznego, lecz konieczne jest przestrzeganie etyki zawodowej, w tym działanie w dobrej wierze. Trybunał wskazywał na triadę obowiązków dziennikarzy¹⁵¹. Należą do nich:

¹⁵⁰ Termin „pełzanie kompetencji” (*competence creep*) oznacza proces, w którym instytucje Wspólnot stopniowo pozbawiają kompetencji państw członkowskich (T.T. Konciewicz, *Niedoskonałości zasady kompetencji powierzonych i teoria kompetencji dorozumianych (domniemanych) Wspólnot Europejskich*, [w:] tenże, *Zasada jurysdykcji powierzonej Trybunału Sprawiedliwości Wspólnot Europejskich*, Warszawa 2009, s. 67). Jest to proces o charakterze politycznym zmierzający do dalszego pogłębienia Wspólnoty. Polega on w szczególności na stosowaniu prawa, kiedy to zniekształceniu ulega element przewidywalności prawa unijnego oraz zaburzony jest system odpowiedzialności, a nie jest to tryb podejmowania decyzji doprecyzowany w postanowieniach traktatu (zob. D. Bach-Golecka, *Otwarta metoda koordynacji*, [w:] *Źródła prawa. Teoria i praktyka*, T. Giaro (red.), Warszawa 2016, s. 25). Pełzanie kompetencji przejawia się także poprzez „liberalną interpretację »podstawy prawnej« zarówno przez instytucje Unii, jak i TS. Przyczynia się do tego także nierozróżnianie w praktyce organów unijnych zakresu zastosowania traktatów od kompetencji do działania, najczęściej stanowienia prawa” (zob. A. Wróbel, *Rec.: L. Bresselink, F. Pennings, S. Prechal (red.), The Eclipse of the Legality Principle in the European Union*, „Europejski Przegląd Sądowy” 2011, nr 11, s. 56–57).

¹⁵¹ Wyrok ETPC z dnia 20 maja 1999 r. w sprawie Bladet Tromsø i Stensaas przeciwko Norwegii, skarga nr 21980/93 (dalej: Wyrok ETPC w sprawie Bladet Tromsø i Stensaas przeciwko Norwegii).

1. przestrzeganie etyki;
2. dobra wiara;
3. szczególna staranność i rzetelność¹⁵².

Trybunał, odwołując się do przesłanek wypracowanych na gruncie art. 10 ust. 2 (trójelementowy test) i dokonując ustalenia dopuszczalności ingerencji w wolność wypowiedzi dziennikarzy, odwołuje się do kodeksów deontologii dziennikarskiej. W treści orzeczeń pojawia się zatem adresowane do dziennikarzy oczekiwanie zachowania dobrej wiary (fr. *bonne foi*), przestrzegania etyki dziennikarskiej (fr. *respecter aux standards éthiques*), potrzeba wykazania działania w granicach usprawiedliwionego błędu (fr. *raisonnablement croire*), równowagi prawdopodobieństwa (fr. *balance de probabilité*) oraz aby informacja przekazywana przez dziennikarzy była wystarczająco precyzyjna i wiarygodna (fr. *suffisamment précis et fiable*), i aby nie dążyła jedynie do zaspokojenia publicznej ciekawości (fr. *curiosité public*), zawierając komponentę ważną ze względu na realizację interesu publicznego (fr. *une composante essentielle de l'intérêt public*). Pojawia się także postulat godziwej informacji (fr. *dignité de l'information*)¹⁵³.

Pojęciami tymi ETPC posługuje się m.in. w sprawach Ciné Revue przeciwko Belgii¹⁵⁴ (ujawnienie notatek sędzi, która miała zeznawać przed komisją parlamentarną podczas badania sprawy porwań dzieci w sprawie afery Dutroux); Stoll przeciwko Szwajcarii¹⁵⁵ (ujawnienie korespondencji dyplomatycznej dotyczącej negocjacji ze Światowym Kongresem Żydów w sprawie wypłat przez banki szwajcarskie odszkodowań ofiarom holokaustu); Ziemiński przeciwko Polsce¹⁵⁶ (zniesławienie starosty polegające na złośliwym pomówieniu go o ukrywanie afery korupcyjnej w miejscowym szpitalu);

¹⁵² I.C. Kamiński, *Ograniczenia swobody wypowiedzi...*, s. 49.

¹⁵³ J. Taczkowska-Olszewska, *Racjonalizacja wolności prasy. Od modelu absolutnego do warunkowego. Europejski i krajowy kontekst wykładni prawa*, „Przegląd Sejmowy” 2018, nr 1, s. 128.

¹⁵⁴ Wyrok ETPC z dnia 9 listopada 2006 r. w sprawie Leempoel and S.A. Ed. Cine Revue przeciwko Belgii, skarga nr 64772/01 (dalej: Wyrok ETPC w sprawie Leempoel przeciwko Belgii).

¹⁵⁵ Wyrok ETPC z dnia 10 grudnia 2007 r. w sprawie Stoll przeciwko Szwajcarii, skarga nr 69698/01.

¹⁵⁶ Wyrok ETPC z dnia 24 listopada 2012 r. w sprawie Ziemiński przeciwko Polsce, skarga nr 46712/06 (dalej: Wyrok ETPC w sprawie Ziemiński przeciwko Polsce).

Sanocki przeciwko Polsce¹⁵⁷ (pomówienie burmistrza Nysy o naruszenie dyscypliny finansów publicznych i odpowiedź burmistrza Nysy w innym czasopiśmie, w którym nazwał rozpowszechnianie nieprawdziwych informacji przez dziennikarza „bolszewickim dziennikarstwem”) – sądy polskie uznały działanie burmistrza za dopuszczalne, dziennikarz odwołał się do Trybunału, a ten powołał się na zasady słusznej równowagi i prasy jako gracza politycznego i stwierdził, że można poddać krytyce działanie prasy; Kania, Kittel przeciwko Polsce¹⁵⁸ (warszawska prokuratura ustaliła: minister wziął); Błaja News przeciwko Polsce¹⁵⁹ (w tygodniku „Fakty i Mity” autor artykułu *Prokurator Anna* stwierdził, że prokurator ma związki ze światem przestępczym, uczestniczy w handlu narkotykami, że toczy się przeciwko niej postępowanie karne; Trybunał uznał, że dziennikarze mają obowiązek dostarczania wiarygodnych informacji, działania w dobrej wierze i zgodnie z etyką zawodową)¹⁶⁰.

Pomimo jednak dużej wagi, jaką w orzecznictwie ETPC przywiązywano do kanonów etyki, Trybunał zakwestionował w sprawie Bajer przeciwko Polsce¹⁶¹ prawo organizacji zawodowych i powołanego przez nie organu, tj. Rady Etyki Mediów¹⁶², do formułowania i publicznego udostępnienia negatywnej

¹⁵⁷ Wyrok ETPC z dnia 17 października 2007 r. w sprawie Sanocki przeciwko Polsce, skarga nr 28949/03.

¹⁵⁸ Wyrok ETPC z dnia 21 czerwca 2011 r. w sprawie Kania i Kittel przeciwko Polsce, skarga nr 35105/04.

¹⁵⁹ Wyrok ETPC z dnia 26 listopada 2013 r. w sprawie Błaja News sp. z o.o. przeciwko Polsce, skarga nr 59545/10 (dalej: Wyrok ETPC w sprawie Błaja przeciwko Polsce).

¹⁶⁰ Wyrok ETPC w sprawie Błaja przeciwko Polsce.

¹⁶¹ Wyrok ETPC w sprawie Lingens przeciwko Austrii. Decyzja ETPC w sprawie Bajer przeciwko Polsce.

¹⁶² Chodzi o Radę Etyki Mediów, która jest organem Stowarzyszenia Konferencja Mediów Polskich (SKMP). Członkowie Rady są wybierani w liczbie od 11 do 13 osób przez SKMP w głosowaniu tajnym większością bezwzględną obecnych prawidłowo zawiadomionych członków. Kadencja Rady trwa cztery lata i kończy się nie później niż z chwilą ukonstytuowania się nowej REM. Członka REM nie można odwołać w czasie trwania kadencji, może on złożyć rezygnację. Zgodnie z § 5 ust. 3 Statutu SKMP zadaniem Rady Etyki Mediów jest w szczególności: a) upowszechnianie, promowanie oraz wzmacnianie norm etycznych i przejawów dobrych praktyk, jakimi powinni kierować się dziennikarze i inne osoby zaangażowane w działalność środków społecznej komunikacji; b) wspieranie zasady wolności wypowiedzi i prawa do rzetelnej informacji i krytyki społecznej oraz kontroli w tym zakresie; c) ochrona niezależność dziennikarzy i środków komunikacji społecznej; d) reprezentowanie stanowiska organizacji dziennikarzy

oceny etycznej postawy dziennikarzy, jeśli ocena ta nie została oparta na rozważeniu przesłanek wynikających z przepisów prawa materialnego (art. 12 ustawy Prawo prasowe¹⁶³) i przesłanek natury prawnej. W Decyzji z dnia 8 listopada 2022 r. ETPC stwierdził, że negatywna ocena pracy dziennikarzy śledczych wyrażona przez REM na podstawie jednego opublikowanego materiału prasowego, który dotyczył osoby publicznej, pomimo że zawierał informacje, które w następstwie postępowania karnego okazały się nieprawdziwe, a osoba ta została uniewinniona od zarzutów, o których pisali dziennikarze, to jednak nie uprawniało to REM do wyrażenia publicznie negatywnej oceny o pracy tych dziennikarzy. ETPC stwierdził, że REM nie przeprowadziła „żadnego dochodzenia w celu ustalenia metody pracy dziennikarzy ani ich rzekomego braku staranności”¹⁶⁴. REM opublikowała jednak oświadczenie, w którym podważyli A.M. i B.K. jako profesjonalnych i rzetelnych dziennikarzy¹⁶⁵.

Rozstrzygnięcie ETPC w sprawie Bajer przeciwko Polsce analizowane na tle opisanej powyżej aktywności prawodawcy europejskiego w dziedzinie samoregulacji potwierdzają, że kodeksy etyki oraz inne uzgodnienia czynione pomiędzy podmiotami prywatnymi poza auspicjami organów publicznych, przede wszystkim bez udziału Komisji Europejskiej, tracą na znaczeniu i przybierają jedynie fasadową postać. Posiadanie kodeksu etyki jest zatem dobrze widziane, ale jego zastosowanie i faktyczne znaczenie zależy od poziomu zbieżności zawartych w nim postanowień z kodeksami postępowania uzgodnionymi z Komisją Europejską.

w istotnych wspólnych dla nich sprawach, włączając się w procesy legislacyjne i opiniując projekty aktów prawnych; Statut SKMP: <https://www.rem.net.pl/projects.php> (dostęp: 23.05.2024).

¹⁶³ Chodziło przede wszystkim o niedokonanie przez REM oceny pod kątem zawartego w art. 12 ustawy z dnia 26 stycznia 1984 r. – Prawo prasowe (t.j. Dz.U. z 2018 r., poz. 1914 – dalej: pr.pr. albo Prawo prasowe) obowiązku szczególnej staranności i rzetelności. Zgodnie z art. 12 ust. 1.: „Dziennikarz jest obowiązany: 1) zachować szczególną staranność i rzetelność przy zbieraniu i wykorzystaniu materiałów prasowych, zwłaszcza sprawdzić zgodność z prawdą uzyskanych wiadomości lub podać ich źródło; 2) chronić dobra osobiste, a ponadto interesy działających w dobrej wierze informatorów i innych osób, które okazują mu zaufanie”.

¹⁶⁴ Decyzja ETPC w sprawie Bajer przeciwko Polsce, pkt 22.

¹⁶⁵ Tamże.

2. Ewolucja ochrony – uwarunkowania (determinanty) jednolitego rynku cyfrowego

A. Internet – nowa przestrzeń korzystania z wolności wypowiedzi

Jednolity rynek cyfrowy stanowi obszar bez granic terytorialnych¹⁶⁶, który ze względu na jego usytuowanie w cyberprzestrzeni¹⁶⁷ oraz specyfikę środków informacyjno-komunikacyjnych (ICT) wykorzystywanych przez jego użytkowników (usługobiorców i usługodawców) do świadczenia usług społeczeństwa informacyjnego¹⁶⁸, tworzy nieograniczone, w znaczeniu faktycznym, możliwości komunikowania, w tym zarówno o charakterze publicznym, jak i prywatnym (poczta elektroniczna, komunikatory internetowe), przy wykorzystaniu tekstu (komunikowanie werbalne) oraz gestu, dźwięku lub obrazu (komunikowanie niewerbalne).

Nieograniczona terytorialnie przestrzeń, która umożliwia bez jakichkolwiek fizycznych barier korzystanie, przekazywanie, otrzymywanie i generowanie treści, nie jest pozbawiona barier regulacyjnych. Granice wolności

¹⁶⁶ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 6 maja 2015 r.: Strategia jednolitego rynku cyfrowego dla Europy, pkt 3.3.1.

¹⁶⁷ Przez pojęcie cyberprzestrzeni, zgodnie z przyjętą na gruncie ustaw o stanach nadzwyczajnych definicją, ustawodawca rozumie przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne – ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2019 r., poz. 700, z późn. zm.), wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami. W treści definicji obecne jest zarówno pojęcie informacji, jak i pojęcie systemów teleinformatycznych, które to pojęcia – jak się wydaje – stanowią jądro definicji cyberprzestrzeni (J. Tackowska-Olszewska, *Cyberprzestrzeń jako...*). Ustawodawca zdecydował się na umieszczenie i zdefiniowanie pojęcia cyberprzestrzeni w treści ustaw o stanach nadzwyczajnych, tj. ustawy o stanie wojennym (art. 2 ust. 1b) – ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (t.j. Dz.U. z 2017 r., poz. 1932) – a także ustawy o stanie wyjątkowym (art. 2 ust. 1a) – ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (t.j. Dz.U. z 2017 r., poz. 1928) – oraz ustawy o stanie klęski żywiołowej (art. 3 ust. 1 pkt 4) – ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (t.j. Dz.U. z 2017 r., poz. 1897).

¹⁶⁸ Usługa społeczeństwa informacyjnego to, zgodnie z art. 1 ust. 1 lit. a dyrektywy w sprawie usług społeczeństwa informacyjnego, każda usługa normalnie świadczona za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy.

wypowiedzi poszerzyły się w związku z likwidowaniem barier fizycznych i technologicznych komunikacji jedynie pozornie i proporcjonalnie do rozrostu przestrzeni oraz środków technicznych ułatwiających komunikację. Korzystanie z wolności wypowiedzi w internecie może bowiem okazać się bardziej ograniczone niż w sferze realnej. Cyberprzestrzeń, ze względu na swoją specyfikę, tworzy nie tylko dogodne warunki dla realizacji wolności wypowiedzi, ale także zachęca do stosowania środków ograniczających tę wolność, takich jak w szczególności monitorowanie, filtrowanie czy śledzenie użytkowników i blokowanie treści. Odczucie braku kontroli i anonimowości towarzyszy zarówno tym, którzy są dostawcami treści, jak i tym, którzy treści te monitorują.

Wolność wypowiedzi w cyberprzestrzeni nie jest zatem nieskrępowana. Przeciwnie, może podlegać reglamentacji zarówno poprzez zastosowanie instrumentów prawnych, jak i narzędzi pozaprawnych znamionujących rzeczywiste władztwo, jakie posiadają niektórzy przedsiębiorcy ze względu na charakter świadczonych przez nich usług. Chodzi o tzw. usługi pośrednie, których niezakłócone świadczenie jest warunkiem dostępu do sieci i jej zawartości. Podmioty świadczące usługi dostępu do internetu oraz transmisji (*mere conduit*) i przechowywania danych (*hosting*) zaliczane są do grupy tzw. pośredników internetowych. Już w 2015 r. Komisja Europejska zauważyła w Komunikacie „Strategia Jednolitego rynku cyfrowego dla Europy”, że pośrednicy, w tym świadczący usługę platformy internetowej (np. wyszukiwarki internetowe, media społecznościowe, platformy handlu elektronicznego, sklepy z aplikacjami, porównywarki cen) odgrywają coraz ważniejszą rolę w życiu społecznym i gospodarczym: umożliwiają one konsumentom znalezienie informacji w internecie, a przedsiębiorstwom – wykorzystanie zalet handlu elektronicznego¹⁶⁹.

Platformy¹⁷⁰ wytwarzają, gromadzą i kontrolują ogromne ilości danych o swoich klientach i za pomocą algorytmów przekształcają je w użyteczne

¹⁶⁹ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 6 maja 2015 r.: Strategia jednolitego rynku cyfrowego dla Europy, pkt 3.3.1.

¹⁷⁰ Próbę zdefiniowania pojęcia platform internetowych podjęto w Rezolucji Parlamentu Europejskiego z dnia 15 czerwca 2017 r. w sprawie platform internetowych i jednolitego rynku cyfrowego, 2016/2276(INI), (Dz.U. UE C z 2018 r. Nr 331, s. 135). Wskazano w niej, że „bardzo trudno będzie osiągnąć jednolitą, odpowiednią pod względem prawnym i ukierunkowaną na przyszłość definicję *platform internetowych* na szczeblu

informacje. Wpływ takich platform na rynek zależy od ich rodzaju i pozycji, jednak niektóre z nich mogą kontrolować dostęp do rynków internetowych i w zasadniczy sposób wpływać na sposób wynagradzania różnych podmiotów na tych rynkach¹⁷¹. Zauważono zarazem, że internet rozwijał się w Europie w oparciu o zasadę zapisaną w dyrektywie o handlu elektronicznym, zgodnie z którą pośredniczący dostawcy usług internetowych nie powinni odpowiadać za treści, które przekazują, przechowują lub hostują, o ile ich działanie ma całkowicie bierny charakter. Jednocześnie w przypadku wykrycia nielegalnych treści, czy to informacji o nielegalnej działalności, np. o terroryzmie lub pornografii dziecięcej, czy to informacji naruszających prawa majątkowe osób trzecich (np. prawa autorskie), pośrednicy powinni podjąć skuteczne działania w celu usunięcia takich treści¹⁷². Spostrzeżono zarazem, że zablokowanie dostępu do nielegalnych treści lub ich usunięcie przez dostawców usług hostingowych bywało długotrwałe i skomplikowane, a jednocześnie zdarzało się, że omyłkowo usuwano treści, które w rzeczywistości nie naruszają prawa¹⁷³. Z oceny KE dokonanej w 2015 r. wynikało, że 52,7% zainteresowanych stron uważa, że działania podejmowane przeciwko nielegalnym treściom są często nieskuteczne i nieprzejrzyste¹⁷⁴.

Wobec powyżej wskazanych ustaleń Komisja Europejska uznała za konieczne zbadanie:

1. przejrzystości np. wyników wyszukiwania (zawierających opłacone linki lub reklamy),
2. wykorzystywania przez platformy pozyskiwanych przez nie informacji,
3. stosunków między platformami i dostawcami,

UE, ze względu na takie czynniki, jak duża różnorodność typów istniejących platform online i obszarów ich działalności, a także szybko zmieniające się środowisko świata cyfrowego; wyraża przekonanie, że w każdym przypadku unijna definicja ani uniwersalne podejście nie pomoże UE w osiągnięciu sukcesu w ramach gospodarki platform” (pkt 6). Wskazano zarazem, że należy dokonać wyraźnego rozróżnienia między platformami B2C i B2B w świetle powstawania platform internetowych B2B, które są kluczowe dla rozwoju internetu przemysłowego (pkt 13).

¹⁷¹ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 6 maja 2015 r.: Strategia jednolitego rynku cyfrowego dla Europy, pkt 3.3.1.

¹⁷² Tamże, pkt 3.3.2.

¹⁷³ Tamże, pkt 3.3.2.

¹⁷⁴ Tamże, pkt 3.3.2.

4. stosowanych wobec osób prywatnych i przedsiębiorstw ograniczeń w przenoszeniu się z jednej platformy na drugą, oraz
5. najlepszych rozwiązań w zakresie zwalczania nielegalnych treści w internecie¹⁷⁵.

Wyniki dokonanej oceny przesądziły ostatecznie o potrzebie wdrożenia wspólnych dla całej Unii regulacji, które normują działalność dostawców usług pośrednich.

W odniesieniu do potrzeby normowania swobody przepływu usług w internecie, a w konsekwencji także regulowania wolności wypowiedzi, ścierały się dwie tendencje, pierwsza ukierunkowująca działania prawodawcze na potwierdzenie i gwarantowanie szerokiego spektrum wolności (koncepcja wolnościowa)¹⁷⁶ oraz druga, zwracająca szczególną uwagę na potrzebę „zarządzania” internetem (koncepcja reglamentacyjna). Ł. Morawski spostrzega, że:

z jednej strony widoczne jest poszanowanie i ochrona wielostronnego modelu zarządzania internetem, a z drugiej tendencja do zwiększania zakresu kontroli i wpływu rządów na internet. Stawką w tej dyskusji jest przyszłość globalnej sieci – jej otwarty, wolny i niepodzielony charakter – z której użytkownicy będą mogli korzystać w bezpieczny sposób, ciesząc się swoimi prawami bez narażania się na utratę prywatności¹⁷⁷.

¹⁷⁵ Tamże, pkt 3.3.2.

¹⁷⁶ J. Sobczak zauważa (*Komentarz...*), że w doktrynie istnieje silna, aczkolwiek wcale nie powszechna tendencja odróżniania wolności od praw. Niektórzy jednak traktują wolności jako specyficzny rodzaj praw obywatelskich, częstokroć dzieląc prawa jednostki na uprawnienia (prawa *sensu stricto*) i wolności. Generalnie jednak prawa i wolności przysługują określonemu podmiotowi. Jak stwierdza L. Wiśniewski, znamieniem wolności jest to, że nie wynika ona, jako wolność człowieka i jako wolność obywatela, z prawa w znaczeniu przedmiotowym, a prawo ustanawia jedynie granice wolności. Poprzez normy prawne państwo ma także obowiązek chronić wolności w zakresie, w jakim nie są one ograniczane (L. Wiśniewski, *Prawo a wolność człowieka – pojęcie i konstrukcja prawna*, [w:] *Podstawowe prawa jednostki i ich sądowa ochrona*, L. Wiśniewski (red.), Warszawa 1997, s. 58).

¹⁷⁷ Ł. Morawski, *Unia Europejska wobec procesu zarządzania internetem*, „Teka Komisji Politologii i Stosunków Międzynarodowych” 2016, t. 11, nr 3, s. 112.

Internet w ujęciu technicznym to:

ogólnoświatowa sieć komputerowa, łącząca lokalne sieci korzystające z pakietowego protokołu komunikacyjnego TCP/IP, mająca jednolite zasady adresowania i nazywania węzłów (komputerów włączonych do sieci) oraz protokoły udostępniania informacji¹⁷⁸.

Takie ujęcie pozwala na wyróżnienie trzech warstw internetu, tj.: fizycznej, logicznej i treści¹⁷⁹. W piśmiennictwie wskazuje się, że:

na warstwę fizyczną nakłada się warstwa logiczna, czyli protokoły, standardy techniczne i oprogramowanie, dzięki któremu warstwa fizyczna może funkcjonować jako narzędzie komunikacji. Mowa tutaj o kodzie komputerowym, który jest odpowiednikiem kodu komunikacyjnego. W tym znaczeniu kod służy do konstruowania i interpretowania wypowiedzi zarówno pomiędzy maszynami, maszyną a człowiekiem, jak i pomiędzy ludźmi¹⁸⁰.

W skład warstwy treści wchodzi przesłane znaki – wiadomości przekazywane za pośrednictwem poczty elektronicznej, teksty, filmy, utwory muzyczne zapisane w postaci cyfrowej¹⁸¹.

¹⁷⁸ Hasło: *Internet*, [w:] *Encyklopedia PWN*, <https://encyklopedia.pwn.pl/haslo/Internet;3915155.html> (dostęp: 23.05.2024). Internet składa się z trzech poziomów: sieć szkieletowa internetu obejmuje zespół węzłów w USA; każdy z węzłów zawiera pełną informację o wszystkich sieciach dołączonych do internetu i o trasach, którymi należy kierować pakiety przeznaczone do tych węzłów; do sieci szkieletowej są przyłączone serwery i rutery, którymi (bezpośrednio bądź pośrednio) administrują dostawcy internetu; użytkownicy są przyłączeni do internetu za pośrednictwem poszczególnych dostawców. Informacje w internecie są przesyłane w postaci tzw. pakietów o średniej wielkości ok. 1500 bajtów; komputery włączone do internetu (węzły, ang. *host*) są oznaczone wieloczlówkowymi identyfikatorami liczbowymi (np. 140.186.81.1) i literowymi (np. *merlin.cobb.ziff.com*), przy czym pierwsza część identyfikatora jest nazwą komputera, a następne określają tzw. domeny (strefy) oznaczające instytucję, rodzaj instytucji (np. *edu* – instytucja edukacyjna, *gov* – rządowa), miasto i in.; ostatnia część identyfikatora zwykle oznacza państwo (np. *pl* – Polska, *uk* – Wielka Brytania).

¹⁷⁹ J. Hofmolk, *Internet jako nowe dobro wspólne*, Warszawa 2009, s. 121; cyt. za: Ł. Morawski, *Unia Europejska wobec...*, s. 112.

¹⁸⁰ Tamże, s. 113.

¹⁸¹ Tamże, s. 113.

W ujęciu EKPC i KPP, a także na gruncie prawa krajowego, w szczególności art. 14 Konstytucji RP, internet jest środkiem społecznego komunikowania (środkiem masowego przekazu), który może być wykorzystywany w różnych celach, a zatem w celu wydawania prasy, nadawania programów radiowych i telewizyjnych, ale także w celu świadczenia innych usług. Sąd Najwyższy wskazał, że:

środkami masowego komunikowania będą wszystkie środki, których działanie sprowadza się do masowego przekazywania rozmaitych treści. Czyli do środków tych wypadnie zaliczyć nie tylko prasę drukowaną, przekaz radiowy i telewizyjny, lecz także książkę, plakat, film oraz przekaz za pomocą Internetu¹⁸².

Cechą internetu jako środka przekazu informacji, na co zwrócił uwagę Sąd Najwyższy, jest to, że:

zapewnia on dostęp do opublikowanych w nim treści każdemu, kto ma odpowiednie do tego urządzenia techniczne, i w każdym dowolnym czasie. Pod określonymi adresami internetowymi – mogącymi pełnić funkcję taką samą jak stały tytuł publikacji wydawanej w formie drukowanej – istnieją strony mające także stałe nazwy, na których mogą być zamieszczane materiały prasowe. Internet jako środek masowego komunikowania umożliwia – inaczej niż wcześniej znane środki przekazywania – bieżącą i wielokrotną aktualizację umieszczonych na stronach internetowych treści. W przypadku prasy w formie drukowanej każde wydanie numeru (np. dziennika czy czasopisma) ma niezmienną treść¹⁸³.

¹⁸² Postanowienie SN z dnia 7 maja 2008 r., III KK 234/07, OSNKW 2008, nr 9, poz. 69. Sąd Najwyższy powiązał w powyższym orzeczeniu dwa terminy, których zakresy są tożsame, tj. „środki masowego przekazu” występujący na gruncie Kodeksu karnego (art. 212 kk) z terminem użytym przez ustrojodawcę w art. 14 Konstytucji, tj.: „środki społecznego komunikowania”, na co zwrócił uwagę Trybunał Konstytucyjny (zob. Wyrok TK z dnia 12 maja 2008 r., SK 43/05, OSNP A 2008, nr 4, poz. 57).

¹⁸³ Wyrok SN z dnia 28 października 2016 r., I CSK 695/15, OSNC 2017, nr 6, poz. 73, podobnie: wyrok NSA z dnia 5 września 2023 r., III OSK 696/22, LEX nr 3601912.

Sąd Najwyższy w postanowieniu z dnia 15.12.2010 r. porównał internet do ryzy papieru:

Internet jest tylko środkiem przekazu, podobnie jak ryza papieru. Papieru jako takiego nikt nie może rejestrować, natomiast rejestracji podlega papier zadrukowany, a w zasadzie nie sam papier, a tylko działalność polegająca na zadrukowywaniu papieru i wydawaniu go w formie dziennika bądź czasopisma – a więc prasy. Internet jest środkiem przekazu. Za jego pośrednictwem wymienia się korespondencję, podobnie jak przekazuje się korespondencję w formie pisemnej na papierze¹⁸⁴.

Wskazuje się, że najbardziej popularne funkcjonalności internetu to:

system dokumentów hipertekstowych (www), z którym jest najczęściej utożsamiany; poczta elektroniczna, system wymiany plików, telefonia internetowa (VoIP), media społecznościowe, portale internetowe, usługi bankowe, platformy handlowe, blogi i vlogi, podcasty, usługi streamingowe¹⁸⁵.

Uzyskanie wpływu na zakres lub sposób wykorzystania internetu, a w tym na decyzje dotyczące dostępu do zasobów danych znajdujących się w internecie oraz zasady ich przechowywania i transmisji, oznacza, w znaczeniu formalnym i materialnym, przejęcie realnego władztwa nad zachowaniem się podmiotów publicznych i prywatnych w cyberprzestrzeni. Zarządzanie internetem, w szerokim rozumieniu¹⁸⁶, wywoływać może skutek faktyczny

¹⁸⁴ Postanowienie SN z dnia 15 grudnia 2010 r., III KK 250/10, OSNKW 2011, nr 3, poz. 26.

¹⁸⁵ J. Czopek, Hasło: *Internet*, [w:] *Leksykon terminów medialnych*, K. Wolny-Zmorszyński (red.), Toruń 2024, s. 311.

¹⁸⁶ Jak zauważa Ł. Morawski, w ujęciu szerokim „zarządzania internetem” poza zagadnieniami technicznymi pojawiają się wartości, normy, procedury decyzyjne oraz całe spektrum podmiotów, które mają za zadanie określenie norm i procedur oraz sposobu ich wdrażania. Ujęcie wąskie sprowadza się do kwestii infrastruktury internetu oraz standardów technicznych, w oparciu o które funkcjonuje. W tym sensie chodzi głównie o dwie pierwsze warstwy internetu (fizyczną i logiczną) oraz o techniczne aspekty funkcjonowania warstwy treści, czyli standardy, za pomocą których dane są przetwarzane i przesyłane w sieci, takie jak HTML₁₃ czy SGML₁₄. W ujęciu szerokim zarządzanie internetem poza oczywistymi zagadnieniami technicznymi wkracza w szeroko rozumiane polityki

w postaci stymulowania zachowań poprzez ich monitorowanie, kontrolowanie i napiętnowanie albo nagradzanie. Wzmacnianiu podlegać mogą zachowania pożądane, zgodnie z priorytetami podmiotu zarządzającego, oraz osłabiane (napiętnowane) mogą być zachowania niezgodne z interesem tego podmiotu.

Organy UE w warstwie werbalnej stoją na stanowisku, zgodnie z którym „Internet powinien pozostać jednolitą, otwartą, wolną, niepodzielną siecią sieci, podlegającą tym samym przepisom i normom, które mają zastosowanie w innych obszarach naszego życia codziennego”¹⁸⁷. Jednocześnie UE uznaje za konieczne zarządzanie internetem, które jest rozumiane jako:

opracowywanie i wypełnianie przez administrację publiczną, sektor prywatny i społeczeństwo obywatelskie, w ich właściwych rolach, wspólnych zasad, norm, przepisów, procedur podejmowania decyzji oraz programów, które kształtują rozwój internetu i korzystanie z niego¹⁸⁸.

społeczne, z którymi globalna sieć jest nierozłącznie związana (*Internet public policy issues*). Mowa tutaj o wszelkiego rodzaju zachowaniach związanych ze sposobem użytkowania internetu na poziomie warstwy treści. (zob. Ł. Morawski, *Unia Europejska wobec...*, s. 112).

¹⁸⁷ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Polityka wobec internetu i zarządzanie internetem. Rola Europy w kształtowaniu przyszłości zarządzania internetem, pkt 9, [https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52014DC0072R\(01\)](https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52014DC0072R(01)) (dostęp: 23.05.2024).

¹⁸⁸ W 2005 r. podczas Światowego Szczytu Społeczeństwa Informacyjnego (*World Summit on Information Society – WSIS*) w Agendzie z Tunisu (*Tunis Agenda*) przyjęto roboczą definicję zarządzania internetem, która określa ten proces jako „rozwój oraz stosowanie przez rządy, sektor prywatny oraz społeczeństwo obywatelskie, odpowiednio w ramach ich zadań, wspólnych zasad, norm, reguł, procedur decyzyjnych oraz programów kształtujących rozwój i sposób korzystania z internetu” (zob. Ł. Morawski, *Unia Europejska wobec...*, s. 112). W dokumentach UE definicja ta jest przytaczana z powołaniem się na „powszechne jej rozumienie” (zob. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Polityka wobec internetu i zarządzanie internetem. Rola Europy w kształtowaniu przyszłości zarządzania internetem, pkt 1). Przytaczane są także stanowiska wypracowane w czasie Światowego Szczytu Społeczeństwa Informacyjnego, który odbył się w dwóch fazach. Pierwsza z nich miała miejsce w Genewie w terminie od 10 do 12 grudnia 2003 r., druga w Tunisie i trwała od 16 do 18 listopada 2005 r. Celem pierwszej fazy było wypracowanie jasnego stanowiska woli politycznej oraz podjęcie konkretnych kroków w celu ustanowienia fundamentów społeczeństwa informacyjnego dla wszystkich, odzwierciedlającego różnorodność interesów. Celem drugiej fazy było wcielenie w życie Planu Działań z Genewy (*Genewa Action Plan*), a także znalezienie

Komisja Europejska w odniesieniu do zarządzania internetem występowała na rzecz podejścia określanego skrótem COMPACT¹⁸⁹, zgodnie z którym internet jest przestrzenią odpowiedzialności obywatelskiej (ang. *civic responsibilities*), jednym niepodzielnym zasobem (ang. *one unfragmented resource*) zarządzanym w sposób oparty na porozumieniu zainteresowanych stron (ang. *multistakeholder approach*) w celu wspierania demokracji i praw człowieka (ang. *promote democracy and human rights*) na podstawie solidnej architektury technicznej (ang. *architecture*), która jest źródłem zaufania (ang. *confidence*) i sprzyja przejrzystości zarządzania (ang. *transparent governance*) zarówno bazową infrastrukturą internetu, jak i usługami wykonywanymi przy jej użyciu¹⁹⁰.

Podejście to wskazuje na próbę pogodzenia tendencji wolnościowych z koncepcjami zalecającymi uruchomienie mechanizmów kontrolnych i nadzorczych. Parlament Europejski w Rezolucji w sprawie zarządzania internetem potwierdził, że „uważa, że Internet jest globalnym publicznym dobrem, i że w związku z tym należy nim zarządzać we wspólnym interesie”¹⁹¹ oraz przyznał, że „Internet ma zasadnicze znaczenie dla praktycznej realizacji wolności słowa” oraz stał się niezbędnym narzędziem debaty politycznej, upowszechniania wiedzy, a „dostęp do Internetu jest uzależniony od korzystania z szeregu praw podstawowych i jednocześnie je gwarantuje, w tym między innymi poszanowanie życia prywatnego, ochronę danych, wolność wypowiedzi, słowa i zrzeszania się, wolność prasy, głoszenia poglądów politycznych i udziału w życiu politycznym”¹⁹².

rozwiązań i osiągnięcie porozumień w dziedzinie zarządzania internetem, mechanizmów finansowania oraz działań następczych i implementacji dokumentów z Genewy i Tunisu, w tym Rezolucji Zgromadzenia Ogólnego ONZ 56/183, World Summit on the Information Society, <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52014IR2448> (dostęp: 10.10.2024). Zob. Ł. Morawski, *Unia Europejska wobec...*, s. 112.

¹⁸⁹ Podejście COMPACT jest oparte na programie z Tunisu z 2005 r.

¹⁹⁰ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Polityka wobec internetu i zarządzanie internetem. Rola Europy w kształtowaniu przyszłości zarządzania internetem.

¹⁹¹ Rezolucja Parlamentu Europejskiego z dnia 15 czerwca 2010 r. w sprawie zarządzania Internetem: kolejne działania (2009/2229(INI)) lit. I pkt 1–3 (Dz.U. UE C z 2011 r., poz. 236).

¹⁹² Tamże.

W opinii Komitetu Regionów internet tworzy „globalną przestrzeń informacji”¹⁹³, a dostęp do niego stanowi „niezbywalne prawo obywatelskie”¹⁹⁴.

W ocenie KE „zarządzanie internetem powinno być zgodne z zapobiegającym wykluczeniu i przejrzystym modelem zarządzania opartym na porozumieniu zainteresowanych stron, z wyraźnie określonym zakresem odpowiedzialności”¹⁹⁵. Już w 2015 r. wyraźnie założono jednak, że model zarządzania internetem, jaki miałyby zostać przyjęty w UE, „nie może wykluczać interwencji regulacyjnej, podejmowanej z uwagi na cele leżące w interesie publicznym”¹⁹⁶.

Wśród celów usprawiedliwiających interwencję w sferę wolności i praw wskazano: „zapewnienie poszanowania praw człowieka, podstawowych wolności i wartości demokratycznych, jak również różnorodności językowej i kulturowej oraz opieki nad osobami wymagającymi szczególnej troski”¹⁹⁷. Wskazane cele wykraczają poza sformułowany w art. 10 ust. 2 EKPC katalog materialnoprawnych przesłanek usprawiedliwiających ingerencję. Różnica w sposobie określanie celów ingerencji ma charakter nie tylko ilościowy, lecz także jakościowy. Za usprawiedliwioną ingerencją w sferę wolności i praw realizowanych w internecie przemawiać ma bowiem także ochrona takich wartości, które albo nie zostały wymienione w art. 10 ust. 2 EKPC (różnorodności językowej i kulturowej oraz opieki nad osobami wymagającymi szczególnej troski), albo zostały ujęte w sposób bardzo szeroki (*largissimo sensu*¹⁹⁸), co pozwala na dużą swobodę interpretacji, a w konsekwencji nie gwarantuje

¹⁹³ Opinia Komitetu Regionów – Polityka wobec internetu i zarządzanie internetem, pkt 1 (Dz.U. UE C z 2015 r. Nr 19, s. 65).

¹⁹⁴ Tamże, pkt 8. W dokumencie zwrócono uwagę, że w niektórych państwach prawo dostępu do internetu zostało uznane za jedno z praw podstawowych. W 2009 r. trybunał konstytucyjny Francji uznał prawo do dostępu do internetu za prawo podstawowe. Podobna decyzja na poziomie konstytucyjnym zapadła w Grecji. Kolejne orzeczenia lub deklaracje polityczne przyjęto m.in. na Kostaryce, w Estonii, Finlandii, Hiszpanii, a nawet na szczęblu Narodów Zjednoczonych.

¹⁹⁵ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Polityka wobec internetu i zarządzanie internetem. Rola Europy w kształtowaniu przyszłości zarządzania internetem, pkt 9.

¹⁹⁶ Tamże, pkt 9.

¹⁹⁷ Tamże, pkt 9.

¹⁹⁸ W wykładni *largissimo sensu* wykładni poddawane są także zachowania pewnych podmiotów, w tym prawodawcy; zob. M. Zieliński, *Wykładnia prawa. Zasady. Reguły. Wskazówki*, Warszawa 2002, s. 59.

pewności prawa (chodzi o cele ujmowane jako: zapewnienie poszanowania praw człowieka, podstawowych wolności i wartości demokratycznych).

Rygory ingerencji w wolność wypowiedzi wypracowane na gruncie art. 10 EKPC i art. 11 KPP okazały się, w sferze cyfrowej, niewystarczające ze względu na specyfikę środowiska wirtualnego, a w szczególności faktycznie osiąganą pozycję przez bardzo duże platformy internetowe i władztwo dostawców niektórych usług pośrednich nad zasobami internetu. Próba lustrzanego zastosowania wolnościowej koncepcji swobody wypowiedzi w takim ujęciu, jakie było wypracowane przez ETPC, wymagała adaptacji i dostosowania do reguł rynku cyfrowego.

Koncepcja zarządzania internetem, a w konsekwencji także podejście do regulowania swobody wypowiedzi w internecie, zostały skonkretyzowane w strategii jednolitego rynku cyfrowego¹⁹⁹. Jednym z elementów konstrukcyjnych jednolitego rynku cyfrowego stało się – obok transgranicznego handlu elektronicznego, usług elektronicznych, dostarczania treści cyfrowych – także zwalczanie nielegalnych treści i mowy nienawiści w internecie. Parlament Europejski wezwał w 2015 r. Komisję Europejską, by „dokonała postępów w polityce i ramach prawnych dotyczących zwalczania cyberprzestępczości oraz nielegalnych treści i materiałów w internecie, w tym mowy nienawiści”²⁰⁰. Wezwanie do podjęcia aktywności w przedmiocie zwalczania nielegalnych treści stawiało przed KE zadanie polegające na zidentyfikowaniu i ustanowieniu mechanizmów ingerowania w swobodę komunikowania w internecie, a zatem także ingerowania w wolność wypowiedzi. Założono zatem, że dotychczasowe modele regulacyjne są nieadekwatne i mogą okazać się nieskuteczne wobec nadużywania wolności wypowiedzi w internecie.

W Rezolucji Parlamentu Europejskiego z dnia 19 stycznia 2016 r. pt. „W kierunku aktu o jednolitym rynku cyfrowym” odwołano się do klasycznego standardu wolności wypowiedzi wypracowanego na gruncie EKPC, otwierając

¹⁹⁹ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Strategia jednolitego rynku cyfrowego dla Europy, <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52015DC0192> (dostęp: 23.05.2024).

²⁰⁰ Rezolucja Parlamentu Europejskiego z dnia 19 stycznia 2016 r. w sprawie „W kierunku aktu o jednolitym rynku cyfrowym” (2015/2147(INI)), pkt 3.3.3 (Dz.U. UE C z 2018 r. Nr 11, s. 55), <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX%3A52016IP0237> (dostęp: 23.05.2024).

zarazem drogę do ustanowienia nowego modelu korzystania z wolności wypowiedzi, który, ze względu na specyfikę komunikowania w cyberprzestrzeni, dawał prawodawcy europejskiemu podstawę do modyfikowania konwencyjnego standardu wolności wypowiedzi w kierunku standardu bardziej wymagającego, a przez to bardziej restrykcyjnego²⁰¹.

Wskazano zatem, że zwalczanie nielegalnych treści powinno odbywać się „zgodnie z prawami podstawowymi określonymi w Karcie praw podstawowych Unii Europejskiej, a zwłaszcza z prawem do wolności słowa i swobodnego dostępu do informacji”, ale „także z zasadami konieczności, proporcjonalności, sprawiedliwości proceduralnej i praworządności” (pkt 88). Obok wypracowanych na gruncie art. 10 ust. 2 EKPC przesłanek usprawiedliwiających ingerencję w wolność wypowiedzi takich jak: wymóg wykazania konieczności ingerencji uzasadnionej potrzebą ochrony innych chronionych wartości (istnienie pilnej społecznej potrzeby) oraz wymogu zachowania proporcjonalności dodano nowe przesłanki, tj.: potrzebę zapewnienia sprawiedliwości proceduralnej oraz wymóg praworządności. Przesłanki te mają mieszany charakter, formalno-materialny, i stanowić mogą *de facto* nie tyle zaostrzenie rygorów testu szkodliwości, co jego złagodzenie. Pozostawiają bowiem w gestii organu nadzorczego zarówno ustalenie *in casu* ich treści, jak i decyzję o ich zastosowaniu. Osiągnięcie „sprawiedliwości proceduralnej” i „praworządności” uzyskuje zarazem prymat nad ochroną innych wartości, stanowiąc warunek konieczny ich ochrony.

Wskazano więc, że „by osiągnąć ten cel, należy:

1. zapewnić europejskim i krajowym służbom policyjnym i organom ścigania spójne i skuteczne narzędzia egzekwowania prawa;
2. zapewnić jasne wytyczne określające, jak postępować z nielegalnymi treściami internetowymi, w tym z mową nienawiści;
3. wspierać partnerstwa publiczno-prywatne i dialog między podmiotami publicznymi i prywatnymi, zgodnie z obowiązującymi przepisami UE;
4. doprecyzować rolę pośredników oraz platform internetowych w świetle Karty praw podstawowych Unii Europejskiej;

²⁰¹ J. Tackowska-Olszewska, *Racjonalizacja wolności prasy...*, s. 117.

5. dopilnować, by ustanowienie w ramach Europolu unijnej jednostki ds. zgłaszania podejrzanych treści w internecie (EU IRU) opierało się na odpowiedniej z punktu widzenia działalności tej jednostki podstawie prawnej;
6. zapewnić specjalne środki służące zwalczaniu wykorzystywania seksualnego dzieci w internecie oraz skuteczną współpracę między wszystkimi zainteresowanymi stronami w celu zagwarantowania praw i ochrony dzieciom korzystającym z internetu oraz sprzyjania inicjatywom, które dążą do tego, by internet stał się bezpieczny dla dzieci;
7. oraz współpracować z odnośnymi zainteresowanymi stronami na rzecz promowania kampanii edukacyjnych i podnoszących świadomość²⁰².

Realizacją zaleceń Parlamentu Europejskiego było przedłożenie przez KE wniosku w sprawie przyjęcia przez PE dwóch rozporządzeń cyfrowych tworzących tzw. pakiet cyfrowy, tj.: rozporządzenia w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (AUC)²⁰³ oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym (akt o rynkach cyfrowych)²⁰⁴. Rada Europejska w komunikacie wydanym w następstwie przyjęcia pakietu cyfrowego przyznała, że:

Akt o usługach cyfrowych uważa się za bezprecedensowy wśród regulacji cyfrowych. Żadne inne przepisy nie są tak ambitne, jeżeli chodzi o regulowanie platform i nadzoru w internecie przy zachowaniu podstawowych zasad rynku wewnętrznego²⁰⁵.

²⁰² Rezolucja Parlamentu Europejskiego z dnia 19 stycznia 2016 r. w sprawie „W kierunku aktu o jednolitym rynku cyfrowym” (2015/2147(INI)), (Dz.U. UE C z 2018 r. Nr 11, s. 55), pkt 3.3.3.

²⁰³ Rozporządzenie w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych) (Dz.U. UE L Nr 277, s. 1 z późn. zm.).

²⁰⁴ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828 (akt o rynkach cyfrowych) (Dz.U. UE L Nr 265, s. 1).

²⁰⁵ Komunikat Rady UE z dnia 4 października 2022 r. <https://www.consilium.europa.eu/pl/meetings/ecofin/2022/10/04/> (dostęp: 23.05.2024).

Przyjęcie AUC i ARC zostało poprzedzone zalegalizowaniem przez Parlament Europejski nowego rynku gospodarczego, jakim jest rynek danych osobowych, co nastąpiło w dwóch aktach prawnych: 1) rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych – dalej: RODO)²⁰⁶ oraz 2) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej²⁰⁷. Powyżej wskazane akty normatywne pozostają zarazem w funkcjonalnym związku z aktem w sprawie sztucznej inteligencji przyjętym w pierwszym czytaniu przez PE w dniu 13 marca 2024 r.²⁰⁸ oraz rozporządzeniem Parlamentu

²⁰⁶ X. Konarski zauważa, że zarówno RODO, jak i – częściowo – Akt w sprawie sztucznej inteligencji oparte są na tej samej podstawie prawnej ich przyjęcia, tj. art. 16 Traktatu o funkcjonowaniu Unii Europejskiej, stanowiącego o ochronie danych osobowych. Pozwala to na stwierdzenie, że RODO i AI Act należy traktować jako „tandem legislacji” chroniący dane osobowe (zob. X. Konarski, *Wzajemna relacja RODO i Aktu w sprawie sztucznej inteligencji – 10 najważniejszych informacji*, 9.04.2024, <https://www.traple.pl/wzajemna-relacja-rodo-i-aktu-w-sprawie-sztucznej-inteligencji-10-najwazniejszych-informacji/> (dostęp: 10.10.2024)).

²⁰⁷ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej (Dz.U. UE L Nr 303, s. 59). W art. 1 rozporządzenia wskazano, że „Celem niniejszego rozporządzenia jest zapewnienie na terytorium Unii swobodnego przepływu danych innych niż dane osobowe poprzez ustanowienie przepisów odnoszących się do wymogów dotyczących lokalizacji danych, dostępności danych dla właściwych organów i przenoszenia danych przez użytkowników profesjonalnych”. W motywach rozporządzenia wskazano, że „Technologie informacyjno-komunikacyjne nie stanowią już specyficznego sektora, lecz są podstawą wszystkich nowoczesnych, innowacyjnych systemów gospodarczych i społeczeństw. Dane elektroniczne znajdują się w centrum tych systemów i mogą przynieść ogromne korzyści, jeżeli podda się je analizie lub połączy z usługami i produktami. Jednocześnie szybki rozwój gospodarki opartej na danych oraz nowo powstające technologie, takie jak sztuczna inteligencja, produkty i usługi internetu rzeczy, systemy autonomiczne i sieci 5G, stwarzają nowe wyzwania prawne dotyczące kwestii dostępu do danych i ich ponownego wykorzystywania” (motyw 1).

²⁰⁸ Akt w sprawie sztucznej inteligencji Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 13 marca 2024 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze Unii, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_PL.html (dostęp: 22.03.2024).

Europejskiego i Rady (UE) 2022/868 z dnia 30 maja 2022 r. w sprawie europejskiego zarządzania danymi²⁰⁹.

Wskazane powyżej akty prawne stworzyły normatywne fundamenty dla rozwoju rynku cyfrowego, jednocześnie pozwalając na zarządzanie zachodzącymi na tym rynku procesami. Zważywszy, że warunkiem nawiązania, utrzymania lub zmiany stosunków na rynku usług cyfrowych jest skuteczna komunikacja i transfer danych, ustanowione we wskazanych powyżej aktach prawnych narzędzia, instrumenty i instytucje oddziałują nie tylko w sferze stosunków gospodarczych, ale ingerują w sferę wolności i praw stron tych stosunków, w szczególności w sferę wolności wypowiedzi.

Model zarządzania internetem²¹⁰ przewiduje zmianę zasad reagowania na nadużycia wolności wypowiedzi poprzez legitymizowanie środków prewencyjnych (*ex ante*), a także poprzez uzupełnienie przesłanek legalizujących ingerencję w wolność wypowiedzi. UE przyjęła koncepcję „współzarządzania” internetem, co w konsekwencji skłoniło ją do zaakceptowania aktywności kontrolnej (monitoring, filtrowanie) realizowanej przez podmioty prywatne i doprowadziło do udzielenia im uprawnień w zakresie stosowania instrumentów zbliżonych do środków zabezpieczających (prewencyjne zawieszanie świadczenia usługi) w celu uzyskania skutku nadzorczego polegającego na zwalczaniu nielegalnych treści (blokowanie dostępu, usuwanie).

B. Transpozycja klasycznego standardu na jednolitym rynku cyfrowym

Potrzeba transpozycji konwencyjnego standardu wolności wypowiedzi i jego dostosowania (dopasowania) do warunków panujących w cyberprzestrzeni została zauważona przez Europejski Trybunał Praw Człowieka²¹¹,

²⁰⁹ Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie europejskiego zarządzania danymi (akt w sprawie zarządzania danymi), <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52020PC0767> (dostęp: 23.05.2024).

²¹⁰ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Polityka wobec internetu i zarządzanie internetem. Rola Europy w kształtowaniu przyszłości zarządzania internetem.

²¹¹ Trybunał przyjmował już w stosunku do publikacji internetowych, iż dana osobom możliwość wyrażenia opinii w internecie stanowi bezprecedensowe narzędzie

który w 2021 r. explicite stwierdził, że „internet jest narzędziem komunikacji i przekazu informacji szczególnie odróżniającym się od mediów drukowanych, zwłaszcza jeśli chodzi o możliwości przechowywania i przesyłania informacji. Elektroniczna sieć obsługująca miliardy użytkowników na całym świecie nie jest i potencjalnie nigdy nie będzie podlegała tym samym regulacjom i zasadom kontroli. Ryzyko wyrządzenia szkody przez treści i przekazy zamieszczane w Internecie przy wykonywaniu i korzystaniu przez jednostki z wolności i praw człowieka, zwłaszcza prawa do poszanowania życia prywatnego – jest z całą pewnością wyższe niż ryzyko pochodzące ze strony prasy. Dlatego też reguły rządzące powielaniem materiałów pochodzących z mediów drukowanych i Internetu mogą się między sobą różnić. Te ostatnie niewątpliwie muszą zostać przystosowane do specyficznych wymogów technologii w celu zapewnienia ochrony odpowiednich praw i wolności”²¹².

Sposób rozłożenia ciężaru obowiązków i włożenie ich na podmioty rynku cyfrowego wymienione w AUC i ARC, w tym dostawców usług pośrednich, a w szczególności tzw. strażników dostępu, a także ustanowienie mechanizmów ułatwiających uchylenie się od odpowiedzialności za wkroczenie w prawa i wolności innych osób w związku z wykonywaniem powierzonych obowiązków zostało podporządkowane realizacji celów gospodarczych

wykonywania wolności wyrażania opinii. Dzięki swej dostępności oraz możliwościom przechowywania i rozpowszechniania dużych ilości danych, strony internetowe przyczyniają się znacznie do polepszenia dostępu opinii publicznej do aktualności oraz, co do zasady, usprawniają przekazywanie informacji. Tym samym internet stał się w dzisiejszych czasach jednym z podstawowych środków wykonywania wolności wypowiedzi, jako że zapewnia podstawowe narzędzia udziału w czynnościach i dyskusjach dotyczących kwestii politycznych i debat prowadzonych w interesie powszechnym. Mimo to, zaletom tego medium towarzyszy określona liczba niebezpieczeństw. Wypowiedzi jednoznacznie bezprawne, zwłaszcza o charakterze zniesławiającym, nienawistnym lub nawołującym do przemocy, mogą być rozpowszechniane jak nigdy wcześniej na cały świat, w kilka sekund, i czasami pozostają online przez długi czas. Jasne jest jednakże, iż wypowiedź opublikowana online dla małej liczby czytelników nie może z pewnością mieć takiego samego zasięgu i oddziaływania jak wypowiedzi publikowane na stronach internetowych otwartych dla szerokiej publiczności lub często odwiedzanych. Tym samym dla oceny potencjalnego oddziaływania publikacji online zasadnicze znaczenie ma określenie jej zasięgu oraz oddziaływania na ludność (zob. Wyrok ETPC z dnia 15 czerwca 2021 r. w sprawie Melike przeciwko Turcji, skarga nr 35786/19.

²¹² Wyrok ETPC w sprawie Pravoye Delo i Shtekel przeciwko Ukrainie, skarga nr 33014/05, § 63 (wyjątki).

i politycznych UE, przy czym najważniejszy z nich stanowiła budowa jednolitego rynku cyfrowego²¹³.

W sferze jednolitego rynku cyfrowego, którego budowanie, rozwijanie i utrzymanie stanowi jeden z filarów europejskiej gospodarki²¹⁴, a zatem także jeden z kluczowych elementów realizowanej przez organy UE polityki²¹⁵, ustawodawca europejski modyfikuje standardy zachowania uczestników tego rynku i wpływa na kształt stosunków prawnych, których przedmiotem jest świadczenie dostępnych na tym rynku usług (usługi cyfrowe). Ustawodawca europejski realizuje powyższe cele poprzez odpowiednie stanowienie i stosowanie prawa, w szczególności inicjując tworzenie nowych regulacji

²¹³ Ustawodawca za pomocą prawa realizuje bowiem cele polityczne, ekonomiczne i społeczne. Cele te mogą być modyfikowane, a w konsekwencji modyfikowane są zakresy obowiązków i praw uprzednio przyznane adresatom norm prawnych.

²¹⁴ Szacuje się, że wielkość gospodarki cyfrowej stanowi 4,5–15,5% światowego PKB w 2019 r. z tendencją wzrostową (zob. ARC).

²¹⁵ Budowanie jednolitego rynku cyfrowego i działania na rzecz transformacji cyfrowej ogłosił w swoim programie politycznym Przewodniczący PE Jean-Claude Juncker (zob. *Nowy początek dla Europy: Mój program na rzecz zatrudnienia, wzrostu, sprawiedliwości oraz zmian demokratycznych*, 15.07.2014, https://ec.europa.eu/commission/presscorner/detail/pl/SPEECH_14_546 dostęp: 10.10.2024). J.C. Juncker powiedział wówczas: „Tworząc połączony, jednolity rynek cyfrowy, w trakcie kadencji następnej Komisji możemy zapewnić w Europie dodatkowy wzrost o wartości nawet 250 mld EUR, dzięki czemu powstanie kilkaset tysięcy nowych miejsc pracy, zwłaszcza dla młodych osób, a także dynamiczne społeczeństwo oparte na wiedzy. Aby osiągnąć ten cel, zamierzam w ciągu pierwszych sześciu miesięcy mojego mandatu przedsięwziąć ambitne działania legislacyjne w kierunku stworzenia połączonego jednolitego rynku cyfrowego, szczególnie przez szybkie zakończenie negocjacji w sprawie wspólnych europejskich przepisów o ochronie danych; przez ambitniejsze podejście do trwającej reformy przepisów w obszarze telekomunikacji; przez unowocześnienie przepisów o prawie autorskim w świetle rewolucji cyfrowej i zmian w zachowaniu konsumenta; a także przez unowocześnienie i uproszczenie zasad ochrony konsumentów” (zob. tamże). Parlament Europejski wezwał państwa członkowskie i Komisję do zaangażowania się w rozwój jednolitego rynku cyfrowego jako nadrzędnego priorytetu politycznego oraz do przedstawienia całościowego podejścia i ambitnej strategii obejmującej zarówno inicjatywy legislacyjne, jak i polityczne w celu uwzględnienia nowych i nadchodzących zmian, co pozwoli na urzeczywistnienie jednolitego rynku cyfrowego – Rezolucja Parlamentu Europejskiego z dnia 4 lipca 2013 r. w sprawie stworzenia jednolitego rynku cyfrowego (Dz.U. UE C z 2016 r. Nr 75, s. 120). Ustanowienie jednolitego rynku cyfrowego zostało wskazywane jako cel polityczny UE przez Przewodniczącą KE Ursulę von der Leyen w orędziu na 2021 r.; zob. *Wyznaczenie kursu na nadchodzący rok. Orędzie o stanie Unii w 2020 r.*, 4.08.2022, Komisja Europejska, https://state-of-the-union.ec.europa.eu/state-union-2020_pl (dostęp: 24.05.2024).

lub zmieniając już istniejące²¹⁶. Prawo, rozumiane jako system norm regulujących pożądane zachowania²¹⁷, może formułować wobec podmiotów operujących na rynku usług cyfrowych wysokie wymagania albo uregulować ich status w sposób elastyczny. Zagadnieniem natury politycznej jest bowiem rozstrzygnięcie na etapie projektowania norm i instytucji prawnych, ustalenie rozkładu praw i ciężaru obowiązków odnoszonych do uczestników rynku usług cyfrowych.

O ile poza sferą cyfrową nie są konieczne specjalne narzędzia i technologie do wymiany informacji i komunikowania – ta bowiem przestrzeń komunikowania (realna) nie wymaga pośrednika – o tyle w internecie nie jest możliwe przekazywanie ani odbieranie treści z pominięciem instrumentów, technik i technologii, które stanowią przedmiot świadczenia „nowej” usługi ujmowanej w aktach normatywnych jako „usługa społeczeństwa informacyjnego”²¹⁸.

²¹⁶ W odniesieniu do realizacji celu, jakim było stworzenie jednolitego rynku cyfrowego, Parlament Europejski wezwał Komisję do podjęcia niezbędnych środków służących zachęcaniu do rozwoju treści cyfrowych, które byłyby dostępne na całym jednolitym rynku cyfrowym. Podkreślił, że założeniem zmienionych ram dotyczących prawa własności intelektualnej powinno być sprzyjanie innowacyjności, nowym modelom usług oraz tworzeniu wspólnych treści przez użytkowników, aby wspierać rozwój konkurencyjnego unijnego rynku ICT, zapewniając jednocześnie posiadaczom praw ochronę i możliwość uzyskania odpowiedniego wynagrodzenia. Rezolucja Parlamentu Europejskiego z dnia 4 lipca 2013 r. w sprawie stworzenia jednolitego rynku cyfrowego (Dz.U. UE C z 2016 r. Nr 75, s. 120, pkt 44).

²¹⁷ Prawo to zespół, całokształt ogólnych norm postępowania ustanowionych lub uznanych przez państwo, regulujących zachowania doniesłe z punktu widzenia państwa, których przestrzeganie jest zagwarantowane przez państwo (zob. A. Łopatka, *Prawoznawstwo*, Warszawa 2006, s. 105, podobnie J. Oniszczyk, *Prawo, jego tworzenie i systematyka. Wybrane zagadnienia*, Warszawa 1999, s. 12–13).

²¹⁸ W zakresie sposobu definiowania pojęcia „usługa społeczeństwa informacyjnego” następuje we wszystkich aktach normatywnych UE odesłanie do art. 1 ust. 2 dyrektywy 98/48/WE Parlamentu Europejskiego i Rady z dnia 20 lipca 1998 r. zmieniająca dyrektywę 98/34/WE ustanawiającą procedurę udzielania informacji w zakresie norm i przepisów technicznych (Dz.U. UE L Nr 217, s. 18 z późn. zm.). Termin „usługa społeczeństwa informacyjnego” obejmuje każdą usługę normalnie świadczoną za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług. Do celów niniejszej definicji: 1) „na odległość” oznacza usługę świadczoną bez równoczesnej obecności stron, 2) „drogą elektroniczną” oznacza, iż usługa jest przesyłana pierwotnie i otrzymywana w miejscu przeznaczenia za pomocą sprzętu elektronicznego do przetwarzania (włącznie z kompresją cyfrową) oraz przechowywania danych, i która jest całkowicie przesyłana, kierowana i otrzymywana za pomocą kabla, odbiornika radiowego, środków optycznych lub innych środków elektromagnetycznych, 3) „na indywidualne

Pojęcie usług²¹⁹, w szerokim rozumieniu, zostało zdefiniowane w art. 57 TFUE²²⁰ i oznacza „świadczenia wykonywane zwykle za wynagrodzeniem w zakresie, w jakim nie są one objęte postanowieniami o swobodnym przepływie towarów, kapitału i osób”. Zawarta w prawie pierwotnym definicja usług ma charakter negatywny. Wskazano w niej bowiem, że pojęciem usługi nie należy obejmować świadczeń, do których nie znajdują zastosowania przepisy traktatowe dotyczące wymiany towarów, przepływu kapitału i osób. Taki sposób definiowania pojęcia usługi kreuje domniemanie pozwalające przyjąć, że każde świadczenie niezwiązane z przepływem towarów, kapitału lub osób należy kwalifikować jako usługę. Usługą będą zatem wszelkie czynności wykonywane za wynagrodzeniem, które służą lub towarzyszą wymianie towarów i swobodzie przepływu kapitału i osób, w tym usługi tzw. pośredników internetowych świadczących usługi dostępu do internetu, a także usługi hostingu lub usługi dostawców platform przechowujących dane²²¹. Opis działalności polegającej na dostarczaniu usług społeczeństwa informacyjnego na jednolitym rynku cyfrowym został zawarty w szczególności w motywie 18 AUC, gdzie wskazano, że usługi społeczeństwa informacyjnego:

obejmują szeroki zakres rodzajów działalności gospodarczej prowadzonych w trybie online; takie rodzaje działalności mogą w szczególności polegać na sprzedaży towarów online; nie zaliczają się jednak do nich rodzaje

żądanie odbiorcy usług” oznacza, że usługa świadczona jest poprzez przesyłanie danych na indywidualne żądanie; art. 1 ust. 2 dyrektywy 98/48/WE Parlamentu Europejskiego i Rady z dnia 20 lipca 1998 r. zmieniającej dyrektywę 98/34/WE ustanawiającą procedurę udzielania informacji w zakresie norm i przepisów technicznych (Dz.U. UE L Nr 217, s. 18 z późn. zm.).

²¹⁹ Z rozwojem sektora usług powiązано oczekiwanie szybkiego wzrostu gospodarczego w całej UE, wskazując, że usługi są sektorem o kluczowym znaczeniu dla ożywienia gospodarki w Europie. Sektor ten zapewnia 70% wszystkich miejsc pracy oraz taki sam odsetek tworzenia miejsc pracy w ujęciu netto na jednolitym rynku (zob. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: W kierunku Aktu o jednolitym rynku. W stronę społecznej gospodarki rynkowej o wysokiej konkurencyjności. 50 propozycji na rzecz wspólnej poprawy rynku pracy, przedsiębiorczości i wymiany, s. 10, <https://eur-lex.europa.eu/legal-content/PL/TXT/?qid=1534167760484&uri=CELEX:52010DC0608> (dostęp: 22.03.2024).

²²⁰ Traktat ustanawiający Europejską Wspólnotę Gospodarczą (Dz.U. z 2004 r. Nr 90, poz. 864/2 z późn. zm.) – dalej jako TFUE.

²²¹ J. Taczowska-Olszewska, K. Chałubińska-Jentkiewicz, *Ustawa o świadczeniu usług drogą elektroniczną. Komentarz*, Warszawa 2019, s. 59.

działalności takie jak dostawa towarów jako taka lub świadczenie usług offline; [...] działania, które ze względu na swój charakter nie mogą być wykonane na odległość lub drogą elektroniczną, takie jak ustawowa kontrola ksiąg rachunkowych lub konsultacja medyczna wymagająca fizycznego badania pacjenta, nie są usługami społeczeństwa informacyjnego.

Rola dostawców usług społeczeństwa informacyjnego polega w pierwszej kolejności na zapewnieniu dostępu do sieci teleinformatycznej (ang. *access provider*) a następnie na umożliwieniu wprowadzania i przechowywania treści (hosting) oraz na zapewnieniu dostępu do treści poprzez ich transmisję od dostawcy usługi do jej odbiorcy (adresata) (ang. *mere conduit* – zwykły przekaz).

Zakres wpływu dostawców usług jest zatem wypadkową wskazanych powyżej trzech zmiennych, które zostały przez ustawodawcę europejskiego wykorzystane jako punkty odniesienia i kryteria regulacyjne. Zasady ponoszenia odpowiedzialności prawnej dostawców usług określone są, co do fundamentów, przez dwa akty normatywne, tj. dyrektywę 2000/31 (o handlu elektronicznym) oraz akt o usługach cyfrowych. W dalszej kolejności, uzupełniając, prawa i obowiązki użytkowników internetu, w tym interesy twórcze autorów treści cyfrowych oraz obowiązki bardzo dużych platform internetowych i bardzo dużych wyszukiwarek, normują akt o rynkach cyfrowych, a także rozporządzenie 2019/790 w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym. Nadal pewne znaczenie posiadają regulacje sektorowe²²².

Rynek usług cyfrowych, w szczególności rynek treści cyfrowych jako rynek transgraniczny, stanowi sferę objętą prawną regulacją UE. W dokumentach Komisji Europejskiej i Parlamentu wskazuje się na art. 4 ust. 2 lit. a TFUE

²²² M.in.: dyrektywa Parlamentu Europejskiego i Rady 2010/13/UE z dnia 10 marca 2010 r. w sprawie koordynacji niektórych przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich dotyczących świadczenia audiowizualnych usług medialnych (dyrektywa o audiowizualnych usługach medialnych), (Dz.U. L Nr 95, s. 1 z późn. zm.); rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym, (Dz.U. L Nr 172, s. 79); rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1148 z dnia 20 czerwca 2019 r. w sprawie wprowadzania do obrotu i stosowania prekursorów materiałów wybuchowych, zmieniające rozporządzenie (WE) nr 1907/2006 i uchylające rozporządzenie (UE) nr 98/2013 (Dz.U. L Nr 186, s. 1 z późn. zm.).

w zw. z art. 26, 27, 114 i 115 TFUE jako podstawę prawną i źródło kompetencji organów UE uprawniających je do kształtowania zakresu praw i obowiązków podmiotów operujących na rynku cyfrowym.

Zgodnie z art. 4 ust. 2 lit. a TFUE Unia dzieli z państwami członkowskimi kompetencje w dziedzinie rynku wewnętrznego. W myśl art. 26 TFUE Unia przyjmuje środki w celu ustanowienia lub zapewnienia funkcjonowania rynku wewnętrznego zgodnie z odpowiednimi postanowieniami Traktatów (art. 26 ust. 1). Rynek wewnętrzny obejmuje obszar bez granic wewnętrznych, w którym jest zapewniony swobodny przepływ towarów, osób, usług i kapitału, zgodnie z postanowieniami Traktatów (art. 26 ust. 2). Rada na wniosek Komisji ustala wytyczne i warunki niezbędne do zapewnienia zrównoważonego postępu we wszystkich odpowiednich sektorach (art. 26 ust. 3). W art. 27 TFUE zastrzeżono, że podczas opracowywania propozycji zmierzających do osiągnięcia celów wymienionych w art. 26 Komisja uwzględnia zakres wysiłku, jaki będą musiały podjąć niektóre gospodarki o zróżnicowanym rozwoju w celu ustanowienia rynku wewnętrznego, i może proponować odpowiednie przepisy.

W celu ustanowienia i zapewnienia funkcjonowania rynku wewnętrznego Parlament Europejski i Rada są upoważnione, na podstawie art. 114 i 115 TFUE, stanowiąc zgodnie ze zwykłą procedurą ustawodawczą i po konsultacji z Komitetem Ekonomiczno-Społecznym, do przyjmowania środków harmonizujących zapewniających zbliżenie przepisów ustawowych, wykonawczych i administracyjnych. Wskazuje się, że art. 114 TFUE stanowi kolejną ogólną podstawę prawną dla wprowadzania harmonizacji²²³. Przepisy traktatu pozwalające albo na skoordynowanie (harmonizacja minimalna²²⁴), albo zbliżenie (harmonizacja częściowa) czy wreszcie zunifikowanie przepisów krajowych (harmonizacja maksymalna, pełna) umożliwiają tzw. integrację

²²³ K. Kowalik-Bańczyk, P. Dąbrowska-Kłosińska, *Komentarz do art. 14 TFUE*, [w:] *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz. Tom II (art. 90–222)*, M. Szwarc-Kuczer (red.), A. Wróbel (red. nauk.), Warszawa 2012, art. 114.

²²⁴ P.P. Polański wskazuje na ewolucję w zakresie harmonizacji prawa europejskiego w dziedzinie handlu elektronicznego (zob. P.P. Polański, *Europejskie prawo handlu elektronicznego. Mechanizmy regulacji usług społeczeństwa informacyjnego*, Warszawa 2014, s. 248–249). Autor wskazuje, że ustawodawca europejski objął harmonizacją nowe obszary regulacji, posługując się tym samym metodą harmonizacji maksymalnej już na gruncie dyrektywy 2000/31 o handlu elektronicznym (tamże, s. 304 i n.).

pozytywną. W doktrynie dokonuje się rozróżnienia pomiędzy koordynacją, harmonizacją i unifikacją²²⁵. Metody integracji pozytywnej są, co do zasady, zróżnicowane ze względu na intensywność ingerencji w krajowe porządki prawne, przy czym najdalej idącą metodą jest unifikacja, która polega na zastąpieniu przepisów krajowych przepisami unijnymi²²⁶. Najczęściej jako instrument unifikacji wykorzystywane są rozporządzenia, przede wszystkim w dziedzinach, w których UE ma wyłączną kompetencję prawodawczą²²⁷.

Jednolity rynek cyfrowy jest definiowany w dokumentach UE jako element (część) rynku wewnętrznego. Pojęcie rynku wewnętrznego zostało wprowadzone do prawa pierwotnego przez Jednolity akt europejski²²⁸ z 1986 r.

²²⁵ K. Kowalik-Bańczyk dokonując analizy zakresów tych terminów, odwołuje się w szczególności do wyroku TS w sprawie Pietro Pinna przeciwko Caisse d'allocations familiales de la Savoie (Wyrok TS z dnia 15 stycznia 1986 r. w sprawie Pietro Pinna przeciwko Caisse d'allocations familiales de la Savoie, sprawa 41/84, nr 1, poz. 1). Jak dowodzi Autorka, Trybunał wyraźnie określił, że jeżeli instytucje unijne nie są upoważnione do prowadzenia harmonizacji prawa państw członkowskich, muszą poprzestać na tym, co jest im dozwolone przez pierwotne prawo unijne, czyli w tym przypadku na koordynacji. Pewnym podtypem koordynacji jest tzw. otwarta metoda koordynacji (ang. *open method of coordination*), którą stosuje się wówczas, gdy nie jest pożądane lub możliwe przeprowadzenie harmonizacji, np. w sytuacji, gdy brak kompetencji prawodawczej po stronie Unii (zob. P. Dąbrowska, *Koncepcja „nowego rządzenia” w prawie Unii Europejskiej a Konstytucja dla Europy*, [w:] *Konstytucja dla Europy. Przyszły fundament Unii Europejskiej*, S. Dudzik (red.), Kraków 2005, s. 202). Przeciwno uznawaniu harmonizacji i koordynacji za synonimy przemawia fakt wyraźnego wykluczenia w niektórych przepisach TFUE harmonizacji, podczas gdy koordynacja jest dopuszczalna (zob. K. Kowalik-Bańczyk, P. Dąbrowska-Kłosińska, [w:] *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz. Tom II (art. 90–222)*, M. Szwarc-Kuczer (red.), A. Wróbel (red. nauk.), Warszawa 2012, art. 114).

²²⁶ K. Kowalik-Bańczyk, P. Dąbrowska-Kłosińska, [w:] *Traktat o...*, M. Szwarc-Kuczer (red.), A. Wróbel (red. nauk.), art. 114.

²²⁷ Tamże.

²²⁸ Jednolity akt europejski (dalej: JAE), <https://www.europarl.europa.eu/about-parliament/files/in-the-past/ep-and-treaties/single-european-act/en-resolution-on-the-single-european-act-19861211.pdf> (dostęp: 22.03.2024). Wskazuje się, że przyjęcie JAE poprzedzono wydaniem w 1985 r. „Białej księgi o rynku wewnętrznym” (Completing The Internal Market: White Paper from The Commission to The European Council), komunikatu KE zawierającego szczegółowy program działań prawodawczych koniecznych do osiągnięcia rynku wewnętrznego. Jednak w deklaracji załączonej do JAE dotyczącej art. 7a (następnie art. 14 TWE, ob. art. 26 TFUE) państwa członkowskie doprecyzowywały, że data 31 grudnia 1992 r. nie miała powodować automatycznych skutków prawnych i pozostawała jedynie deklaracją o charakterze politycznym (zob. K. Kowalik-Bańczyk, P. Dąbrowska-Kłosińska, [w:] *Traktat o...*, M. Szwarc-Kuczer (red.), A. Wróbel (red. nauk.), art. 114). Terminem, którym operowano we wcześniejszych dokumentach UE, było pojęcie rynku wspólnego. Ideą wspólnego rynku, stworzonego na mocy traktatu

do Traktatu ustanawiającego Europejską Wspólnotę Gospodarczą (EWG). Zgodnie z nim włączono cel polegający na utworzeniu rynku wewnętrznego, który zdefiniowano jako „obszar bez granic wewnętrznych, w którym jest zapewniony swobodny przepływ towarów, osób, usług i kapitału”²²⁹.

Ustanowienie rynku wewnętrznego jest jednym z celów działania UE, co wynika wprost z treści art. 3 ust. 3 TUE²³⁰. Przepis ten jest bardzo rozbudowany, co zachęca do jego szerokiej interpretacji²³¹. Z celem, jakim jest ustanowienie rynku wewnętrznego, powiązane są, jak się wskazuje w doktrynie, cele szczegółowe, w tym także zwalczanie wykluczenia społecznego i dyskryminacji (art. 34 KPP, art. 9 i 18 TFUE) oraz równość kobiet i mężczyzn, a także wsparcie sprawiedliwości i ochrony socjalnej czy zapewnienie solidarności między pokoleniami²³².

Centralnym elementem definicji rynku wewnętrznego, pomimo że nie wynika to wprost z treści art. 3 ust. 3 TUE, uczyniono, począwszy od 2010 r., pojęcie jego jednolitości. W sprawozdaniu „Nowa strategia na rzecz jednolitego rynku” z dnia 9 maja 2010 r. zauważono, że „proces integracji nie jest procesem nieodwracalnym oraz że dalsze istnienie rynku wewnętrznego nie

rymskiego z 1958 r., było zniesienie barier handlowych między państwami członkowskimi, aby zwiększyć dobrobyt gospodarczy i przyczynić się do „coraz ściślejszego związku między narodami Europy”; zob. *Rynek wewnętrzny: zasady ogólne*, 05.2024, Noty tematyczne o Unii Europejskiej, <https://www.europarl.europa.eu/factsheets/pl/sheet/33/rynek-wewnetrzny-zasady-ogolne> (dostęp: 24.05.2024).

²²⁹ Art. 7a JAE.

²³⁰ Traktat o Unii Europejskiej (Dz.U. z 2004 r. Nr 90, poz. 864/30 z późn. zm.).

²³¹ Art. 3 ust. 3 TUE ma następujące brzmienie: „Unia ustanawia rynek wewnętrzny. Działa na rzecz trwałego rozwoju Europy, którego podstawą jest zrównoważony wzrost gospodarczy oraz stabilność cen, społeczna gospodarka rynkowa o wysokiej konkurencyjności zmierzająca do pełnego zatrudnienia i postępu społecznego oraz wysoki poziom ochrony i poprawy jakości środowiska. Wspiera postęp naukowo-techniczny. Zwalcza wykluczenie społeczne i dyskryminację oraz wspiera sprawiedliwość i ochronę socjalną, równość kobiet i mężczyzn, solidarność między pokoleniami i ochronę praw dziecka. Wspiera spójność gospodarczą, społeczną i terytorialną oraz solidarność między Państwami Członkowskimi. Szanuje swoją bogatą różnorodność kulturową i językową oraz czuwa nad ochroną i rozwojem dziedzictwa kulturowego Europy”.

²³² Zwraca się uwagę, że nie jest jasne, „jakimi środkami UE ma osiągnąć cele polegające na wsparciu sprawiedliwości i ochrony socjalnej czy zapewnieniu solidarności między pokoleniami. Dla tych celów trudno odnaleźć szczegółowe przepisy w TFUE” (zob. A. Grzelak, *Komentarz do art. 6 TFUE*, [w:] *Traktat o Unii Europejskiej. Komentarz*, R. Grzeszczak, D. Kornobis-Romanowska (red. nauk.), Warszawa 2023, art. 3).

powinno być uważane za pewnik”²³³. Wzmocnieniu i utrzymaniu procesów integracyjnych służyć miało zapewnienie jednolitości rynku wewnętrznego we wszystkich jego sferach, w tym poprzez „wykorzystanie potencjału wzrostu i bogatej oferty towarów i usług, które może dostarczać rynek cyfrowy”²³⁴. Zapewnienie jednolitości obejmować winno, zgodnie z przyjętą strategią, zarówno sfery przepływu usług i ich transgraniczności, jak i likwidowania barier fiskalnych, a także budowania europejskiej tożsamości. W Strategii na rzecz jednolitego rynku wskazano, że „Jednolity rynek uczestniczy również w tworzeniu tożsamości każdego obywatela”²³⁵. Podkreślono, że w art. 9 TFUE została „Zapisana horyzontalna klauzula społeczna, która pozwala na dokonanie oceny znaczenia wszystkich środków o charakterze politycznym ze względu na ich społeczne konsekwencje, musi być stosowana i towarzyszyć każdego rodzaju wspólnej refleksji”²³⁶. Model ten został oparty na idei głoszącej, że do wzrostu gospodarczego należy dochodzić poprzez rynek realizujący cele społeczne²³⁷.

Zaproponowane w 2010 r., a następnie rozwijane podejście²³⁸ oparte na przesłance *sine qua non* budowy jednolitego rynku, będącej odejściem

²³³ Sprawozdanie Mario Monti dla Przewodniczącego Komisji Europejskiej: „Nowa strategia na rzecz jednolitego rynku” z dnia 9 maja 2010 r., Bruksela 2010, s. 9 cyt. za: Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: W kierunku Aktu o jednolitym rynku. W stronę społecznej gospodarki rynkowej o wysokiej konkurencyjności. 50 propozycji na rzecz wspólnej poprawy rynku pracy, przedsiębiorczości i wymiany.

²³⁴ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: W kierunku Aktu o jednolitym rynku. W stronę społecznej gospodarki rynkowej o wysokiej konkurencyjności. 50 propozycji na rzecz wspólnej poprawy rynku pracy, przedsiębiorczości i wymiany, s. 9.

²³⁵ Tamże, s. 21.

²³⁶ Tamże, s. 21.

²³⁷ K. Szczerski zauważa, że zaproponowany model rozwoju gospodarczego oparty o budowanie jednolitego rynku w szerokim rozumieniu stanowi „kompletny system, łącząc w nim solidarność, odpowiedzialność i konkurencyjność. [...] Co więcej, porozumienie dotyczące modelu uzależnione jest od utrzymania równowagi między jego wymiarem społecznym a rynkowym” (zob. K. Szczerski, *Skrępowani serdecznym uściskiem – społeczna gospodarka rynkowa o wysokiej konkurencyjności. Europejskie konteksty gospodarki społecznej*, Ośrodek Myśli Politycznej, <http://www.omp.org.pl/artukul.php?artukul=205> (dostęp: 22.03.2024)).

²³⁸ Podejście to było kontynuowane w kolejnych krokach podejmowanych przez KE i PE. W październiku 2012 r. Komisja, aby dalej rozwijać jednolity rynek i spożytkować jego niewykorzystany potencjał jako motor wzrostu, przedstawiła „Akt o jednolitym

od koncepcji rynku zinstytucjonalizowanego, charakteryzującego się tym, że operują na nim przede wszystkim podmioty gospodarcze na rzecz koncepcji społecznej gospodarki rynkowej, w której obywatele, jednostki są równie ważnym uczestnikiem tego rynku jak przedsiębiorcy, co oznacza przeniesienie uwagi z aspektów gospodarczych na aspekty tożsamościowe i społeczne, stało się dla organów UE źródłem upoważnienia do regulowania jednolitego rynku w aspekcie praw podstawowych. Środowisko cyfrowe jest zarazem, co zostało bardzo szybko zauważone i wykorzystane początkowo przez pośredników internetowych, podatne na regulacje o charakterze kształtującym prawa i wolności.

Jednolity rynek cyfrowy jest definiowany w sposób analogiczny do pojęcia rynku wewnętrznego z tą różnicą, że rynek cyfrowy, ze względu na jego specyfikę, stanowi obszar działalności gospodarczej, w obrębie którego możliwe jest świadczenie wyłącznie usług i nie obejmuje on wymiany towarów ani przepływu osób. Jednolity rynek cyfrowy oznacza „przestrzeń, w której zapewniony jest swobodny przepływ towarów, osób, usług i kapitału, a obywatele i przedsiębiorstwa mogą bez przeszkód i na zasadach uczciwej

rynku II” (Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Akt o jednolitym rynku II. Razem na rzecz nowego wzrostu gospodarczego, <https://eur-lex.europa.eu/legal-content/PL/TXT/?qid=1534172039517&uri=CELEX:52012DC0573> (dostęp: 24.05.2024)). W akcie tym określono 12 działań podstawowych, które miały być szybko podjęte przez instytucje UE. Koncentrowały się one na czterech głównych czynnikach: 1) zintegrowanych sieciach, 2) transgranicznej mobilności obywateli i przedsiębiorstw, 3) gospodarce cyfrowej oraz 4) działaniach wzmacniających spójność i zwiększających korzyści dla konsumentów. W Komunikacie KE z 2012 r. podjęto próbę określenia „cyklu zarządzania jednolitym rynkiem, tj. sposobu projektowania, wdrażania, stosowania i egzekwowania przepisów”; zob. Komunikat KE do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Lepsze zarządzanie jednolitym rynkiem, <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:52012DC0259> (dostęp: 24.05.2024). Dnia 28 października 2015 r. Komisja opublikowała komunikat pt. „Usprawnianie jednolitego rynku: więcej możliwości dla obywateli i przedsiębiorstw”, identyfikując i nazywając w nim m.in. nowy typ gospodarki, którego potencjał jest związany z operowaniem na rynkach cyfrowych, tj. „gospodarkę dzielenia się”; zob. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Usprawnianie jednolitego rynku: więcej możliwości dla obywateli i przedsiębiorstw, <https://eur-lex.europa.eu/legal-content/PL/TXT/?qid=153417238870&uri=CELEX:52015DC0550> (dostęp: 24.05.2024)).

konkurencji uzyskać dostęp do usług online lub je świadczyć²³⁹. Strategia budowy Jednolitego rynku cyfrowego (JRC) została uruchomiona przez Komisję Europejską w maju 2015 r.²⁴⁰

Strategia jednolitego rynku cyfrowego²⁴¹ stanowiła „program legislacyjny budowy europejskiej gospodarki cyfrowej”²⁴², kontynuowany w Europejskiej agendzie cyfrowej²⁴³. W centrum programu dla Europy z 2019 r. Komisja wyrażenie umieściła wzmocnienie jednolitego rynku cyfrowego. Zobowiązanie to odnowiono w dokumencie strategicznym Komisji z lutego 2020 r. pt. „Kształtowanie cyfrowej przyszłości Europy”²⁴⁴, w którym przedstawiono sposoby urzeczywistnienia jednolitego rynku cyfrowego²⁴⁵. Założono, że osiągnięcie celu polegającego na stworzeniu JRC powinno być poprzedzone ustanowieniem europejskiego jednolitego rynku danych i stworzeniem za pomocą spójnych regulacji równych warunków działania w internecie i poza nim²⁴⁶. Zarazem w przedstawionym programie dla Europy jednym z czterech priorytetowych obszarów aktywności regulacyjnej UE uczyniono kwestię „ochrony

²³⁹ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Strategia jednolitego rynku cyfrowego dla Europy, s. 3.

²⁴⁰ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 6 maja 2015 r.: Strategia jednolitego rynku cyfrowego dla Europy, <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=COM:2015:192:FIN> (dostęp: 22.03.2024).

²⁴¹ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Strategia jednolitego rynku cyfrowego dla Europy.

²⁴² *Rynek wewnętrzny: zasady ogólne* 05.2024, Noty tematyczne o Unii Europejskiej <https://www.europarl.europa.eu/factsheets/pl/sheet/33/rynek-wewnetrzny-zasady-ogolne> (dostęp: 24.05.2024).

²⁴³ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Europejska agenda cyfrowa, <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:pl:PDF> (dostęp: 10.10.2024).

²⁴⁴ *Kształtowanie cyfrowej przyszłości Europy*, 19.02.2020, EU4Digital, <https://eufordigital.eu/library/shaping-europes-digital-future/> (dostęp: 24.05.2024).

²⁴⁵ Etapy budowy jednolitego rynku cyfrowego zostały szczegółowo opisane na stronach Parlamentu Europejskiego, *Powszechny jednolity rynek cyfrowy* 05.2024, Noty tematyczne o Unii Europejskiej, <https://www.europarl.europa.eu/factsheets/pl/sheet/43/powszechny-jednolity-rynek-cyfrowy> (dostęp: 22.03.2024).

²⁴⁶ *Rynek wewnętrzny: zasady ogólne*, Noty tematyczne o Unii Europejskiej, <https://www.europarl.europa.eu/factsheets/pl/sheet/33/rynek-wewnetrzny-zasady-ogolne> (dostęp: 22.03.2024).

obywateli i wolności”²⁴⁷. Dnia 9 marca 2021 r. Komisja przedstawiła swoją wizję transformacji cyfrowej Europy do 2030 r. w Cyfrowym Kompasie: europejska droga w cyfrowej dekadzie²⁴⁸. We wrześniu 2021 r. Komisja wskazała ramy zarządzania służące osiągnięciu tych celów cyfrowych w dokumencie zatytułowanym „Droga ku cyfrowej dekadzie”²⁴⁹. W styczniu 2023 r. opublikowano w Dzienniku Urzędowym UE²⁵⁰ Deklarację praw i zasad cyfrowych w cyfrowej dekadzie²⁵¹, podpisaną przez Przewodniczących: Komisji, Parlamentu Europejskiego i Rady. Deklaracja praw i zasad cyfrowych, jak wskazano w jej motywie 7, opiera się na Europejskim filarze praw socjalnych i uzupełnia go. Ma ona charakter deklaratoryjny i jako taka nie wpływa na treść przepisów prawnych ani na ich stosowanie²⁵². Deklaracja została uzgodniona równolegle

²⁴⁷ Nowy program strategiczny dla UE 2019–24, <https://www.consilium.europa.eu/en/eu-strategic-agenda-2019-2024/> (dostęp: 22.03.2024).

²⁴⁸ *Cyfrowa dekada Europy: Komisja wyznacza kierunek w celu utworzenia do 2030 r. Europy opartej na technologiach cyfrowych*, 9.03.2021, Komisja Europejska, https://ec.europa.eu/commission/presscorner/detail/pl/IP_21_983.

²⁴⁹ *Ogłoszenie o stanie Unii: Komisja proponuje Drogę ku cyfrowej dekadzie w celu przeprowadzenia transformacji cyfrowej UE do 2030 r.*, 15.09.2021, Komisja Europejska, https://ec.europa.eu/commission/presscorner/detail/pl/ip_21_4630 (dostęp: 24.05.2024).

²⁵⁰ Dz.U. UE C z 2023 r. Nr 23, s. 1.

²⁵¹ Deklaracja w sprawie europejskich praw i zasad cyfrowych, <https://digital-strategy.ec.europa.eu/pl/library/declaration-european-digital-rights-and-principles#Declaration> (dostęp: 24.05.2024). Deklaracja stanowi uzupełnienie wcześniejszych inicjatyw cyfrowych podjętych przez państwa członkowskie, takich jak deklaracja z Tallina, <https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration> (dostęp: 24.05.2024), Deklaracja berlińska w sprawie społeczeństwa cyfrowego i rządu cyfrowego opartego na wartości, <https://digital-strategy.ec.europa.eu/en/news/berlin-declaration-digital-society-and-value-based-digital-government> (dostęp: 24.05.2024), Deklaracja z Lizbony – demokracja cyfrowa z celem, <https://futurium.ec.europa.eu/en/digital-compass/digital-principles/library-video/lisbon-declaration-digital-democracy-purpose> (dostęp: 24.05.2024).

²⁵² Na stronach KE wskazano, że „podpisanie na najwyższym szczeblu Europejskiej deklaracji praw i zasad cyfrowych w cyfrowej dekadzie odzwierciedla wspólne zobowiązanie polityczne UE i jej państw członkowskich do promowania i wdrażania tych zasad we wszystkich obszarach cyfrowego życia, aby osiągnąć cele cyfrowego kompasu na 2030 r. Deklaracja posłuży również jako wytyczne dla konkretnych prac nad programem polityki dotyczącym cyfrowej dekady, czyli mechanizmem monitorowania i współpracy służącym osiągnięciu wspólnych celów cyfrowych na koniec tego dziesięciolecia”; zob. Europejska deklaracja praw i zasad cyfrowych, https://poland.representation.ec.europa.eu/news/europejska-deklaracja-praw-i-zasad-cyfrowych-2022-12-15_pl (dostęp: 22.03.2024).

z przyjęciem przez PE i Radę rozporządzeń tworzących tzw. pakiet cyfrowy, tj. aktu o usługach cyfrowych²⁵³ i aktu o rynkach cyfrowych²⁵⁴.

Rozwijanie rynku cyfrowego Rada Europejska uznaje za filar rozwoju gospodarki europejskiej²⁵⁵. W październiku 2020 r., a zatem w okresie trwania pandemii COVID-19. Rada Europejska zwróciła się do Komisji Europejskiej z oczekiwaniem przedłożenia do końca 2020 r. wniosku dotyczącego aktu prawnego o usługach cyfrowych oraz, do marca 2021 r., kompleksowego „cyfrowego kompasu” określającego – jak to przedstawiono – „konkretne cyfrowe ambicje UE na 2030 r.”²⁵⁶. Taki „kompas” powinien obejmować ustanowienie systemu monitorowania europejskich zdolności i możliwości cyfrowych o znaczeniu strategicznym²⁵⁷. Wskazano, że UE, aby być suwerenna cyfrowo, musi zbudować w pełni cyfrowy jednolity rynek, wzmocnić swoje zdolności do określania własnych przepisów, dokonywania autonomicznych wyborów technologicznych oraz opracowywania i wdrażania zdolności cyfrowych i infrastruktury cyfrowej o znaczeniu strategicznym²⁵⁸. Rozwój cyfrowy powinien – jak podkreśliła Rada Europejska – „chronić nasze wartości, prawa podstawowe i bezpieczeństwo, musi także być społecznie zrównoważony”²⁵⁹. Podejście to określone zostało przez Radę jako „humanocentryczne”.

²⁵³ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych) (Dz.U. UE L Nr 277, s. 1 z późn. zm.).

²⁵⁴ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828 (akt o rynkach cyfrowych) (Dz.U. UE L Nr 265, s. 1).

²⁵⁵ W lipcu 2020 r. Rada Europejska uzgodniła bezprecedensowy pakiet na rzecz odbudowy, by przeciwdziałać skutkom COVID-19 dla naszych gospodarek i społeczeństw oraz by promować silną odbudowę Europy i transformację oraz reformę naszych gospodarek. Dwa wzajemnie wzmacniające się filary takiej odbudowy – transformacja ekologiczna i transformacja cyfrowa – w połączeniu z silnym i głębokim jednolitym rynkiem będą sprzyjać nowym formom wzrostu, wspierać spójność i konwergencję oraz wzmocnią odporność UE; zob. Konkluzje Rady Europejskiej w sprawie kształtowania cyfrowej przyszłości Europy z dnia 2 października 2020 r., <https://www.consilium.europa.eu/media/45927/021020-euco-final-conclusions-pl.pdf> (dostęp: 24.05.2024).

²⁵⁶ Konkluzje Rady Europejskiej w sprawie kształtowania cyfrowej przyszłości Europy z dnia 2 października 2020 r., s. 4, <https://www.consilium.europa.eu/media/45927/021020-euco-final-conclusions-pl.pdf> (dostęp: 24.05.2024).

²⁵⁷ Tamże, s. 4.

²⁵⁸ Tamże, pkt 7.

²⁵⁹ Tamże, pkt 7.

Rada uznała, że będzie ono wyróżniać UE, a także zwiększy atrakcyjność modelu europejskiego. Rada stwierdziła także, że wsparciem dla rozwoju rynku cyfrowego jest „gospodarka oparta na danych”²⁶⁰ i zadeklarowała, że na transformację cyfrową przeznaczy 20 proc. na mocy instrumentu na rzecz Odbudowy i Zwiększania Odporności²⁶¹.

Zważywszy na wagę, jaką organy UE przykładają do tworzenia jednolitego rynku cyfrowego, należy wskazać, że *ratio legis* ustanowienia nowych rozwiązań prawnych zawartych w pakiecie cyfrowym stanowiła potrzeba realizacji celów gospodarczych i politycznych UE²⁶². Spostrzeżenie to potwierdza zarówno charakter i treść, jak i okoliczności podpisania w grudniu 2022 r. przez przewodniczących Parlamentu Europejskiego, Komisji i Rady Europejskiej deklaracji praw i zasad cyfrowych²⁶³, która to deklaracja – jak wskazano w jej motywach – „odzwierciedla wspólne zaangażowanie polityczne w te prawa i zasady”²⁶⁴, jak również treść wcześniej przyjętych aktów nienormatywnych, w szczególności Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. w sprawie aktu prawnego o usługach cyfrowych

²⁶⁰ Tamże, pkt 9.

²⁶¹ Tamże, pkt 8.

²⁶² W dniu 15 grudnia 2022 r. przewodnicząca Komisji Europejskiej Ursula von der Leyen podpisała deklarację europejską w sprawie praw i zasad cyfrowych, wraz z przewodniczącą Parlamentu Europejskiego Robertą Metsoli i premierem Czechem Petrem Fialą. Prawa i zasady cyfrowe określone w Deklaracji będą uzupełniać istniejące prawa, takie jak prawa zakorzenione w Karcie praw podstawowych UE oraz prawodawstwo w zakresie ochrony danych i prywatności. Zapewnią one obywatelom ramy odniesienia dla ich praw cyfrowych, a także wytyczne dla państw członkowskich UE i przedsiębiorstw w odniesieniu do nowych technologii. Mają one pomóc wszystkim w UE jak najlepiej wykorzystać transformację cyfrową; zob. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en#digital-rights-and-principles (dostęp: 20.03.2024). Wskazano także, że realizacja tych celów wymaga przeszkolenia 20 mln specjalistów w dziedzinie ICT do 2030 r.; zob. *Europejska Dekada Cyfrowa: cele cyfrowe na 2030 rok*, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en (dostęp: 20.03.2024).

²⁶³ Europejska deklaracja praw i zasad cyfrowych w cyfrowej dekadzie [https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32023C0123\(01\)](https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32023C0123(01)) (dostęp 10.10.2024).

²⁶⁴ Zestawienie informacji na rzecz praw cyfrowych i zasad, <https://digital-strategy.ec.europa.eu/en/library/digital-rights-and-principles-factsheet> (dostęp: 24.05.2024).

i związanych z nim kwestii z zakresu praw podstawowych²⁶⁵, a także, finalnie, rozporządzeń PE i Rady w sprawie usług cyfrowych (AUC) i w sprawie rynków cyfrowych (pakietu cyfrowego).

W Rezolucji Parlamentu Europejskiego z dnia 20 października 2020 r. w sprawie aktu prawnego o usługach cyfrowych i związanych z nim kwestii z zakresu praw podstawowych PE zauważył, że „niezbędne jest szybkie i konsekwentne usuwanie treści niezgodnych z prawem w celu zwalczania czynów zabronionych i naruszeń praw podstawowych” (pkt S ppkt 3). Uznał zarazem za niewystarczające działania na podstawie dobrowolnie przyjmowanych kodeksów etycznych (pkt S ppkt 4) i za konieczne, by dostawcy usług społeczeństwa informacyjnego podejmowali bardziej zdecydowane działania wobec autorów nielegalnych treści i wezwał dostawców usług cyfrowych „do usuwania treści internetowych z zachowaniem staranności, proporcjonalności i zasady niedyskryminacji, z należyтым uwzględnieniem wszystkich okoliczności dotyczących praw podstawowych użytkowników” (pkt S ppkt 4). Jednocześnie zaproponował wprowadzenie instrumentu „etykietowania takich treści zamiast ich usuwania z internetu” (tamże). W tym samym dokumencie PE wyraził stanowisko, zgodnie z którym „należy zatamować rozpowszechnianie takich szkodliwych treści” (pkt S ppkt 7), podkreślając, że „szczególną klasę zagrożeń internetowych” stanowi „wprowadzająca w błąd lub niejasna reklama polityczna” (pkt 3 ppkt 10), a w konsekwencji PE wskazał, że „treści niezgodne z prawem należy usuwać konsekwentnie i bez zbędnej zwłoki, aby zwalczać przypadki naruszeń” (pkt S ppkt 11) i sformułował postulat, by „treści usuwać tam, gdzie są hostowane” (pkt S ppkt 16) oraz by „dostawcy usług cyfrowych byli w stanie jednoznacznie identyfikować użytkowników w sposób równoważny z usługami poza internetem” (pkt S ppkt 22). W tym celu PE uznał, że „niezbędna jest pełna harmonizacja i wyjaśnienie zasad dotyczących odpowiedzialności na szczeblu UE” (pkt S ppkt 24) i zaproponował „wprowadzenie wspólnych ram odpowiedzialności, aby skutecznie identyfikować i usuwać treści niezgodne z prawem” (pkt S ppkt 26). PE uznał także, że „przepisy dotyczące mechanizmów zgłaszania i usuwania treści niezgodnych z prawem należy

²⁶⁵ Akt prawny o usługach cyfrowych i związane z nim kwestie z zakresu praw podstawowych Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. w sprawie aktu prawnego o usługach cyfrowych i związanych z nim kwestii z zakresu praw podstawowych (2020/2022(INI)).

uzupełnić wymogami zobowiązującymi platformy do podejmowania konkretnych działań proporcjonalnych do skali ich zasięgu oraz ich możliwości technicznych i operacyjnych w celu skutecznego przeciwdziałania pojawianiu się niezgodnych z prawem treści w ramach ich usług” (pkt S ppkt 27) oraz że „w przypadkach, gdy jest to technicznie wykonalne – na podstawie dostatecznie uzasadnionych poleceń niezależnych właściwych organów publicznych oraz przy pełnym uwzględnieniu specyficznego kontekstu treści – od dostawców usług cyfrowych można wymagać okresowego wyszukiwania określonych elementów treści” (pkt S ppkt 27). W konsekwencji PE wskazał na konieczność przyjęcia i zastosowania „uzgodnionych standardów podstawowego bezpieczeństwa w cyberprzestrzeni, aby obywatele mogli w pełni korzystać z usług cyfrowych” (pkt S ppkt 45), widząc potrzebę „podjęcia przez państwa członkowskie skoordynowanych działań w celu zapewnienia podstawowej higieny cybernetycznej i zapobiegania niebezpieczeństwom w cyberprzestrzeni, których można uniknąć, w tym za pomocą środków ustawodawczych” (pkt S ppkt 45).

W motywach Deklaracji praw i zasad cyfrowych wskazano natomiast, że jej celem jest „wyjaśnienie wspólnych intencji politycznych. Nie tylko przypomina się w niej o najistotniejszych prawach w kontekście transformacji cyfrowej, ale także powinna ona służyć jako punkt odniesienia dla przedsiębiorstw i innych podmiotów istotnych dla opracowywania i wdrażania nowych technologii” (motyw 5 Deklaracji)²⁶⁶. W rozdziale IV Deklaracji zatytułowanym „Udział w cyfrowej przestrzeni publicznej” postanowiono, że:

Każdy ma prawo do wolności wypowiedzi w środowisku internetowym, bez obaw przed cenzurą lub zastraszeniem. Każdy powinien mieć możliwość dowiedzenia się, kto jest właścicielem usług, z których korzysta, lub kto je kontroluje.

Ponadto w tym samym rozdziale postuluje się, by „bardzo duże platformy internetowe wspierały swobodną debatę demokratyczną w internecie, ze względu na rolę swoich usług w kształtowaniu opinii publicznej i dyskursu”.

²⁶⁶ Europejska deklaracja praw i zasad cyfrowych w cyfrowej dekadzie, [https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32023Co123\(01\)](https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32023Co123(01)) (dostęp: 24.05.2024).

Rozdział IV zawiera także przyjęte przez sygnatariuszy Deklaracji w imieniu – jak należy sądzić – reprezentowanych przez nich organów zobowiązanie:

do dalszej ochrony praw podstawowych w internecie, w szczególności wolności wypowiedzi i informacji; do wprowadzenia środków mających na celu zwalczanie wszelkich form nielegalnych treści proporcjonalnie do szkód, jakie mogą one wyrządzić, przy pełnym poszanowaniu prawa do wolności wypowiedzi i informacji oraz bez ustanawiania jakichkolwiek ogólnych obowiązków w zakresie monitorowania; oraz do stworzenia środowiska internetowego, w którym ludzie są chronieni przed dezinformacją i innymi formami szkodliwych treści²⁶⁷.

Treść Deklaracji potwierdza, że wolą organów prawodawczych UE jest, z jednej strony, utrzymanie gwarancji ochronnych wolności wypowiedzi, a z drugiej strony, zmiana modelu, w ramach którego gwarancje te są wykonywane. Zmiana dotyczy zatem zarówno kręgu podmiotów, na których ma spoczywać obowiązek zapewnienia ochrony wolności wypowiedzi, jak i katalogu tych obowiązków, a także charakteru zaangażowania tych podmiotów w realizację obowiązków. O ile zatem organy UE zobowiązały się „do dalszej ochrony praw podstawowych w internecie, w szczególności wolności wypowiedzi i informacji”, o tyle – jak wynika z Deklaracji – po pierwsze, dopuszczają współdzielenie obowiązków i odpowiedzialności z podmiotami prywatnymi; po drugie, w miejsce postawy pasywnej, znanej na gruncie klasycznego standardu, oczekują działania („wspieranie swobodnej debaty demokratycznej”) i angażowania się podmiotów „w zwalczanie wszelkich form nielegalnych treści”; po trzecie, dokonują rozróżnienia dwóch kategorii wypowiedzi, spośród których tylko „legalne” treści będą zasługiwały na ochronę, podczas gdy „nielegalne treści” mają być zwalczane; po czwarte, uznają za niezbędne stworzenie instrumentów prawnych służących zwalczaniu „nielegalnych treści”; po piąte, przyjmują, że ocena „nielegalności” może być dokonywana *ex ante*, a zatem nie musi zostać poprzedzona ustaleniami dokonywanymi przez niezawisły sąd, lecz oceny „nielegalności” mogą dokonywać także inne podmioty i organy jeszcze przed rozpowszechnieniem

²⁶⁷ Tamże, rozdział IV.

wypowiedzi, co zarazem usprawiedliwia stosowanie środków zabezpieczających; po szóste, proponują stosowanie przesłanki proporcjonalności w sposób odwrócony, tj. przyjmując, że o proporcjonalności ingerencji przesądza rozmiar szkody powstałej w związku z rozpowszechnieniem wypowiedzi, nie zaś, jak tego dokonywano na gruncie klasycznego standardu, poprzez ocenę ryzyka związanego z powstaniem skutku mrożącego (ang. *chilling effect*) i uszczerbku, jaki mógłby powstać w związku z brakiem rozpowszechnienia wypowiedzi dla swobody debaty publicznej jako fundamentu demokracji.

Transpozycja klasycznego standardu wolności wypowiedzi polega zatem na odejściu od koncepcji absolutyzującej wolność wypowiedzi mającej swe źródło w modelu „wolnego rynku opinii” znanej na gruncie prawa amerykańskiego i zastąpieniu jej koncepcją relatywizującą wolność wypowiedzi poprzez przyjęcie, że wolność wypowiedzi nie tylko jest dobrem zastępowalnym, ale nadto może zostać usunięta z katalogu wartości prawnie chronionych, co stawia *de facto* pod znakiem zapytania przyrodzony walor tej wolności. W konsekwencji, transponowanie standardu wolności wypowiedzi do sfery cyfrowej i jednolitego rynku cyfrowego następuje poprzez modyfikowanie statusu i roli państwa w sferze regulowania wolności i praw człowieka i obywatela. Następuje odejście od gwarancyjnej roli państwa, charakterystycznej dla modelu wolnościowego, w którym „wolność należy regulować w aktach normatywnych w formie normy deklaratywnej z wymienieniem jej ograniczeń, ponieważ nosicielem wolności jest człowiek, a nie państwo”²⁶⁸, na rzecz powierzenia państwu kompetencji do konstytuowania wolności i praw. Spoiwo tej koncepcji stanowi termin „nielegalne treści”, zawierający domniemanie zawartego w nim nakazu dokonywania oceny treści pod kątem jej legalności oraz eliminowania treści nielegalnych jako niechronionych.

²⁶⁸ L. Wiśniewski, *Zakres ochrony prawnej wolności człowieka i warunki jej dopuszczalnych ograniczeń w praktyce*, [w:] *Wolności i prawa jednostki oraz ich gwarancje w praktyce*, L. Wiśniewski (red.), Warszawa 2006, s. 23.

3. Konstrukcja standardu

Standard wolności i praw w państwach demokratycznych oznacza istnienie wzorca normatywnego oddziałującego na sposób stanowienia i stosowania prawa, w szczególności ustalającego katalog obowiązków państwa, których celem jest ochrona wolności, a także określającego zasady i przesłanki dopuszczalnych ograniczeń tej wolności. Realizacja standardu łączy się z zaakceptowaniem modelu działania, który wymaga stosowania wspólnej metodyki przy dokonywaniu oceny istnienia naruszenia, jak i charakteru tego naruszenia, w szczególności przesłanek jego bezprawności. Pojęcie modelu oznacza konstrukcję teoretyczną powstałą na bazie wykładni językowej przepisów prawa krajowego i regulacji zawartych w prawie międzynarodowym, definiującą w sposób abstrakcyjny zakres podmiotowy i przedmiotowy danej wolności, w tym wolności wypowiedzi, oraz kryteria dopuszczalnych jej ograniczeń. Istniejące modele wolności wypowiedzi nie tworzą automatycznie standardu. Możliwe jest jednak, że będą one miały wpływ na standard wolności wypowiedzi, dokonując w efekcie jego uchylenia bądź zmiany²⁶⁹.

W wąskim ujęciu standard wolności wypowiedzi obejmuje treść i formę wypowiedzi (werbalnej lub niewerbalnej), której ochrona została potwierdzona przez niezawisły organ zgodnie z przyjętą w ustawie metodyką przeprowadzania oceny i ustalania jej wyników. Oznacza to, że ta sama wypowiedź może uzyskiwać różne oceny ze względu na zastosowany wzorzec, a w konsekwencji może mieścić się w standardzie albo go naruszać (wykraczać poza standard; nie odpowiadać standardowi). Standard wolności wypowiedzi ma zatem zawsze charakter umowny i może podlegać zmianom.

W szerokim ujęciu na pojęcie standardu wolności wypowiedzi składa się nie tylko wyobrażenie o tym, co dopuszczalne w związku z zastosowaniem sformalizowanego wzorca oceny, lecz także sam wzorzec. Przyjąć bowiem można, że dopiero sprzężenie metody dokonywania oceny z jej wynikiem pozwala na wypracowanie standardu wolności wypowiedzi. Nie jest jednak bez znaczenia, że uzyskanie tego rezultatu wymaga, by zarówno podmioty korzystające z wolności wypowiedzi, jak i organy dokonujące oceny

²⁶⁹ J. Tackowska-Olszewska, *Racjonalizacja wolności prasy...*, s. 115.

przestrzegały standardów. Czym innym będzie zatem przestrzeganie standardów przy dokonywaniu oceny sposobu korzystania z wolności wypowiedzi, a czym innym działanie w granicach standardu, tj. w ramach tego, co uprzednio zostało uznane za dopuszczalne.

Konwencyjny standard wolności wypowiedzi ustanowiony na podstawie art.10 EKPC pozwala przyjąć, że:

1. wolność wypowiedzi stanowi filar demokracji, będąc warunkiem koniecznym istnienia systemów demokratycznych²⁷⁰;
2. pod ochroną prawa pozostają także takie wypowiedzi, których treść lub forma oburza lub wprowadza niepokój²⁷¹;
3. zasadą jest swoboda wypowiedzi, podczas gdy jej ograniczenie jest wyjątkiem (odstępstwem od zasady), a w konsekwencji powinno zostać każdorazowo precyzyjnie uzasadnione²⁷²;
4. wypowiedzi dotyczące spraw budzących powszechne zainteresowanie podlegają dalej idącej ochronie niż pozostałe wypowiedzi;
5. osoby pełniące funkcje publiczne podejmują ryzyko zawodowe polegające na tym, że ich działania i zaniechania mogą być poddawane nawet dotkliwej krytyce uznawanej za uprawnioną²⁷³;
6. państwo ma spełniać funkcje gwaranta wolności wypowiedzi, ale nie jest wykluczone, że spoczywać będą na nim obowiązki pozytywne nawet w stosunkach pomiędzy podmiotami prywatnymi²⁷⁴;

²⁷⁰ Wyrok ETPC w sprawie Handyside przeciwko Wielkiej Brytanii, § 49–50.

²⁷¹ W sprawie Handyside ETPC wypowiedział fundamentalne dla ustalenia zakresu standardu wolności wypowiedzi stanowisko, zgodnie z którym: „Wolność słowa jest jednym z zasadniczych fundamentów takiego społeczeństwa, jednym z podstawowych warunków jego postępu i rozwoju każdej jednostki. Z zastrzeżeniem artykułu 10 ustęp 2, stosuje się ono nie tylko do »informacji« lub »idei«, które są przychylnie przyjmowane lub uważane za nieszkodliwe lub obojętne, ale także do tych, które obrażają, szokują lub niepokoją państwo lub jakąkolwiek część społeczeństwa. To jest istota pluralizmu, tolerancji i ducha otwartości, bez których nie może być mowy o »społeczeństwie demokratycznym«. Wynika z tego w szczególności, że wszelkie »formalności«, »warunki«, »ograniczenia« lub »sankcje« nałożone w tym względzie muszą być proporcjonalne do zamierzonego słusznego celu” (Wyrok ETPC w sprawie Handyside przeciwko Wielkiej Brytanii, § 49–50).

²⁷² Wyrok ETPC w sprawie Handyside przeciwko Wielkiej Brytanii, § 49–50.

²⁷³ Wyrok ETPC w sprawie Oberschlick przeciwko Austrii (nr 2), § 29.

²⁷⁴ ETPC stwierdził, że: „Rzeczywiste i skuteczne korzystanie z wolności wypowiedzi nie zależy jedynie od spoczywającego na państwie obowiązku powstrzymania się od ingerencji, ale może wymagać pozytywnych środków w celu ochrony jednostek, nawet

7. ochrona wolności wypowiedzi obejmuje nie tylko treść, ale także formę jej wyrażenia²⁷⁵;
8. ocena dopuszczalności wypowiedzi musi uwzględniać, czy wypowiedź ma charakter oceny, czy stanowi twierdzenie o faktach, nawet jednak jeśli ma charakter oceny, to ocena ta powinna posiadać podstawę faktyczną²⁷⁶.

Artykuł 10 EKPC chroniący swobodę wypowiedzi składa się z dwóch części²⁷⁷. W pierwszym ustępie określa zakres przyznanej ochrony. Ta ochrona dotyczy następujących wolności: do posiadania poglądów, do przekazywania informacji i idei oraz do ich otrzymywania. Artykuł 10 gwarantuje wolność wypowiedzi „każdej osobie” i nie dokonuje rozróżnienia w zależności od charakteru realizowanego celu ani ze względu na rolę, jaką osoby fizyczne lub prawne odgrywają w korzystaniu z tej swobody²⁷⁸. Dotyczy ona nie tylko treści informacji, lecz także środków, za pomocą których są one rozpowszechniane, w tym internetu, ponieważ każde ich ograniczenie narusza

w ich wzajemnych stosunkach, a w niektórych przypadkach państwo ma pozytywny obowiązek ochrony prawa do wolności wypowiedzi, nawet przed naruszeniami ze strony osób prywatnych” (Wyrok ETPC z dnia 12 września 2011 r. w sprawie Palomo Sánchez i inni przeciwko Hiszpanii (Wielka Izba), skarga nr 28955/06 i 3 inne, § 59).

²⁷⁵ Wyrok ETPC z dnia 3 lutego 2009 r. w sprawie Women on Waves przeciwko Portugalii, skarga nr 31276/05, § 38; podobnie wyroki ETPC: w sprawie Appleby przeciwko Wielkiej Brytanii, § 39; w sprawie VgT Verein Gegen Tierfabriken przeciwko Szwajcarii; z dnia 30 czerwca 2009 r. w sprawie VgT Verein Gegen Tierfabriken przeciwko Szwajcarii (nr 2), skarga nr 32772/02, § 80; zob. również *mutatis mutandis* Wyrok ETPC z dnia 16 marca 2000 r. w sprawie Özgür Gündem przeciwko Turcji, skarga nr 23144/93, § 42–46; Wyrok ETPC z dnia 29 lutego 2000 r. w sprawie Fuentes Bobo przeciwko Hiszpanii, skarga nr 39293/98, § 38 (dalej: Wyrok ETPC w sprawie Fuentes Bobo przeciwko Hiszpanii).

²⁷⁶ Wyroki ETPC: z dnia 19 czerwca 2003 r. w sprawie Pedersen i Baadsgaard przeciwko Danii, skarga nr 49017/99, § 76 (dalej: Wyrok ETPC w sprawie Pedersen i Baadsgaard przeciwko Danii); z dnia 22 stycznia 2015 r. w sprawie Pinto Pinheiro Marques przeciwko Portugalii, skarga nr 26671/09, § 43; z dnia 19 lipca 2018 r. w sprawie Makraduli przeciwko Była Jugosłowiańska Republika Macedonii, skargi nr 64659/11 i 24133/13, § 62.

²⁷⁷ I.C. Kamiński, *Pojęcie „mowy nienawiści” w orzecznictwie Europejskiego Trybunału Praw Człowieka*, [w:] *Kwalifikacja prawna mowy nienawiści – krajowe i europejskie uwarunkowania normatywne, społeczne i obyczajowe nadużycia wolności wypowiedzi*, J. Taczowska-Olszewska (red.), Warszawa 2024, s. 203.

²⁷⁸ Wyrok ETPC z dnia 13 lutego 2003 r. w sprawie Çetin i in. przeciwko Turcji, skargi nr 40153/98 i 40160/98, § 57.

prawo do otrzymywania i przekazywania informacji²⁷⁹. Podobnie Trybunał wielokrotnie stwierdzał, że art. 10 gwarantuje nie tylko prawo do przekazywania informacji, ale również prawo społeczeństwa do ich otrzymywania²⁸⁰.

Ustęp drugi art. 10 EKPC odnosi się do możliwości ingerencji w swobodę wypowiedzi. Każde ograniczenie musi łącznie spełniać trzy warunki: być przewidziane przez prawo, służyć realizacji uprawnionego celu oraz być konieczne w demokratycznym społeczeństwie. Nakaz legalności oznacza, że ingerencja musi wynikać z prawa adekwatnie dostępnego i sformułowanego w dostatecznie precyzyjny sposób²⁸¹. Ponadto ingerencji można dokonać tylko wtedy, gdy służy ochronie zamkniętego katalogu wyraźnie wskazanych celów (dóbr). Są to: bezpieczeństwo państwa, integralność terytorialna lub bezpieczeństwo publiczne; zapobieżenie zakłóceniu porządku lub przestępstwu; ochrona zdrowia i moralności; ochrona dobrego imienia i praw innych osób; zapobieżenie ujawnieniu informacji poufnych; zagwarantowanie powagi i bezstronności władzy sądowej. Wymóg konieczności w demokratycznym społeczeństwie oznacza natomiast, że każda ingerencja musi zostać poparta istnieniem „pilnej potrzeby społecznej”. Jak podkreśla I.C. Kamiński, „racje uzasadniające zastosowanie konkretnego środka prawnego muszą być dodatkowo istotne i wystarczające/dostateczne (ang. *relevant and sufficient*; fr. *pertinents et suffisants*), a relacja między użytym środkiem a chronionym celem – proporcjonalna²⁸².

Do uprawnionej ingerencji w swobodę wypowiedzi może dojść zatem w przypadku spełnienia łącznie kilku przesłanek²⁸³, które składają się na tzw. test szkodliwości (ang. *harm test*). Dopiero po jego przeprowadzeniu i ustaleniu, że zawarte w nim przesłanki zaistniały, możliwe jest zaakceptowanie ingerencji w wolność wypowiedzi jako działania usprawiedliwionego. Konieczne jest zatem, jak wskazano powyżej, ustalenie, czy:

1. zastosowane ograniczenie wolności wypowiedzi było przewidziane przez prawo;

²⁷⁹ Wyrok ETPC z dnia 22 maja 1990 r. w sprawie Autronic AG przeciwko Szwajcarii, skarga nr 12726/87, § 47.

²⁸⁰ Wyroki ETPC: z dnia 26 listopada 1991 r. w sprawie Observer and Guardian przeciwko Wielkiej Brytanii, skarga nr 13585/88, § 59 lit. b) oraz z dnia 19 lutego 1998 r. w sprawie Guerra i in. przeciwko Włochom, § 53.

²⁸¹ Wyrok ETPC w sprawie The Sunday Times przeciwko Wielkiej Brytanii (nr 1), § 49.

²⁸² I.C. Kamiński, *Pojęcie „mowy nienawiści”...*, s. 203.

²⁸³ Wyrok SN z dnia 21 kwietnia 2021 r., I NSKN 89/20, OSNKN 2021, nr 3, poz. 23.

2. ingerencja była niezbędna (konieczna) w społeczeństwie demokratycznym;
3. zastosowane środki były proporcjonalne w stosunku do celu ograniczenia.

Przeprowadzenie testu na „niezbędność w demokratycznym społeczeństwie” wymaga stwierdzenia, czy zaskarżona ingerencja odpowiada naglącej potrzebie społecznej, czy była proporcjonalna do realizacji prawnie uzasadnionego celu oraz czy podane przez władze państwowe powody dla jej uzasadnienia są istotne i wystarczające²⁸⁴.

Powyższe zasady znajdują zastosowanie także w orzecznictwie Trybunału Sprawiedliwości UE, co wynika przede wszystkim z treści art. 52 ust. 3 Karty praw podstawowych²⁸⁵. Wyrażne powołanie się Trybunału Sprawiedliwości UE (wcześniej ETS) na art. 10 EKPC miało miejsce w sprawie ERT²⁸⁶, w której Trybunał zauważył, że przepisy państwa członkowskiego odnoszące się do telewizji muszą być oceniane w świetle swobody wypowiedzi sformułowanej w art. 10 EKPC jako ogólnej zasady prawa, którą ETS przestrzega. Przy okazji rozpatrywania sprawy ERT Rzecznik Generalny Lenz podkreślił, że funkcja art. 10 EKPC nie polega na podważeniu monopolu państwowego telewizji, a jedynie na zapewnieniu dostępu do informacji. Ponadto Rzecznik wspomniał, że przy wykładni prawa wspólnotowego ETS musi uwzględniać przepisy EKPC²⁸⁷. ETS powołał się również na art. 10 i 11 KPP UE w orzeczeniu w sprawie RTL²⁸⁸ dotyczącej emitowania reklam w telewizji. Trybunał

²⁸⁴ Wyroki ETPC m.in.: w sprawie Błaja przeciwko Polsce, § 56; z dnia 18 września 2012 r. w sprawie Lewandowska-Malec przeciwko Polsce, skarga nr 39660/07, § 58, w sprawie The Sunday Times przeciwko Wielkiej Brytanii (nr 1), § 62; oraz w sprawie Skałka przeciwko Polsce, § 35.

²⁸⁵ Zgodnie z tym przepisem „W zakresie, w jakim niniejsza Karta zawiera prawa, które odpowiadają prawom zagwarantowanym w europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności, ich znaczenie i zakres są takie same jak praw przyznanych przez tę konwencję”.

²⁸⁶ Wyrok TS z dnia 18 czerwca 1991 r. w sprawie Elliniki Radiophonia Tikorassi AE przeciwko Dimotiki Etairia Pliroforisis i Sotirios Kawelas (ERT), nr C-260/89, s. 1–2925.

²⁸⁷ T. Jurczyk, *Ochrona wybranych praw jednostki zawartych w Karcie Praw Podstawowych i Europejskiej Konwencji Praw Człowieka w świetle orzecznictwa ETS*, [w:] tenże, *Prawa jednostki w orzecznictwie Europejskiego Trybunału Sprawiedliwości*, Warszawa 2009, s. 189.

²⁸⁸ Wyrok TS z dnia 23 października 2003 r. w sprawie RTL Television GmbH przeciwko Niedersechsische Landes medienausalt für privaten Rundfunk, nr C-245/01, s. 1.

podniósł, że państwa członkowskie same mogą decydować, kiedy ograniczać wolność wypowiedzi. Natomiast w sprawie TV 10 ETS stwierdził, że celem prawodawstwa dotyczącego mediów powinno być stworzenie pluralistycznego i niekomercyjnego systemu nadawczego w ramach polityki kulturalnej, zapewniającej swobodę wyrażania poglądów²⁸⁹.

Artykuł 11 KPP odpowiada standardowi z art. 10 EKPC. Prawo zagwarantowane w art. 11 Karty, które „obejmuje wolność posiadania poglądów oraz otrzymywania i przekazywania informacji i idei bez ingerencji władz publicznych i bez względu na granice państwowe”, odpowiada prawu przewidzianemu w art. 10 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności. Zgodnie z art. 52 ust. 3 Karty te dwa prawa mają zatem takie samo znaczenie lub co najmniej ten sam zakres. Z powyższego wynika, że art. 11 Karty należy interpretować w świetle art. 10 EKPC i związanego z nim orzecznictwa Europejskiego Trybunału Praw Człowieka²⁹⁰.

TSUE uznał, podobnie jak uczynił to wcześniej ETPC na gruncie art. 10 EKPC, że wolności wypowiedzi i informacji nie mają charakteru absolutnego i mogą podlegać ograniczeniom. Zgodnie z postanowieniami Karty (art. 52 ust. 1) takie ograniczenia są dopuszczalne, o ile są przewidziane ustawą i szanują istotę praw i wolności, w które ingerują. Ponadto wszelkie takie ograniczenia muszą spełniać wymogi zasady proporcjonalności, tj. być konieczne i rzeczywiście odpowiadać celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób²⁹¹. W tym zakresie Trybunał stwierdził, że wymóg, zgodnie z którym wszelkie ograniczenia korzystania z praw podstawowych muszą być przewidziane ustawą, oznacza, że akt, który pozwala na ingerencję w te prawa, musi sam określać zakres ograniczenia wykonywania danego prawa²⁹². Jednakże, zgodnie

²⁸⁹ Wyrok TS z dnia 5 października 1994 r. w sprawie TV 10 SA przeciwko Commissariaat voor de Media, nr C-23/93, s. 1–4.

²⁹⁰ Opinia Rzecznika Generalnego UE z dnia 15 lipca 2021 r., sprawa C-401/19 Rzeczpospolita Polska przeciwko Parlamentowi Europejskiemu, Radzie Unii Europejskiej.

²⁹¹ S. Hambura, M. Muszyński, *Karta Praw Podstawowych z komentarzem*, Bielsko-Biała 2001, s. 22, cyt. za: T. Jurczyk, *Wolności wynikające z Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności oraz Karty Praw Podstawowych*, [w:] tenże, *Prawa jednostki...*, s. 45.

²⁹² Wyrok TS z dnia 16 lipca 2020 r. w sprawie Facebook Ireland i Schrems, C-311/18, pkt 175 i przytoczone tam orzecznictwo.

z orzecznictwem Europejskiego Trybunału Praw Człowieka, wymaganie, by wszelkie ograniczenia korzystania z prawa podstawowego były przewidziane przez ustawę, nie wyklucza, by uregulowanie zawierające to ograniczenie było sformułowane w sposób wystarczająco otwarty, tak aby można je było dostosować do zmieniających się sytuacji²⁹³. I.C. Kamiński zwraca uwagę, że w ujęciu Europejskiego Trybunału Praw Człowieka termin „ustawa” należy rozumieć w znaczeniu materialnym, a nie tylko w ujęciu formalnym, „ponieważ może ono obejmować zarówno »prawo pisane«, jak i »prawo niepisane«, a także »prawo wypracowane« przez sądy”²⁹⁴.

W odniesieniu do zasady proporcjonalności wymaga ona, by ograniczenia, które mogą być zwłaszcza nałożone przez akty prawa Unii na prawa i wolności ustanowione w Karcie, nie wykaczały poza granice tego, co jest odpowiednie i konieczne do realizacji uzasadnionych celów lub potrzeby ochrony praw i wolności innych osób, przy czym tam, gdzie istnieje możliwość wyboru spośród większej liczby odpowiednich rozwiązań, należy stosować rozwiązania najmniej dotkliwe, a wynikające z tego niedogodności nie mogą być nadmierne w stosunku do zamierzonych celów²⁹⁵. W przypadku, gdy sprawa dotyczy różnych praw podstawowych i zasad ustanowionych w traktatach, ocena poszanowania zasady proporcjonalności powinna być dokonywana z należytym uwzględnieniem koniecznego pogodzenia wymogów dotyczących ochrony poszczególnych praw i zasad, o których mowa, oraz odpowiedniej równowagi między tymi prawami i zasadami²⁹⁶. W szczególności, jeśli chodzi o ograniczenie w korzystaniu z prawa do wolności wypowiedzi i informacji, z orzecznictwa Europejskiego Trybunału Praw Człowieka wynika²⁹⁷, że o ile art. 10 EKPC sam w sobie nie zakazuje jakiegokolwiek uprzedniego

²⁹³ Wyrok ETPC z dnia 16 czerwca 2015 r. w sprawie Delfi AS przeciwko Estonii, skarga nr 64569/09, § 121 (dalej: Wyrok ETPC w sprawie Delfi AS przeciwko Estonii) i przytoczone tam orzecznictwo.

²⁹⁴ I.C. Kamiński, *Falszywe wiadomości (fake news) oraz dezinformacja a Europejska Konwencja Praw Człowieka*, „Przegląd Prawa Publicznego” 2023, nr 11, s. 90–107.

²⁹⁵ Wyroki TS: z dnia 13 marca 2019 r. w sprawie Polska/Parlament i Rada, C-128/17, pkt 94 i przytoczone tam orzecznictwo; z dnia 17 grudnia 2020 r. w sprawie Centraal Israëlitisch Consistorie van België i in., C-336/19, pkt 64 i przytoczone tam orzecznictwo.

²⁹⁶ Wyrok TS z dnia 17 grudnia 2020 r. w sprawie Centraal Israëlitisch Consistorie van België i in., C-336/19, pkt 65 i przytoczone tam orzecznictwo.

²⁹⁷ S. Hambura, M. Muszyński, *Karta Praw Podstawowych...*, cyt. za: T. Jurczyk, *Wolności wynikające...*, [w:] *Prawa jednostki...*, s. 45.

ograniczenia środka rozpowszechniania treści, o tyle takie ograniczenia stanowią zagrożenie dla poszanowania tego prawa podstawowego na tyle duże, że winny one być ujęte w szczególnie ścisłe ramy prawne²⁹⁸.

Stanowisko wyrażane przez ETPC i TSUE (ETS) na gruncie odpowiednio art. 10 EKPC i art. 11 KPP, wskazuje, że nie mają one charakteru konkurencyjnego, lecz uzupełniający. Zarówno w Karcie, jak i w EKPC przyznano, że możliwe jest ograniczenie korzystania z praw i wolności, ingerencja w korzystanie z praw lub ograniczenie korzystania z wolności, które one gwarantują. Europejski Trybunał Praw Człowieka – jak zauważa I.C. Kamiński – odwołując się głównie do zasady rządów prawa ustanowionej w preambule do EKPC, stworzył na podstawie tego wyrażenia i zasadniczo za pomocą pojęcia „jakości prawa” doktrynę marginesu uznania państwa, zgodnie z którą każde ograniczenie lub ingerencja powinny być uprzednio przedmiotem przepisu ustawowego, co najmniej w materialnym znaczeniu tego terminu, który jest wystarczająco jasny w świetle wyznaczonego celu, czyli zgodny z minimalnymi wymogami²⁹⁹.

Standard wolności wypowiedzi ustalony na gruncie art. 10 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności i art. 11 Karty praw podstawowych są, co do zasady, tożsame, a w rezultacie pozwalają na dążenie, zarówno w obrębie państw członkowskich Rady Europy, jak i Unii Europejskiej, do osiągnięcia podobnego poziomu ochrony wolności wypowiedzi. O ile zatem na płaszczyźnie postulatywnej można dostrzec dążenie państw, bez względu na granice, do osiągnięcia podobnego standardu ochrony wolności wypowiedzi, o tyle na przeszkodzie osiągnięcia tego standardu stają względy technologiczne związane z przeniesieniem debaty publicznej do internetu, a w konsekwencji potrzeba dostosowania zarówno w aspekcie proceduralnym (formalnym), jak i materialnoprawnym kształtu wolności wypowiedzi i wzorca jej ochrony.

W odniesieniu do znaczenia internetu dla korzystania z wolności wyrażania opinii ETPC ustalił, że w świetle swojej dostępności oraz możliwości przechowywania i przekazywania dużych ilości informacji internet

²⁹⁸ Wyrok ETPC z dnia 18 grudnia 2012 r. w sprawie Ahmet Yildirim przeciwko Turcji, skarga nr 3111/10, § 48 (dalej: Wyrok ETPC w sprawie Ahmet Yildirim przeciwko Turcji).

²⁹⁹ I.C. Kamiński, *Pojęcie „mowy nienawiści”...*, s. 203.

odgrywa ważną rolę w poprawie publicznego dostępu do informacji i ogólnie ich udostępnianiu³⁰⁰. Jednocześnie ryzyko zagrożenia stwarzane przez treści i komunikację w internecie dla egzekwowania i korzystania z praw człowieka i wolności, w szczególności prawa do poszanowania życia prywatnego, jest z pewnością wyższe niż to stwarzane przez prasę³⁰¹. Ze względu na szczególny charakter internetu, jeżeli chodzi o treści osób trzecich, dla celów art. 10 takie „obowiązki i odpowiedzialność” internetowych portali informacyjnych mogą w pewnym stopniu różnić się od tych spoczywających na wydawcy w rozumieniu tradycyjnym³⁰². Jakkolwiek cytowane powyżej stanowisko Trybunał wypowiedział, dokonując porównania pomiędzy dystrybucją informacji w internecie a wydawaniem prasy, to jednak znajduje ono zastosowanie nie tylko do wydawania prasy, lecz także do innych niż prasa, tradycyjnych środków komunikowania.

Trybunał orzekł, że zasady dotyczące powielania materiałów z mediów drukowanych i internetu mogą się różnić. W tym drugim przypadku, aby zapewnić ochronę i wspieranie danych praw i wolności, niewątpliwie konieczne jest dostosowanie wzorców ochrony do specyfiki nowych technologii³⁰³. Zarazem należało uwzględnić, że w ramach wolności wypowiedzi na ochronę zasługuje także prawo dostępu do internetu, które zostało uznane przez sądy konstytucyjne niektórych państw członkowskich UE za prawo człowieka³⁰⁴.

³⁰⁰ Wyrok ETPC w sprawie Ahmet Yildirim przeciwko Turcji, § 48.

³⁰¹ Wyrok ETPC z dnia 7 listopada 2017 r. w sprawie Egill Einarsson przeciwko Islandii, skarga nr 24703/15, § 46.

³⁰² Wyrok ETPC w sprawie Delfi AS przeciwko Estonii, § 113.

³⁰³ Wyrok ETPC z dnia 5 maja 2011 r. w sprawie Redakcja Prawoje Dielo i Sztekel przeciwko Ukrainie, skarga nr 33014/05, § 63.

³⁰⁴ W decyzji z dnia 10 czerwca 2009 r. (decyzja nr 2009580 DC) Francuska Rada Konstytucyjna wyjaśniła, że wolność wypowiedzi oznacza wolność dostępu do internetu. Podano w niej również szereg podstawowych zasad dotyczących ograniczenia dostępu do internetu. Wskazano, że ograniczenie swobody publicznego dostępu do usług łączności online może zostać zarządzone wyłącznie przez sędziego, po przeprowadzeniu sprawiedliwego procesu, i musi być proporcjonalne. Biorąc pod uwagę, że „charakter wolności zagwarantowanej w art. 11 Deklaracji z 1789 r., ustawodawca nie mógł [...] powierzyć władzom administracyjnym uprawnienia [do ograniczenia lub uniemożliwienia dostępu do Internetu] w celu ochrony praw podmiotów praw autorskich i praw pokrewnych”, Rada Konstytucyjna uznała za niezgodne z konstytucją artykuły ustawy, które przewidywały, w przypadku naruszenia praw autorskich, odcięcie dostępu do internetu bez uprzedniego orzeczenia sądowego. Orzekł on, że zawieszenie dostępu jest możliwe tylko wtedy, gdy zostało zarządzone po zakończeniu kontradiktoryjnego postępowania sądowego jako kara

Z analizy przeprowadzonej przez ETPC dotyczącej ustawodawstwa dwudziestu państw członkowskich Rady Europy (Austrii, Azerbejdżanu, Belgii, Republiki Czeskiej, Estonii, Finlandii, Niemiec, Francji, Irlandii, Włoch, Litwy, Niderlandów, Polski, Portugalii, Rumunii, Rosji, Słowenii, Hiszpanii, Szwajcarii i Zjednoczonego Królestwa) wynika, że prawo dostępu do internetu jest teoretycznie chronione przez mające zastosowanie konstytucyjne gwarancje wolności wypowiedzi. Uważa się, że jest ono nierozdzielnie związane z prawem dostępu do informacji i komunikacji chronionym przez konstytucje krajowe oraz że obejmuje prawo każdego do uczestnictwa w społeczeństwie informacyjnym i obowiązek państw do zagwarantowania obywatelom dostępu do internetu. Z wszystkich ogólnych gwarancji chroniących wolność wypowiedzi można zatem wywnioskować, że należy również uznać prawo do nieskrępowanego dostępu do internetu³⁰⁵.

ETPC zauważył, że jeśli chodzi o możliwe środki mające na celu ograniczenie nielegalnych treści w internecie, w tekstach krajów europejskich istniało wiele różnych podejść i środków legislacyjnych, począwszy od indywidualizowanego zawieszenia dostępu do internetu, poprzez usuwanie nielegalnych treści, aż po zakaz dostępu do konkretnej strony internetowej. W większości państw europejskich ochrona praw nieletnich i walka z ich seksualnym wykorzystywaniem stanowią podstawę do podjęcia odpowiednich środków w celu ograniczenia dostępu do danych stron (Niemcy, Wielka Brytania, Szwajcaria i Francja). Jeśli chodzi o zwykłą przestępczość, ograniczenia dostępu są różne i mniej dotkliwe w sześciu krajach (Austria, Estonia, Finlandia, Włochy, Litwa, Niderlandy)³⁰⁶.

dodatkowa, i przypomniał, że środki tymczasowe lub nakazy sądowe mogą być zarządzone przez sędziego orzekającego w przedmiocie środków tymczasowych, pod warunkiem że są one „absolutnie niezbędne do ochrony danych praw” (Wyrok ETPC w sprawie Ahmet Yildirim przeciwko Turcji, pkt 32). Francuska Rada Konstytucyjna wypowiedziała się we wskazanej powyżej decyzji w związku z procedowaną wówczas tzw. ustawą Hadopi (*Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet* – „Wysoki urząd ds. rozpowszechniania utworów i ochrony praw w Internecie” – zob. Hadopi, <https://www.hadopi.fr/organisation/presentation>, dostęp: 2.04.2024).

³⁰⁵ Wyrok ETPC w sprawie Ahmet Yildirim przeciwko Turcji, pkt 32.

³⁰⁶ Tamże, pkt 33. ETPC zauważył, że jeśli chodzi o zakres środków ograniczających dostęp, zasadniczo dokonuje się rozróżnienia w zależności od charakteru popełnionego przestępstwa, w zależności od tego, czy chodzi o naruszenie praw własności intelektualnej, czy o inne przestępstwo. Zgodnie z raportem OBWE „Wolność wypowiedzi w Internecie: badanie przepisów prawnych i praktyk związanych z wolnością wypowiedzi, swobodnym

Artykuł 10 EKPC jako taki nie zakazuje stosowania uprzednich ograniczeń w zakresie rozpowszechniania wypowiedzi (*ex ante*). Trybunał wskazał³⁰⁷, że o braku takiego zakazu przesądzają użyte w art. 10 EKPC terminy: „warunki”, „ograniczenia”, „zapobieganie”, „sankcje”, a także wyroki w sprawie Sunday Times przeciwko Wielkiej Brytanii³⁰⁸. EKPC zauważył zarazem, że:

takie ograniczenia są jednak tak niebezpieczne, że wymagają najbardziej skrupulatnej kontroli ze strony Trybunału. Jest to szczególnie prawdziwe w przypadku prasy: informacja jest towarem łatwo psującym się, a opóźnianie jej publikacji, nawet na krótki czas, może pozbawić ją wszelkiej wartości i zainteresowania. Ryzyko to istnieje również w przypadku publikacji innych niż periodyki, które dotyczą aktualnego tematu³⁰⁹.

W odniesieniu do znaczenia dostępu do stron internetowych w realizacji wolności wypowiedzi Trybunał przypomniał, że aktualne pozostaje stanowisko wypowiedziane w sprawie Times Newspapers Ltd przeciwko Wielkiej Brytanii³¹⁰, zgodnie z którym:

oprócz dostępności i możliwości przechowywania i rozpowszechniania dużych ilości danych, strony internetowe odgrywają ważną rolę w poprawie publicznego dostępu do wiadomości i ogólnie w ułatwianiu przekazywania informacji³¹¹.

przepływem informacji i pluralizmem mediów w Internecie w państwach członkowskich OBWE” w Austrii, Niemczech, Polsce i Republice Czeskiej nie istnieją ogólne przepisy prawne dotyczące blokowania dostępu do internetu, a pięć państw nie posiada przepisów przewidujących ogólne blokowanie w przypadku jakiegokolwiek przestępstwa, ale posiada szczegółowe przepisy ustawowe przewidujące blokowanie w przypadku niektórych rodzajów przestępstw (Estonia, Federacja Rosyjska, Finlandia, Niderlandy, Wielka Brytania), np. w przypadkach pornografii dziecięcej lub rasizmu, nawoływania do nienawiści, podżegania do terroryzmu lub zniesławienia (tamże, pkt 34).

³⁰⁷ Wyrok ETPC w sprawie Ahmet Yildirim przeciwko Turcji, pkt 47.

³⁰⁸ Wyroki ETPC: w sprawie The Sunday Times przeciwko Wielkiej Brytanii (nr 1), oraz z dnia 20 listopada 1989 r. w sprawie Markt intern Verlag GmbH i Klaus Beermann przeciwko Niemcom, skarga nr 10572/83.

³⁰⁹ Wyrok ETPC w sprawie Ahmet Yildirim przeciwko Turcji, pkt 47.

³¹⁰ Wyrok ETPC z dnia 10 marca 2009 r. w sprawie Times Newspapers Ltd przeciwko Wielkiej Brytanii (nr 1 i 2), skargi nr 3002/03 i 23676/03, § 27.

³¹¹ Wyrok ETPC w sprawie Ahmet Yildirim przeciwko Turcji, pkt 48.

O ile zatem standard ochrony wolności wypowiedzi wypracowany na gruncie KPP i ETPC był adekwatny i skuteczny w odniesieniu do tradycyjnych mediów, o tyle zmiana modelu korzystania z wolności wypowiedzi determinowana nowymi technologiami wymusiła wypracowanie nowego wzorca ochrony, a w konsekwencji także nowego kształtu wolności wypowiedzi w ujęciu materialnoprawnym. Wzorzec ten jest zbudowany na odmiennych założeniach mających swe źródło w domniemaniu dotyczącym zagrożeń, jakie łączą się z korzystaniem z wolności wypowiedzi w internecie i ryzyku szkód, jakie mogłyby powstać w razie zaniechania działań o charakterze prewencyjnym.

W konsekwencji postulowany wzorzec zakłada:

1. dopuszczalność stosowania prewencyjnych środków ochrony służących przeciwdziałaniu rozpowszechnieniu nielegalnych (niepożądanych) treści niezależnie od środków zabezpieczających zarządzanych w toku postępowań sądowych;
2. włączenie środków ochrony stosowanych *ex ante* do arsenału środków zwykłego reagowania na naruszenia;
3. współdzielenie przez organy publiczne z podmiotami prywatnymi kompetencji w zakresie reagowania na nadużycia wolności wypowiedzi, w tym przyznanie podmiotom prywatnym prawa do dokonywania uprzedniej oceny i kategoryzowania (kwalifikowania) wypowiedzi (legalne vs. nielegalne);
4. potwierdzenie istnienia po stronie państwa obowiązków pozytywnych w zakresie reagowania na akty korzystania z wolności wypowiedzi;
5. nałożenie na państwo obowiązku działania w zakresie wykrywania nielegalnych treści;
6. modyfikacje przesłanek legalizujących ingerencję w wolność wypowiedzi zarówno poprzez poszerzenie ich katalogu, jak i zmianę o charakterze jakościowym.

Zastosowanie zmienionego wzorca oceny wypowiedzi może prowadzić do odmiennych ustaleń dotyczących dopuszczalności objęcia jej ochroną i, ewentualnie, zastosowania ograniczeń dotyczących jej rozpowszechnienia.

II. Kategorie wypowiedzi – złożoność standardu

Wypowiedzi – ze względu na ich różnorodność formalną (wypowiedzi werbalne i niewerbalne), różnorodność źródła, zakres rozpowszechnienia, intencje autora oraz tło i okoliczności, a także forum, na jakim wypowiedź zostaje wygłoszona, oraz ocenę istnienia lub nieistnienia twórczego wkładu autora w powstanie wypowiedzi, a przede wszystkim ze względu na ich złożoność treściową – mogą być klasyfikowane według wielu kryteriów dobieranych adekwatnie do przedmiotu i celu prowadzonych badań. I.C. Kamiński podsumowując strasburskie orzecznictwo, zauważa, że Trybunał wyróżnił następujące obszary wypowiedzi: wypowiedź polityczna, wypowiedź w sprawach mających publiczne (ogólne) znaczenie, wypowiedź artystyczna i wypowiedź komercyjna¹. W dwóch pierwszych obszarach, które są kluczowe dla demokratycznego państwa, każda ingerencja musi zostać przekonująco uzasadniona przez władze krajowe i każda sankcja podlega w Strasburgu drobiazgowej, rygorystycznej kontroli². Zarazem autor ten spostrzega, że wraz z przyjęciem w 2022 r. nowej rekomendacji w sprawie zwalczania mowy nienawiści³ nastąpiła zmiana kontekstu normatywnego, który ETPC stosuje, dokonując

¹ I.C. Kamiński, *Pojęcie „mowy nienawiści”...*, s. 205.

² Wyrok ETPC z dnia 17 grudnia 2004 r. w sprawie Cumpăna i Mazăre przeciwko Rumunii, skarga nr 33348/96, §§ 114 i 116 (dalej: Wyrok ETPC w sprawie Cumpăna i Mazăre przeciwko Rumunii).

³ Rekomendacja z 20 maja 2022 r. w sprawie zwalczania mowy nienawiści, *Combating hate speech*, <https://rm.coe.int/prems-083822-gbr-2018-recommendation-on-combating-hate-speech-memorand/1680a710c9> (dostęp: 10.10.2024).

wykładni zakresu wolności wypowiedzi⁴. Stosowany dotychczas sposób klasyfikowania wypowiedzi traci na znaczeniu. Funkcję klasyfikacyjną pełnić zaczęła nowa kategoria wypowiedzi, która w dokumentach zarówno RE, jak i UE jest ujmowana jako „mowa nienawiści”⁵. Konstrukcja mowy nienawiści:

służy do nazwania (określenia) danej wypowiedzi. Jeżeli wypowiedzi przyzna się przymiot mowy nienawiści, to niezależnie od innych atrybutów wypowiedzi oraz jej okoliczności pojawia się domniemanie zgodności krajowej ingerencji z Konwencją. Tylko nieproporcjonalność sankcji może prowadzić do naruszenia art. 10⁶.

Stanowisko ETPC, zważywszy na treść art. 52 Karty praw podstawowych, rzutuje na treść poglądów wyrażanych na gruncie prawa UE. Trudno zarazem dostrzec istnienie różnicy w koncepcjach i podejściu do ochrony wolności wypowiedzi na gruncie EKPC i KPP. Jednakże to organy UE, ze względu na posiadane narzędzia i instrumenty, w szczególności możliwość uchwalania przez PE rozporządzeń, kształtuje rzeczywistość prawną obywateli i państw członkowskich UE.

Zasadnicze znaczenie dla klasyfikowania rodzajów wypowiedzi, a w konsekwencji ustalenia zasad ich ochrony, mają rozporządzenia:

1. rozporządzenie PE i Rady w sprawie jednolitego rynku usług cyfrowych⁷ oraz
2. rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym⁸.

⁴ I.C. Kamiński, *Mowa nienawiści – pojęcie i jego zakres*, [w:] *Kwalifikacja prawna...*, J. Taczowska-Olszewska (red.), s. 85.

⁵ Autor ten zauważa, że „tradycyjne standardy związane z kwalifikacją wypowiedzi jako twierdzenia lub opinii tracą znaczenie w kontekście wypowiedzi, które są identyfikowane jako mowa nienawiści. Analogiczne dzieje się i z tezami akcentującymi konieczność mocnej ochrony debaty politycznej i wokół spraw mających publiczne znaczenie. Kluczowe i centralne staje się uznanie danej wypowiedzi za mowę nienawiści (tamże, s. 85).

⁶ Tamże, s. 85.

⁷ AUC.

⁸ ARC.

Na gruncie rozporządzeń cyfrowych (AUC i ARC) ustawodawca europejski posłużył się terminem „nielegalne treści”, który definiuje jako:

informacje, które same w sobie lub przez odniesienie do działania, w tym sprzedaży produktów lub świadczenia usług, nie są zgodne z prawem Unii lub z prawem jakiegokolwiek państwa członkowskiego, które jest zgodne z prawem Unii, niezależnie od konkretnego przedmiotu lub charakteru tego prawa (art. 3 lit. h AUC).

Jak zostanie to poniżej wykazane, zasadą jest odmowa ochrony nielegalnych treści, które ustawodawca europejski uznaje za niezgodne z europejskim standardem, a w konsekwencji stwierdza, że nie tylko nie zasługują one na ochronę, ale ponadto konieczne jest ich usuwanie jako szkodliwych z debaty publicznej. Mowa nienawiści jest kwalifikowanym typem nielegalnych treści, co oznacza, że na gruncie AUC i ARC może zostać wyodrębnionych wiele rodzajów (kategorii) treści (wypowiedzi), które – zgodnie z przyjętymi w rozporządzeniach cyfrowych mechanizmami – będą usuwane z przestrzeni publicznej.

Zasadnicza linia podziału rodzajów wypowiedzi musi obecnie uwzględniać kryterium legalności (zgodności wypowiedzi z prawem europejskim). Następuje zatem podział wypowiedzi na: 1) treści legalne oraz 2) treści nielegalne. Tylko te wypowiedzi, które nie zostały uznane za nielegalne, korzystają z ochrony na zasadach wypracowanych przez ETPC na gruncie art. 10 EKPC. W odniesieniu do tych wypowiedzi nadal aktualny pozostaje standard ochrony oparty w szczególności na domniemaniu bezprawności ingerencji w wolność wypowiedzi. Perspektywa ta jest jednak całkowicie odmienna w odniesieniu do wypowiedzi zaliczonych do „nielegalnych treści”. Ze względu na niejednorodny charakter tych wypowiedzi, zmienność kontekstów oraz ich wielowymiarowość, a nawet intuicyjność, znajdują się one na granicy tego, co objęte ochroną i tego, co zabronione. Zakwalifikowanie wypowiedzi do kategorii nielegalnych treści uruchamia reakcję silnie ingerującą w wolność wypowiedzi, pozbawiając autora możliwości dalszego jej rozpowszechniania.

Omówione poniżej kategorie wypowiedzi uwzględniają obie perspektywy, a zatem zarówno tę, która odpowiada klasycznie rozumianemu standardowi wolności wypowiedzi, w którym ingerencja w wolność wypowiedzi jest wyjątkiem, a państwo dokonując ingerencji, musi mieć silną podstawę faktyczną

i prawną, jak też tę, w której ze względu na atrybut „nielegalności” odmawia się ochrony niektórym kategoriom wypowiedzi.

1. Wypowiedzi mające znaczenie dla debaty publicznej

Znaczenie „debaty publicznej” jako okoliczności ukierunkowującej zastosowanie przesłanek uwalniających od odpowiedzialności za naruszenie prawa związane z treścią lub formą wypowiedzi było wielokrotnie podkreślane w orzecznictwie ETPC. Debatę publiczną Trybunał uznaje za jedną z podstawowych wartości państwa demokratycznego. Z tych też względów na gruncie art. 10 ust. 2 EKPC istnieje bardzo niewielkie pole do ograniczania debaty w kwestiach pozostających w zainteresowaniu publicznym, w szczególności w odniesieniu do działalności prasowej⁹.

Znaczenie wypowiedzi dla debaty publicznej oraz staranność i rzetelność autora wypowiedzi, który przed jej rozpowszechnieniem podjął próby weryfikowania podstaw faktycznych, na których opierała się wypowiedź, stanowią także, na gruncie prawa krajowego, wystarczające okoliczności wyłączające odpowiedzialność autora wypowiedzi, choćby zawarte w niej twierdzenia okazały się nieprawdziwe albo ich prawdziwości nie udało się z całą pewnością dowieść w procesie. Zdaniem Sądu Najwyższego wypowiedź taka mieści się bowiem w obszarze, do którego w pierwszej kolejności mają zastosowanie konstytucyjne gwarancje wolności słowa. Z treści stanowiska wyrażonego przez Sąd Najwyższy w wyroku z dnia 21 kwietnia 2021 r.¹⁰ wynika zarazem, że nie tylko dziennikarze i funkcjonariusze sprawujący funkcje kontrolne, ale także obywatele niewykonujący takich funkcji są uprawnieni, by – w ramach społecznej

⁹ Wyroki ETPC: z dnia 29 marca 2016 r. w sprawie Bédát przeciwko Szwajcarii, skarga nr 56925/08, § 49 (dalej: Wyrok ETPC w sprawie Bédát przeciwko Szwajcarii); oraz z dnia 17 maja 2016 r. w sprawie Karácsony i in. przeciwko Węgrom, skarga nr 42461/13 i 44357/13, § 144; z dnia 8 lipca 1999 r. w sprawie Sürek przeciwko Turcji (nr 1), skarga nr 26682/95, § 61; z dnia 3 listopada 2015 r. w sprawie Stankiewicz i in. przeciwko Polsce, skarga nr 48053/11, § 34; z dnia 20 marca 2018 r. w sprawie Falzon przeciwko Malcie, skarga nr 45791/13, § 58 (dalej: Wyrok ETPC w sprawie Falzon przeciwko Malcie).

¹⁰ Wyrok SN z dnia 21 kwietnia 2021 r., I NSNC 89/20, OSNKN 2021, nr 3, poz. 23.

kontroli organów realizujących zadania publiczne – formułować twierdzenia i oceny dotyczące ich działalności¹¹. Sąd Najwyższy zwrócił uwagę, że:

treść, jak i okoliczności wypowiedzi, która stała się przyczyną procesu, w całości dotyczyły kontroli społecznej działalności podmiotów publicznych, jawności życia publicznego i społecznej kontroli nad działaniami władzy. W tych okolicznościach sprowadzenie całego sporu jedynie do czysto cywilistycznego wymiaru ochrony dóbr osobistych, prowadziłoby do całkowitego pominięcia, pierwszoplanowych w tej sprawie, gwarancji prowadzenia swobodnej publicznej debaty nad zagadnieniami istotnymi dla życia publicznego w Rzeczypospolitej Polskiej¹².

Deбата publiczna stanowić może zatem okoliczność przesądającą o zakresie i zasadach zastosowania przesłanek uchylających bezprawność i winę po stronie autora wypowiedzi. Niebagatelny wydaje się jednak temat debaty publicznej. Nie chodzi zatem o drobne, incydentalnie toczące się spory, których tłem są interesy polityczne, gospodarcze lub społeczne spierających się stron, ale problemy ważkie z punktu widzenia przemian ustrojowych w kraju oraz historii państwa i narodu. Sąd Najwyższy zauważył bowiem, że „spór, jaki legł u podstaw procesu zakończony wyrokiem poddanym kontroli nadzwyczajnej, ma istotne znaczenie dla dyskusji o historii przemian demokratycznych w Polsce”. W konsekwencji, co podkreślił Sąd Najwyższy, „rozpatrywanie tego zagadnienia jedynie w perspektywie art. 23 i 24 k.c., jako przykładu publicznej krytyki osoby prywatnej, w sytuacji, gdy krytyka odnosiła się w pierwszej kolejności do decyzji organu administracji publicznej, prowadziłoby do całkowitego zlekceważenia konstytucyjnych gwarancji wolności słowa i tym samym do naruszenia art. 54 Konstytucji RP i to w stopniu rażącym”¹³.

Szczególną rolę w inicjowaniu i prowadzeniu debaty publicznej ETPC i sądy krajowe przypisywały do niedawna prasie i dziennikarzom, upatrując w nich publicznego kontrolera i stróża interesu publicznego. Dla opisan

¹¹ Wyrok SN z dnia 21 kwietnia 2021 r., I NSNc 89/20, OSNKN 2021, nr 3, poz. 23.

¹² Tamże, pkt 17 uzasadnienia wyroku SN z dnia 21 kwietnia 2021 r., I NSNc 89/20, OSNKN 2021, nr 3, poz. 23.

¹³ Tamże, pkt 18 uzasadnienia wyroku SN z dnia 21 kwietnia 2021 r., I NSNc 89/20, OSNKN 2021, nr 3, poz. 23.

szczególnej doniosłości prasy i – szerzej – mediów dla właściwego funkcjonowania społeczeństwa demokratycznego Trybunał zaczął używać określenia publicznego stróża (ang. *public watchdog*)¹⁴. Status ten z czasem zaczął być rozciągany również na inne kategorie podmiotów, które pełnią analogiczne funkcje dla debaty publicznej i kontroli społecznej¹⁵. W pierwszej kolejności kategorię „public watchdog” poszerzono o organizacje pozarządowe zajmujące się kontrolą organów władzy¹⁶, ale również na naukowców i osoby publikujące na tematy istotne dla debaty publicznej. Wraz z rozwojem środków komunikacji status ten przypisuje się również internetowym bloggerom oraz szczególnie popularnym użytkownikom mediów społecznościowych, których funkcja w debacie publicznej nakazuje odnosić do nich intensywniejszą ochronę z tytułu obowiązywania art. 10 EKPC, przypisywaną właśnie kategorii podmiotów określanych mianem „public watchdogs”¹⁷. Nie chodzi jednak o jakiegokolwiek wypowiedzi tych podmiotów, ale o te, które ściśle wiążą się z zapewnieniem jawności życia publicznego i swobody debacie publicznej. W odniesieniu do tej grupy podmiotów okolicznością wyłączającą bezprawność działania jest należyta staranność, działanie w dobrej wierze, przy czym w takim przypadku nie zachodzi konieczność wykazania, że postawione zarzuty były prawdziwe¹⁸.

W odniesieniu do osób, które nie posiadają statusu dziennikarza i nie zostały zaliczone do grup podmiotów, których działalność *ex lege* identyfikowana była

¹⁴ Wyroki ETPC: z dnia 21 lipca 2015 r. w sprawie Satakunnan Markkinapörssi Oy i Satamedia Oy przeciwko Finlandii, skarga nr 931/13, § 126; w sprawie Bédat przeciwko Szwajcarii, § 51; z dnia 7 lutego 2012 r. w sprawie Axel Springer AG przeciwko Niemcom, skarga nr 39954/08, § 79 (dalej: Wyrok ETPC w sprawie Axel Springer AG przeciwko Niemcom); z dnia 26 kwietnia 1991 r. w sprawie The Sunday Times przeciwko Wielkiej Brytanii (nr 2), skarga nr 6538/74, § 50; w sprawie Bladet Tromsø i Stensaas przeciwko Norwegii, §§ 59 i 62; w sprawie Pedersen i Baadsgaard przeciwko Danii, § 71.

¹⁵ Spostrzeżenie to zostało poczynione przez Sąd Najwyższy w wyroku SN z dnia 21 kwietnia 2021 r., I NSNc 89/20, OSNKN 2021, nr 3, poz. 23 pkt 3.

¹⁶ Wyroki ETPC: z dnia 22 kwietnia 2013 r. w sprawie Animal Defenders International przeciwko Wielkiej Brytanii, skarga nr 48876/08, § 103; z dnia 27 czerwca 2017 r. w sprawie Medžlis Islamske Zajednice Brčko i in. przeciwko Bośni i Hercegowinie, skarga nr 17224/11, § 86.

¹⁷ Wyrok ETPC z dnia 8 listopada 2016 r. Magyar Helsinki Bizottság przeciwko Węgrom, skarga nr 18030/11, § 168.

¹⁸ Wyroki ETPC: z dnia 28 września 1999 r. w sprawie Dalban przeciwko Rumunii, skarga nr 28114/95 (dalej: Wyrok ETPC w sprawie Dalban przeciwko Rumunii), w sprawie Bladet Tromsø i Stensaas przeciwko Norwegii.

z realizacją interesu publicznego (organizacje NGO, naukowcy), stosowano, tak na gruncie EKPC, jak również na gruncie krajowego orzecznictwa, podwyższone rygory oceny dopuszczalności uchylenia się od odpowiedzialności za treść lub formę rozgłoszonej wypowiedzi.

EKPC nie omieszczał zwrócić uwagi na istniejące, także w Polsce, podwójne standardy ochrony wolności wypowiedzi. ETPC w sprawie Braun przeciwko Polsce¹⁹ uznał za niedopuszczalną praktykę, która polega na stosowaniu odmiennego katalogu kontratypów w odniesieniu do dziennikarzy i pozostałych uczestników debaty publicznej. Trybunał zauważył, że Sąd Najwyższy dokonał rozróżnienia standardów obowiązujących dziennikarzy od tych mających zastosowanie do innych uczestników debaty publicznej. Uczynił tak, nie badając, czy takie rozróżnienie jest zgodne z art. 10 Konwencji. Zdaniem Sądu Najwyższego, które ETPC przywołał w orzeczeniu, zasady należytej staranności i dobrej wiary powinny być stosowane tylko do dziennikarzy, którzy wypełniają szczególnie ważną funkcję społeczną. ETPC stanowisko to zakwestionował. Podobnie nie zgodził się z poglądem Sądu Najwyższego, że pozostałe osoby są zobowiązane do spełnienia wyższego standardu również przez to, że powinny udowodnić prawdziwość swoich twierdzeń (zobacz punkt 22 powyżej). W takim przypadku kwestia należytej staranności będzie brana pod uwagę wyłącznie przy ustalaniu ich winy, jako przesłanki odpowiedzialności. W niniejszej sprawie sądy krajowe uznały, że skarżący należy do tej drugiej kategorii, a w związku z tym, że nie był w stanie udowodnić prawdziwości swojego twierdzenia, uznano, że naruszył dobra osobiste powoda. Rząd i sądy krajowe twierdziły, że skarżący nie jest dziennikarzem. Z drugiej strony skarżący podkreślał, że od wielu lat pozostaje aktywnym, profesjonalnym dziennikarzem. Trybunał zauważył, że skarżący jest historykiem, autorem artykułów prasowych i programów telewizyjnych, a także aktywnie i publicznie wypowiadał się na temat spraw bieżących. Jako dziennikarz został zaproszony do udziału w programie radiowym na temat lustracji. Niemniej jednak uznano, że wypowiedź skarżącego miała charakter prywatny. Trybunał zauważył, że przy ocenie legalności działań skarżącego Sąd Najwyższy nie odniósł się do kwestii, czy skarżący był zaangażowany w debatę publiczną.

¹⁹ Wyrok ETPC z dnia 4 listopada 2014 r w sprawie Braun przeciwko Polsce, skarga nr 30162/10 (dalej: Wyrok ETPC w sprawie Braun przeciwko Polsce).

Trybunał uznał, że skarżący w rozpatrywanej sprawie był wyraźnie zaangażowany w debatę publiczną na temat ważnej kwestii. W związku z tym Trybunał stwierdził, że nie może zaakceptować podejścia sądów krajowych, które wymagają od skarżącego udowodnienia prawdziwości swoich twierdzeń. W świetle orzecznictwa Trybunału i okoliczności sprawy nie było uzasadnione wymaganie od skarżącego spełnienia standardów bardziej wymagających niż należyta staranność tylko na tej podstawie, że prawo krajowe nie uznało go za dziennikarza. Sądy krajowe, stosując takie podejście, skutecznie pozbawiły skarżącego ochrony przyznanej na mocy art. 10²⁰.

Sądy krajowe w późniejszym orzecznictwie coraz częściej uwzględniały stanowisko ETPC, a tym samym rozszerzając stosowały wyrażoną w uchwale (7) w 2005 r. zasadę, zgodnie z którą:

Wykazanie przez dziennikarza, że przy zbieraniu i wykorzystaniu materiałów prasowych działał w obronie społecznie uzasadnionego interesu oraz wypełnił obowiązek zachowania szczególnej staranności i rzetelności, uchyla bezprawność działania dziennikarza²¹.

Zasada ta coraz częściej znajduje bowiem zastosowanie nie tylko wobec dziennikarzy, lecz także innych osób, o ile biorą one aktywnie udział w debacie publicznej na ważne tematy budzące powszechne zainteresowanie²².

Fakt inicjowania i prowadzenia debaty publicznej oddziałuje na wyrażane w orzecznictwie stanowisko nie tylko w ten sposób, że ukierunkowuje sposób i zakres stosowania przesłanek wyłączających odpowiedzialność prawną

²⁰ W uzasadnieniu wyroku ETPC wskazał, że nie jest powołany do przesądzenia, czy skarżący w niniejszej sprawie oparł się na dostatecznie dokładnych i wiarygodnych informacjach. Nie będzie również decydować, czy podstawa faktyczna, na której oparł się skarżący, uzasadniała charakter i stopień poważnego zarzutu, jaki skierował. To zadanie sądów krajowych, które co do zasady są w stanie lepiej ocenić okoliczności faktyczne sprawy. Jednak przy podejmowaniu tych kwestii sądy krajowe muszą przestrzegać standardów wolności wypowiedzi zawartych w Konwencji (zob. Wyrok ETPC w sprawie Braun przeciwko Polsce, pkt 49).

²¹ Uchwała SN z dnia 18 lutego 2005 r., III CZP 53/04, OSNC 2005, nr 7–8, poz. 114.

²² Stanowisko takie zawarto m.in. w orzeczeniach: Postanowienie SN z dnia 30 listopada 2022 r. I CSK 3650/22, LEX nr 3559545; Wyrok SN z dnia 25 listopada 2022 r., II CSKP 246/22, OSNC 2023, nr 6, poz. 61.

autora wypowiedzi, ale także przesądzać o udzieleniu albo braku udzielenia ochrony naruszcicielowi.

Deбата publiczna zyskuje na gruncie prawa europejskiego status wartości samoistnie chronionej. Dowodzą tego prace podjęte w Komisji i Parlamencie Europejskim nad tekstem dyrektyw w sprawie ochrony osób, które angażują się w debatę publiczną, przed ewidentnie bezpodstawnymi lub stanowiącymi nadużycie postępowaniami sądowymi („strategiczne powództwa zmierzające do stłumienia debaty publicznej”)²³. W treści uzasadnienia wniosku Komisji Europejskiej kierowanego do PE o przyjęcie dyrektywy wskazuje się, że „prawidłowo funkcjonująca i rozwijająca się demokracja wymaga, aby obywatele mogli aktywnie uczestniczyć w debacie publicznej bez nieuprawnionej ingerencji ze strony organów publicznych lub innych potężnych grup interesu. Ewidentnie bezpodstawne lub stanowiące nadużycie postępowania sądowe zmierzające do stłumienia debaty publicznej (często określane również mianem strategicznych powództw zmierzających do stłumienia debaty publicznej lub SLAPP) są zjawiskiem obserwowanym w Unii Europejskiej od niedawna, ale wraz z upływem czasu stają się coraz powszechniejsze. Stanowią one szczególnie szkodliwą formę nękania i zastraszania stosowaną przeciwko osobom działającym na rzecz ochrony interesu publicznego. Postępowania te są bezpodstawnymi lub wyolbrzymionymi postępowaniami sądowymi wszczynanymi zazwyczaj przez wpływowe osoby fizyczne, grupy lobbystyczne, korporacje i organy państwowe przeciwko stronom wyrażającym krytyczne opinie lub przekazującym komunikaty niewygodne dla powodów w sprawie leżącej w interesie publicznym. Celem takich postępowań jest cenzurowanie, zastraszanie i uciszanie krytyków poprzez obciążenie ich kosztami obrony prawnej, dopóki nie zrezygnują z krytyki lub sprzeciwu. W odróżnieniu od standardowych postępowań, powództw typu SLAPP nie wytacza się w celu wykonania prawa dostępu do wymiaru sprawiedliwości, wygrania postępowania sądowego ani dochodzenia roszczeń. Zamiast tego służą one zastraszeniu pozwanych i pozbawieniu ich zasobów. Nadrzędnym

²³ Wniosek KE dnia 27 kwietnia 2022 r. Dyrektywa Parlamentu Europejskiego i Rady w sprawie ochrony osób, które angażują się w debatę publiczną, przed ewidentnie bezpodstawnymi lub stanowiącymi nadużycie postępowaniami sądowymi („strategiczne powództwa zmierzające do stłumienia debaty publicznej”); <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52022PC0177> (dostęp: 10.06.2024).

celem tego rodzaju postępowań jest wywołanie efektu mrozącego, uciszenie pozwanych i zniechęcenie ich do kontynuowania prowadzonej przez nich działalności²⁴. Wzmocnione gwarancje ochrony przeciwko bezpodstawnym powództwom Komisja Europejska przewiduje także dla dziennikarzy²⁵. Miałyby one zostać zawarte nie tylko w dyrektywie w sprawie SLAPP, lecz także w europejskim akcie o wolności mediów²⁶.

W art. 3 projektu dyrektywy w sprawie SLAPP zawarta została propozycja definicji terminu „debatę publiczną”. Debatę publiczną definiuje się szeroko jako dowolne oświadczenie lub działanie wyrażone lub zrealizowane w ramach:

1. wykonywania prawa do wolności wypowiedzi i informacji, w tym tworzenia, wystawiania, reklamowania lub innego promowania komunikatów, publikacji lub utworów o charakterze dziennikarskim, politycznym, naukowym, akademickim, artystycznym, komentatorskim lub satyrycznym, a także działania przygotowawcze, wspierające lub wspomagające bezpośrednio związane z takimi oświadczeniami lub działaniami;
2. wykonywania prawa do wolności zrzeszania się i pokojowego gromadzenia się, np. organizowanie działań lobbingsowych, demonstracji i protestów lub działań wynikających z wykonywania prawa do dobrej

²⁴ Zachęca się państwa członkowskie do dokonania przeglądu ich sytuacji krajowej, aby zagwarantować, że w ich mających zastosowanie ramach prawnych przewidziano gwarancje niezbędne do radzenia sobie z powództwami typu SLAPP przy pełnym poszanowaniu praw podstawowych, uwzględniając prawo do wolności wypowiedzi, prawo dostępu do wymiaru sprawiedliwości oraz prawo do ochrony danych osobowych i wartości demokratycznych. Państwa członkowskie zachęca się również do zawarcia w ich prawie krajowym gwarancji odnoszących się do spraw krajowych podobnych do gwarancji przewidzianych w instrumentach unijnych, które mają na celu przeciwdziałanie ewidentnie bezpodstawnym lub stanowiącym nadużycie postępowaniom w sprawach cywilnych o skutkach transgranicznych. Państwom członkowskim zaleca się m.in. zniesienie kar pozbawienia wolności w sprawach o zniesławienie, a także popieranie prowadzenia postępowań w tym zakresie na gruncie prawa administracyjnego lub cywilnego, a nie na gruncie prawa karnego, pod warunkiem że odpowiednie przepisy mają mniej represyjny skutek i że w przepisach prawa administracyjnego wykluczono możliwość stosowania jakichkolwiek form pozbawienia wolności (zob. tamże, pkt 1).

²⁵ *Komisja zajmuje się problemem nadużywania powództw przeciwko dziennikarzom i obrońcom praw człowieka (powództw typu SLAPP)*, 27.04.2022, Komisja Europejska, https://ec.europa.eu/commission/presscorner/detail/pl/ip_22_2652 (dostęp: 10.06.2024).

²⁶ *Pytania i odpowiedzi: europejski akt o wolności mediów*, 21.12.2023, Komisja Europejska, https://ec.europa.eu/commission/presscorner/detail/pl/qanda_22_5505 (dostęp: 10.06.2024).

administracji i prawa do skutecznego środka odwoławczego, takich jak składanie skarg, petycji lub skarg administracyjnych i powództw, lub udział w wyżej wymienionych działaniach, udział w wysłuchaniach publicznych, a także działania przygotowawcze, wspierające lub wspomagające bezpośrednio związane z takimi oświadczeniami lub działaniami.

Debata publiczna obejmuje ponadto inne działania mające na celu informowanie opinii publicznej lub wywieranie na nią wpływu lub wspieranie działań realizowanych przez społeczeństwo, w tym działania podejmowane przez jakiegokolwiek podmiot prywatny lub publiczny w związku z kwestią leżącą w interesie publicznym, takie jak organizowanie badań, sondaży, kampanii lub wszelkich innych działań zbiorowych lub uczestnictwo w nich, a także działania przygotowawcze, wspierające lub wspomagające bezpośrednio związane z takimi działaniami²⁷. Zastrzega się zarazem, że debata publiczna nie powinna zazwyczaj obejmować komercyjnej działalności reklamowej i marketingowej (wypowiedzi o charakterze handlowym)²⁸.

Sprawę leżącą w interesie publicznym definiuje się również szeroko w odniesieniu do wszelkich kwestii, które:

mają wpływ na społeczeństwo w takim stopniu, że mogą one z uzasadnionych względów wzbudzić jego zainteresowanie w takich dziedzinach, jak na przykład zdrowie publiczne, bezpieczeństwo, środowisko, klimat lub korzystanie z praw podstawowych²⁹.

Fakt udziału w debacie publicznej może zatem stanowić usprawiedliwienie dla treści podnoszonych zarzutów choćby zawarte w wypowiedzi twierdzenia stanowiły dolegliwą ingerencję w dobra osobiste osoby, której dotyczy wypowiedź. Niemniej znaczenie, jakie przypisuje się debacie publicznej, nie przesądza o usprawiedliwieniu rozgłoszenia każdej wypowiedzi, lecz tylko takiej, która służy interesowi publicznemu. O ile na gruncie orzecznictwa ETPC

²⁷ Wniosek dnia 27 kwietnia 2022 Dyrektywa Parlamentu Europejskiego i Rady w sprawie ochrony osób, które angażują się w debatę publiczną, przed ewidentnie bezpodstawnymi lub stanowiącymi nadużycie postępowaniami sądowymi („strategiczne powództwa zmierzające do stłumienia debaty publicznej”), s. 13, <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52022PC0177> (dostęp: 10.06.2024).

²⁸ Tamże, s. 13.

²⁹ Tamże, s. 14.

i sądów krajowych istotne znaczenie dla oceny dopuszczalności wypowiedzi miało ustalenie zarówno statusu autora wypowiedzi, jak i statusu pokrzywdzonego, w szczególności wówczas, gdy była nim osoba pełniąca funkcje publiczne, to na gruncie projektu dyrektywy w sprawie SLAPP szczególne ważna jest tematyka debaty publicznej, ponieważ tylko wówczas, gdy przedmiot wypowiedzi jest ważki dla społeczeństwa i państwa, autor wypowiedzi może liczyć na zastosowanie złagodzonych rygorów ponoszenia odpowiedzialności, a nawet – jak proponuje się w dyrektywie w sprawie SLAPP – umarzanie postępowań sądowych o naruszenie dóbr osobistych albo „wczesne oddalenie ewidentnie bezpodstawnego powództwa” (art. 9 projektu dyrektywy w sprawie SLAPP).

Proponuje się, by sankcja polegająca na „wczesnym oddaleniu ewidentnie bezpodstawnego powództwa”, która skutkuje powstaniem stanu rzeczy osądzonej (*res iudicata*), była stosowana wówczas, gdy powód, wytaczając postępowanie, nadużył prawa. W projekcie dyrektywy wskazuje się, że konstrukcja:

nadużycia postępowań sądowych zmierzających do stłumienia debaty publicznej odnosi się do postępowań sądowych wszczynanych w związku z debatą publiczną, które są w całości lub częściowo bezpodstawne, a ich głównym celem jest uniemożliwianie lub ograniczanie debaty publicznej lub karanie za debatę publiczną. Niewyczerpujący wykaz obejmuje najczęstsze oznaki nadużycia, takie jak nieproporcjonalny, nadmierny lub nieuzasadniony charakter powództwa lub jego części, fakt wszczęcia przez powoda lub podmioty powiązane wielu postępowań w związku z podobnymi sprawami lub zastraszanie, nękanie lub groźby ze strony powoda lub jego przedstawicieli³⁰.

Kierunek projektowanych rozwiązań wskazuje, że przesądzające dla oceny charakteru wypowiedzi, a w konsekwencji przypisania odpowiedzialności za

³⁰ Wskazuje się, że postępowania sądowe stanowiące nadużycie często obejmują taktyki procesowe stosowane w złej wierze, takie jak opóźnianie postępowań, narażanie pozwanego na nieproporcjonalnie wysokie koszty postępowania lub wybór sądu ze względu na możliwość korzystniejszego rozstrzygnięcia sprawy. Takie taktyki, stosowane przez powoda w celach innych niż uzyskanie dostępu do wymiaru sprawiedliwości, często – chociaż nie zawsze – są połączone z różnymi formami zastraszania, nękania lub gróźb przed rozpoczęciem postępowania lub w jego toku mającymi na celu utrudnienie debaty publicznej (zob. tamże, s. 15).

treść lub formę wypowiedzi, nie będzie ustalenie statusu autora wypowiedzi (podmiot publiczny/podmiot prywatny) ani forum, w którego ramach została wygłoszona wypowiedź, lecz istotne znaczenie będzie mieć temat wypowiedzi i jego związek z interesem publicznym. Zarówno zatem wypowiedzi pochodzące od osób, które nie pełnią funkcji publicznych, jak i takie, które zostały rozgłoszone w miejscach publicznych, a także rozpowszechnione za pomocą środków społecznego komunikowania, w tym mediów elektronicznych (internet), będą mogły – w myśl projektu dyrektywy i kierunku orzecznictwa ETPC oraz sądów krajowych – zostać objęte ochroną. Skutkiem proponowanych rozwiązań, o ile wejdą w życie, byłoby niewątpliwie wzmocnienie pozycji procesowej autorów wypowiedzi. Powyższe instrumenty, jak należy przewidywać, mogą wywierać wpływ na kształt europejskiego standardu wolności wypowiedzi przede wszystkim w jego ujęciu proceduralnym. W roli skarżących naruszenie wolności wypowiedzi (art. 10 EKPC) będą występować – częściej niż do tej pory – osoby, których powództwa zostały oddalone na wczesnym etapie postępowania ze względu na nadużycie prawa polegające na tłumieniu debaty publicznej.

Wobec powyższych spostrzeżeń niezbędne wydaje się ustalenie, jakie rodzaje wypowiedzi zarówno publicznych, jak i prywatnych, a także wypowiedzi anonimowych mogą zostać objęte intensywną ochroną i nadto jakiego rodzaju musi istnieć związek między tymi wypowiedziami a interesem publicznym.

A. Wypowiedź publiczna

Wypowiedź publiczna to każda wypowiedź, z którą może zapoznać się nieograniczony krąg osób, a autor wypowiedzi ze względu na forum, na jakim została ona rozpowszechniona, nie jest władny ograniczyć do niej dostępu. Bez znaczenia jest zatem, co do zasady, temat wypowiedzi i jego związek z interesem publicznym. Nie jest także istotny status jej autora. W orzecznictwie europejskim, a także w treści judykatów krajowych pojęcie wypowiedzi publicznej jest używane w sposób automatyczny i obejmuje grupę wypowiedzi niejednorodnych zarówno pod względem znaczenia, powszechności dostępu czy autorstwa, jak i tematyki.

Spośród wypowiedzi publicznych wyodrębnić można grupę, której dotyczą powyżej wskazane cechy i obejmuje ona wypowiedzi stanowiące element debaty publicznej, a z tego powodu objęta jest dalej idącą ochroną niż pozostałe wypowiedzi publiczne. Przyjmując zatem, że jednym z kryteriów klasyfikacji wypowiedzi, istotnym (relevantnym) z tego powodu, że pozwala na wyodrębnienie kategorii wypowiedzi objętych dalej idącą ochroną prawną, jest ich znaczenie dla debaty publicznej. Ustalenie znaczenia wypowiedzi dla debaty publicznej wymaga powiązania wypowiedzi z realizacją celu, jakiemu ona służy. W konsekwencji stwierdzenie, że wypowiedź realizuje cele interesu publicznego przesądza o przyznaniu jej statusu dobra objętego ochroną prawa.

Związek z interesem publicznym może następować poprzez temat wypowiedzi, jej autora, forum, na którym została wygłoszona wypowiedź, ale także ze względu na jej formę albo kontekst. Zarazem istnienie związku wypowiedzi z interesem publicznym ma istotne znaczenie dla oceny zarówno jej dopuszczalności, jak i zakresu odpowiedzialności za jej treść i formę. Powyżej wskazane elementy zapewniające łączność wypowiedzi z interesem publicznym przesądzają także o jej charakterze jako wypowiedzi publicznej.

Próbę dookreślenia pojęcia „interesu publicznego” ETPC podjął w sprawie Couderc i Hachette Filipacchi Associés przeciwko Francji³¹. Trybunał stwierdził wówczas, że „interes publiczny dotyczy spraw, które wywierają wpływ na ogół w takim stopniu, że ogół może w sposób uprawniony się nimi interesować, które przykuwają uwagę ogółu lub w znacznym stopniu go dotyczą”³², szczególnie w tym zakresie, że wywierają wpływ na dobrobyt obywateli lub życie społeczności³³. Powyższe dotyczy także spraw, które mogą budzić istotne kontrowersje, a odnoszących się do ważnej kwestii społecznej³⁴. Próbując uchwycić prawidłowość zmian zachodzących w wyrażanym przez ETPC stanowisku, należy zwrócić uwagę, że Trybunał odchodzi od stosowania kryterium podmiotowego (kto jest autorem wypowiedzi,

³¹ Wyrok ETPC z dnia 10 listopada 2015 r. w sprawie Couderc i Hachette Filipacchi Associés przeciwko Francji, skarga nr 40454/07.

³² Podobnie w: wyrok ETPC w sprawie The Sunday Times przeciwko Wielkiej Brytanii (nr 1).

³³ Wyrok ETPC z dnia 25 marca 1985 r. w sprawie Barthold przeciwko Niemcom, skarga nr 8734/79 (dalej: Wyrok ETPC w sprawie Barthold przeciwko Niemcom).

³⁴ Wyrok ETPC z dnia 10 lipca 2012 r. w sprawie Erla Hlynssdóttir przeciwko Islandii, skarga 43380/10, § 62.

czy autorem jest dziennikarz, czy wypowiedź została opublikowana w prasie) na rzecz kryterium przedmiotowego – czego dotyczy wypowiedź, jaką ma wagę, a w szczególności, czy jest to wypowiedź o sprawach budzących powszechne zainteresowanie, czy o sprawach mających publiczne znaczenie³⁵. Trybunał nadal posługuje się zatem pojęciem *questions d'intérêt général*, jednak dokonuje innej jego interpretacji³⁶. Należy podkreślić, że posługiwanie się pojęciem *questions d'intérêt général* musiało prowadzić do niespójnych, a czasami nawet sprzecznych ustaleń. Mogło ono być bowiem interpretowane jako „sprawa mająca publiczne znaczenie”, jak również „sprawa budząca powszechne zainteresowanie”.

Cecha ta stanowi najważniejsze kryterium przedmiotowe, którym posługuje się Trybunał, oceniając wypowiedzi i kwalifikując niektóre z nich do kategorii wypowiedzi publicznych. Wydaje się, że kryterium to może być traktowane jako szersze ujęcie pojęcia debaty publicznej w znaczeniu nadanym

³⁵ Wypowiedź klasyfikowana przez Trybunał jako publiczna powinna poruszać kwestie „rodzące publiczne zainteresowanie i mające publiczne znaczenie”. Trybunał operuje sformułowaniem „*question d'interet general*” (ang. *matters of public interest*), które – jak słusznie zauważa I.C. Kamiński – może mieć dwojakie znaczenie. Francuskie słowo „interet”, podobnie jak angielskie „interest” może być bowiem tłumaczone zarówno jako „zainteresowanie”, jak i jako „znaczenie”. I.C. Kamiński podkreśla, że w orzecznictwie Trybunału nie chodzi jednak o „empiryczne”, rzeczywiste zainteresowanie społeczeństwa jakimiś sprawami, lecz zainteresowanie „normatywne”, tzn. rangę zagadnień wynikającą z ich związku z pojęciem demokratycznego społeczeństwa (zob. I.C. Kamiński, *Swoboda wypowiedzi...*, s. 171). Kryterium przedmiotowe znalazło zastosowanie w sprawach Zybertowicz przeciwko Polsce (wyrok z dnia 17 stycznia 2017 r., skarga nr 59138/10); Sanocki przeciwko Polsce (wyrok z dnia 17 lipca 2007 r., skarga nr 28949/03); Kurski przeciwko Polsce (wyrok z dnia 5 lipca 2016 r., skarga nr 26115/10).

³⁶ W ocenie ETPC nie jest dopuszczalne powołanie się przez prasę na realizację interesu publicznego wówczas, gdy materiał prasowy służy wyłącznie zaspokojeniu ciekawości pewnej grupy odbiorców odnośnie do faktów z życia prywatnego innych osób. Ustalenie tej okoliczności pozwala Trybunałowi na stwierdzenie, że nie doszło do naruszenia art. 10 EKPC i oddalenie skargi wniesionej przez dziennikarzy lub wydawcę nawet wówczas, gdy sądy krajowe nakazały skarżącym przeproszenie pokrzywdzonych i zapłatę na ich rzecz odszkodowania (zob. orzeczenia: z dnia 1 lipca 2003 r. w sprawie Société Prisma Presse przeciwko Francji, skarga nr 71612/01; z dnia 12 grudnia 2000 r. w sprawie Jaime Campmany y Diez de Revenga i Juan Luís Lopez-Galiacho Perona przeciwko Hiszpanii, skarga nr 54224/00; z dnia 13 maja 2003 r. w sprawie Julio Bou Gibert i El Hogar y La Moda J.A. przeciwko Hiszpanii, skarga nr 14929/02; z dnia 4 czerwca 2009 r. w sprawie Standard Verlags GmbH przeciwko Austrii (nr 2), skarga nr 21277/05).

mu w dokumentach Zgromadzenia Parlamentarnego Rady Europy³⁷. Trybunał przyjął bowiem, dokonując w ten sposób wykładni autentycznej swojego stanowiska, że nie ma podstaw, by wprowadzać rozróżnienie pomiędzy pojęciem dyskusji politycznej a debaty w innych sprawach budzących publiczne zainteresowanie³⁸.

Do spraw, które spełniły kryterium „publicznego zainteresowania i publicznego znaczenia”, zaliczone zostały zarówno wypowiedzi poddające krytyce sposób sprawowania władzy przez aparat państwowy³⁹, postępowanie polityków, funkcjonowanie legalnie działających instytucji, organizacji i stowarzyszeń⁴⁰, działania pracodawcy⁴¹, jak i funkcjonowanie nocnej opieki weterynaryjnej w mieście⁴² oraz efektywność i bezpieczeństwo przeprowadzania operacji plastycznych⁴³.

Okolicznością, która może przesądzić o zaliczeniu wypowiedzi do domeny publicznej, jest także opublikowanie jej w prasie. Należy przypuszczać, że pewne treści, poglądy i informacje nie uzyskałyby takiego statusu, gdyby nie ich publikacja. Oceniane w oderwaniu od tej okoliczności trudno

³⁷ Zalecenie 1407, *Media et culture democratique*, tekst przyjęty przez Zgromadzenie dnia 29 kwietnia 1999 r.; Zalecenie 1506, *Liberte d'expression et d'information dans les medias en Europe*, tekst przyjęty przez Zgromadzenie dnia 24 kwietnia 2001 r.; Rezolucja 1003, *Relative a l'ethique du journalisme*, tekst przyjęty przez Zgromadzenie dnia 1 lipca 1993 r.

³⁸ Wyrok ETPC z dnia 25 czerwca 1992 r. w sprawie Thorgeir Thorgeirson przeciwko Islandii, skarga nr 13778/88 (dalej: Wyrok ETPC w sprawie Thorgeir Thorgeirson przeciwko Islandii).

³⁹ Szereg spraw przeciwko Turcji, które przegrywa ona w związku z niedopuszczalną zdaniem Trybunału ingerencją w swobodę wypowiedzi osób poddających krytyce działania aparatu państwowego wobec mniejszości kurdyjskiej. Zob. Wyroki ETPC: z dnia 19 października 2004 w sprawie Varli i in. przeciwko Turcji, skarga nr 38586/97; z dnia 29 marca 2005 r. w sprawie Alinak przeciwko Turcji, skarga nr 40287/98 (dalej: Wyrok ETPC w sprawie Alinak przeciwko Turcji); z dnia 18 lipca 2000 r. w sprawie Sener przeciwko Turcji, skarga nr 26680/95. Trybunał nie tylko uznał działania władz za naruszenie Konwencji, lecz także wskazał na obowiązki pozytywne, jakie ciąży na organach władzy państwowej w celu ochrony toczącej się debaty publicznej w ważnych kwestiach społecznych. Zob. Wyrok ETPC z dnia 16 marca 2000 r. w sprawie Ozgur Gundem przeciwko Turcji, skarga nr 23144/93 (dalej: Wyrok ETPC w sprawie Ozgur Gundem przeciwko Turcji).

⁴⁰ Wyrok ETPC z dnia 27 lutego 2001 r. w sprawie Jerusalem przeciwko Austrii, skarga nr 26958/95 (dalej: Wyrok ETPC w sprawie Jerusalem przeciwko Austrii).

⁴¹ Wyrok ETPC w sprawie Fuentes Bobo przeciwko Hiszpanii.

⁴² Wyrok ETPC w sprawie Barthold przeciwko Niemcom.

⁴³ Wyrok z dnia 2 maja 2000 r. w sprawie Bergens Tidende i in. przeciwko Norwegii, skarga nr 26132/95 (dalej: Wyrok ETPC w sprawie Bergens Tidende przeciwko Norwegii).

byłoby uznać za „wzbudzające publiczne zainteresowanie i mające publiczne znaczenie”⁴⁴.

Sprawy budzące powszechne zainteresowanie obejmują wiedzę nie tylko o zdarzeniach, lecz także osobach, w szczególności osobach pełniących funkcje publiczne. Wolność wypowiedzi na temat osób publicznych podlega intensywniejszej ochronie prawnej niż w odniesieniu do osób prywatnych⁴⁵. Europejski Trybunał Praw Człowieka wielokrotnie podkreślał, że status prawa do otwartej i nieskrępowanej debaty publicznej także wówczas, gdy wypowiedzi ingerują w dobra osobiste osób pełniących funkcje publiczne, stanowi jedną z podstawowych wartości państwa demokratycznego, a nawet, że jest rdzeniem społeczeństwa demokratycznego⁴⁶.

Ustawodawca nie określił wprost definicji terminu „osoba publiczna”, ale także w żaden sposób nie ograniczył zakresu jego stosowania, trzeba zatem przyjąć, że należy je wyklądać szeroko. Pojęcie osoby publicznej obejmuje niewątpliwie osoby, które stały się albo mogą stać się rozpoznawalne, w szczególności dlatego, że same rozpowszechniły swój wizerunek, co pozwala na identyfikowanie ich z prowadzoną przez nie działalnością publiczną. Do kategorii tej należą zatem osoby będące funkcjonariuszami publicznymi wykonującymi zadania publiczne, zwłaszcza gdy pozostają w czynnej służbie i podejmują czynności służbowe w miejscu publicznym, a świadkami (obserwatorami) tych czynności może być nieograniczony krąg odbiorców (każdy). Nadto wówczas, gdy zarówno ze względu na rodzaj czynności, jak i zasady oraz okoliczności ich wykonywania budzą one powszechne zainteresowanie, a skutki ich działań lub zaniechań wpływają na funkcjonowanie społeczeństwa.

Pojęcie osoby publicznej, którym posługuje się doktryna i orzecznictwo, jest skorelowane z pojęciem osoby powszechnie znanej użytym w treści art. 81

⁴⁴ W taki sposób można byłoby potraktować informacje o problemach pacjentek po poddaniu się operacji plastycznej piersi (zob. sprawa Bergens Tidende przeciwko Norwegii). Publicznego znaczenia nie miałyby też, gdyby nie artykuł w prasie, kłopoty właścicielki schorowanego kota, która w nocy nie mogła znaleźć czynnej kliniki weterynaryjnej (sprawa Barthold przeciwko Niemcom).

⁴⁵ Wyrok TK z dnia 11 października 2006 r., P 3/06.

⁴⁶ Wyrok SN z dnia 30 czerwca 2017 r., I CSK 603/16 oraz wyroki ETPC: w sprawie Lingens przeciwko Austrii; w sprawie Castells przeciwko Hiszpanii, w sprawie Oberschlick przeciwko Austrii (nr 2).

ust. 2 pkt 1 ustawy o prawie autorskim i prawach pokrewnych⁴⁷. Ustalenie, czy daną osobę można uznać za osobę powszechnie znaną, nie wymaga wiadomości specjalnych i posiłkowania się opinią biegłego, nie jest bowiem ustaleniem okoliczności faktycznej, ale kwalifikacją prawną. Kwalifikacji tej powinien dokonać sąd orzekający merytorycznie w sprawie na podstawie własnej oceny ustalonych w sprawie okoliczności faktycznych⁴⁸.

Sama przynależność do grona osób powszechnie znanych nie oznacza jednak, że dana osoba jest osobą publiczną, a tym bardziej, że pełni ona funkcję publiczną albo jest funkcjonariuszem publicznym. W orzecznictwie pojawia się natomiast często prezentowane stanowisko, zgodnie z którym występujące łącznie dwie przesłanki – tj.: 1) okoliczność wskazująca na to, że dana osoba jest powszechnie znana, a zarazem 2) podjęła ona aktywność w sferze publicznej (prowadzi działalność publiczną) – wystarczają do tego, by danej osobie przyznać status osoby publicznej⁴⁹.

Dopuszczalność ujawnienia informacji dotyczących osoby publicznej wymaga dodatkowo ustalenia, że informacja, która ma zostać ujawniona, dotyczy aktywności danej osoby podjętej w związku z jej publiczną aktywnością. Ujawnienie informacji z życia prywatnego osoby prowadzącej działalność publiczną wymaga istnienia związku między tą działalnością a podawaną informacją. Konieczne jest zatem wykazanie zależności między zachowaniem danej osoby w sferze działalności publicznej, a jej zachowaniem w sferze prywatnej, przy czym nie chodzi o związek przypadkowy czy formalny. Ujawnienie takiej informacji powinno służyć ochronie konkretnego, społecznie uzasadnionego interesu, którego przemilczenie byłoby dla interesu publicznego szkodliwe⁵⁰.

Ustalenie statusu osoby publicznej następuje dwuetapowo. W pierwszej kolejności ocenie poddany zostaje charakter podjętej przez tę osobę

⁴⁷ Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, (t.j. Dz.U. z 2022 r. poz. 2509 – dalej: pr. aut.).

⁴⁸ Wyrok Sądu Apelacyjnego w Warszawie z dnia 6 lutego 2018 r., V ACa 1040/17, Legalis nr 1865625.

⁴⁹ J. Taczkowska-Olszewska, *Funkcjonariusz publiczny vs. Osoba pełniąca funkcje publiczne*, [w:] J. Taczkowska-Olszewska, A. Brzostek, K. Walczuk, *Status prawny funkcjonariusza publicznego. Ochrona-obowiązki-odpowiedzialność*, Warszawa 2020, s. 32.

⁵⁰ Wyrok Sądu Apelacyjnego w Warszawie z dnia 22 lutego 2018 r., I ACa 2187/16, Legalis nr 1760469.

aktywności, w tym oceniany jest stopień przyczynienia się tej osoby do rozpowszechnienia w sferze publicznej informacji o podjętym przez nią działaniu, a następnie oceniany jest stopień, w jakim osoba ta oddziałuje lub może oddziaływać w sferze publicznej. Ocenie podlega w szczególności stopień jej rozpoznawalności.

Należy podkreślić zarazem, że termin „osoba publiczna” – w przeciwieństwie do terminów „funkcjonariusz publiczny” i „osoba pełniąca funkcję publiczną” – nie ma legalnej definicji. Jest to termin wypracowany przez doktrynę i orzecznictwo, który ułatwia i systematyzuje stosowanie regulacji gwarantujących ochronę prywatności jednostki⁵¹.

Pojęcie funkcjonariusza publicznego ma znaczenie normatywne zarówno na gruncie krajowego, jak i ponadnarodowego systemu prawa. Należy przez to rozumieć, że sposób definiowania pojęcia „funkcjonariusza publicznego” w prawie stanowionym, w szczególności prawie cywilnym, karnym, jak i administracyjnym wywołuje skutek prawokształtujący, modelując w sposób odmienny sytuację prawną osób objętych zakresem tego pojęcia i różnicując ją względem sytuacji osób nieposiadających takiego statusu. Zarazem jednak w prawie ponadnarodowym pojęcie to jest używane często w sposób intuicyjny. Pomimo zatem powszechnego używania tego pojęcia, zarówno w treści aktów prawnych, jak i w orzecznictwie sądów i trybunałów międzynarodowych oraz wysiłków podejmowanych przez unijnego prawodawcę w kierunku doprecyzowania treści tego pojęcia, bywa ono różnorodnie interpretowane.

Na gruncie prawa ponadnarodowego termin ten jest rozumiany bardzo szeroko i obejmuje w szczególności osoby zatrudnione w instytucjach władzy publicznej, w tym pracowników umysłowych w publicznych instytucjach edukacyjnych, a także członków sił zbrojnych oraz przedstawicieli służb odpowiedzialnych za utrzymanie porządku i bezpieczeństwa publicznego⁵². Odwołując się do sposobu interpretowania tego pojęcia na gruncie prawa administracyjnego w ujęciu zaproponowanym w Traktatach Europejskich⁵³

⁵¹ J. Tackowska-Olszewska, *Funkcjonariusz publiczny...*, s. 35.

⁵² Na brak definicji legalnej pojęcia funkcjonariusza publicznego w regulacjach ponadnarodowych zwraca uwagę I.C. Kamiński (zob. I.C. Kamiński, *Ograniczenia swobody...*, s. 206).

⁵³ Traktat ustanawiający Europejską Wspólnotę Gospodarczą (Dz.U. z 2004 r. Nr 90, poz. 864/2 z późn. zm.). Artykuł 228 Traktatu o funkcjonowaniu Unii Europejskiej upoważnia Europejskiego Rzecznika Praw Obywatelskich do prowadzenia dochodzeń

oraz Karcie Praw Podstawowych⁵⁴, w szczególności art. 41 KPP gwarantującym prawo do dobrej administracji⁵⁵ oraz przyjętym przez Parlament Europejskim kodeksie dobrej praktyki administracyjnej, przyjąć należy, że organy UE uznają pojęcie funkcjonariusza publicznego za zakresowo zbieżne z pojęciem urzędnika. W art. 2 ust. 4 lit. b Europejskiego kodeksu dobrej praktyki administracyjnej wskazuje się, że „pojęcie »urzędnik« obejmuje urzędników i pozostałych funkcjonariuszy Unii Europejskiej”⁵⁶.

Oceniając status wypowiedzi, Europejski Trybunał Praw Człowieka posłużył się trzema rodzajami kryteriów: podmiotowym, przedmiotowym i celowościowym, dając niekiedy priorytet ostatniemu z nich. Wydaje się, że kryterium celowościowe, rozumiane jako prymat debaty publicznej nad rzetelną informacją, skłoniło Trybunał do uznania za uprawnione także takie informacje, które wprowadzają w błąd, i których nieprawdziwość została dowiedziona w toku postępowań toczących się przed sądami krajowymi⁵⁷. Kryterium celowościowe stosuje także Trybunał w odniesieniu do wypowiedzi publicznych dotyczących funkcjonariuszy oraz przedstawicieli wymiaru sprawiedliwości. W tych sytuacjach Trybunał uznaje często wyższość powagi

w zakresie niewłaściwego administrowania w instytucjach, organach, urzędach i agencjach unijnych, z wyjątkiem Trybunału Sprawiedliwości Unii Europejskiej w zakresie prowadzonych przez niego postępowań sądowych. Każdy obywatel Unii ma prawo zgłosić skargę do Rzecznika. Skargi mogą zgłaszać również rezydenci, przedsiębiorstwa i stowarzyszenia.

⁵⁴ Karta Praw Podstawowych.

⁵⁵ Zgodnie z art. 4 KPP: 1. Każdy ma prawo do bezstronnego i sprawiedliwego rozpatrzenia swojej sprawy w rozsądnym terminie przez instytucje, organy i jednostki organizacyjne Unii. 2. Prawo to obejmuje: a) prawo każdego do bycia wysłuchanym, zanim zostaną podjęte indywidualne środki mogące negatywnie wpłynąć na jego sytuację; b) prawo każdego do dostępu do akt jego sprawy, przy poszanowaniu uprawnionych interesów poufności oraz tajemnicy zawodowej i handlowej; c) obowiązek administracji uzasadniania swoich decyzji. 3. Każdy ma prawo domagania się od Unii naprawienia, zgodnie z zasadami ogólnymi wspólnymi dla praw państw członkowskich, szkody wyrządzonej przez instytucje lub ich pracowników przy wykonywaniu ich funkcji. 4. Każdy może zwrócić się pisemnie do instytucji Unii w jednym z języków Traktatów i musi otrzymać odpowiedź w tym samym języku.

⁵⁶ Europejski kodeks dobrej praktyki administracyjnej, <https://www.ombudsman.europa.eu/pl/publication/pl/3510> (dostęp: 10.06.2024).

⁵⁷ Zob Wyrok ETPC w sprawie Cumpănă i Mazăre przeciwko Rumunii; podobnie: Wyrok ETPC w sprawie Bladet Tromsø i Stensaas przeciwko Norwegii.

wymiaru sprawiedliwości oraz zaufania obywateli do państwa i wymiaru sprawiedliwości nad wartością, jaką jest publiczna debata⁵⁸.

Fakt udostępnienia przez autora szerokiemu gronu odbiorców własnej wypowiedzi albo zgoda na jej prezentację widzom, czytelnikom bądź słuchaczom daje zwykle podstawę do zakwalifikowania jej jako wypowiedzi publicznej. Stosowane kryterium publicznego udostępnienia wypływa z ustawy o prawie autorskim i prawach pokrewnych, która traktuje je jako jedno – obok prawa do integralności i do autorstwa – z triady fundamentalnych praw autorskich. Publiczne udostępnienie utworu za zgodą jego twórcy stanowi w rozumieniu prawa autorskiego kryterium decydujące o publicznym charakterze utworu. Prawo do publicznego udostępnienia utworu ma charakter jednorazowy⁵⁹.

Stanowisko orzecznictwa Europejskiego Trybunału Praw Człowieka dowodzi, że wypowiedź może nabrać publicznego charakteru nawet wówczas, gdy jej autor nie zamierzał prezentować jej publicznie. Okoliczność ta dotyczy autorów wypowiedzi posiadających status osób publicznych, jeśli ich wypowiedzi dotyczą wydarzeń publicznych lub mają związek z pełnioną przez nie funkcją. Ich publiczny charakter wypływa wówczas nie ze zgody autora na publiczne jej udostępnienie, lecz z cech tkwiących w treści i formie samej wypowiedzi, a także w osobie mówcy⁶⁰.

⁵⁸ Zob. Wyrok ETPC z dnia 29 sierpnia 1997 r. w sprawie Worm przeciwko Austrii, skarga nr 22714/93; podobnie: Wyroki ETPC w sprawie Pedersen i Baadsgaard przeciwko Danii; z dnia 21 stycznia 1999 r. w sprawie Janowski przeciwko Polsce, skarga nr 25716/94.

⁵⁹ J. Barta (red.), *Prawo autorskie*, t. 13, Warszawa 2003, s. 182 (System Prawa Prywatnego); także: B. Michalski, *Podstawowe problemy prawa prasowego*, Warszawa 1998, s. 57.

⁶⁰ W sprawie Oberschlick przeciwko Austrii Trybunał objął ochroną publikację w formie doniesienia o popełnieniu przestępstwa przez sekretarza Austriackiej Partii Liberalnej. Oberschlick jako dziennikarz i zarazem wnioskujący o wszczęcie postępowania karnego, zarzucił krytykowanemu politykowi podżeganie do nienawiści rasowej, a także szerzenie poglądów nazistowskich. Podstawą sformułowania takich zarzutów stała się wypowiedź, w której polityk ów opowiedział się za zróżnicowaniem wysokości zasiłków rodzinnych dla Austriaczek oraz matek z rodzin imigrantów. Sądy krajowe uznały, że dziennikarz przekroczył granice dozwolonej krytyki, a stawiane przez niego zarzuty w formie doniesienia o popełnieniu przestępstwa nie znajdują potwierdzenia w faktach. Trybunał wyraził odmienny pogląd. Uznał bowiem, że wypowiedź w tej formie nie stanowi informacji o faktach, które podlegałyby dowodzeniu, ale wyraża jedynie oceny, do których formułowania ma prawo dziennikarz. Można w tym wypadku uznać, że polityk stracił kontrolę nad sposobem korzystania z jego własnej wypowiedzi, która została zaliczona do domeny publicznej i poddana surowej krytyce. Trybunał dopuścił zatem, by wypowiedzi

Status wypowiedzi publicznych – jak wynika z analizy rozstrzygnięć Trybunału – nie jest zatem uzależniony od prawdziwości, wiarygodności ani też użyteczności wypowiedzi. Kryterium tym nie jest także decyzja autora o jej publicznym udostępnieniu, forma wypowiedzi ani jej zgodność z obyczajami czy normami współżycia społecznego. Za wypowiedzi publiczne, niezależnie od spełnienia wcześniej wymienionych kryteriów, Trybunał uznaje wypowiedzi pochodzące od osób publicznych i/lub dotyczące spraw, które mogą być potraktowane jako „wzbudzające szczególne zainteresowanie lub mające szczególne znaczenie dla odbiorców”. Debata publiczna może toczyć się zatem niemal na każdy temat i wszystkie środki, którymi dysponują debatujący, mogą w jej trakcie być wykorzystane.

B. Wypowiedź prywatna

O prywatnym charakterze wypowiedzi przesądza intencja jej autora, a w szczególności jego wola, by wypowiedź trafiła wyłącznie do oznaczonego przez niego kręgu adresatów. Nie ma zatem istotnego znaczenia treść wypowiedzi. Charakter wypowiedzi prywatnej może mieć zarówno wypowiedź dotycząca spraw publicznych, jak i prywatnych faktów. Nawet jeśli wypowiedź ma znaczenie dla debaty publicznej, to nie traci ona prywatnego charakteru dopóty, dopóki nie zostanie rozpowszechniona. Przez rozpowszechnienie należy rozumieć sytuację, w której istnieje realna możliwość zapoznania się z treścią wypowiedzi przez nieograniczony krąg osób⁶¹.

pochodzące od osoby publicznej mogły przybierać formę karykaturalną, poprzez fragmentaryczne ich wykorzystanie, umieszczanie w zmienionym kontekście oraz jednostronne komentowanie, które przeradza się w formułowanie zarzutów karnych. Artykuł opublikowany w formie doniesienia o popełnieniu przestępstwa został uznany za formę dozwolonego komentarza (zob. Wyrok ETPC w sprawie Oberschlick przeciwko Austrii (nr 1)).

⁶¹ Rozpowszechnienie oznacza uczynienie określonych treści powszechnie dostępnymi, umożliwienie zapoznania się z nimi bliżej nieokreślonej liczbie osób (zob. L. Wilk, *Odpowiedzialność karna w Prawie prasowym*, [w:] *Prawo mediów*, P. Ślęzak (red. nauk.), Warszawa 2020; podobnie: T. Oczkowski, [w:] *Kodeks karny. Komentarz*, V. Konarska-Wrzošek (red. nauk.), Warszawa 2023, art. 305. W ten sam sposób pojęcie „rozpowszechnienia jest definiowane przez orzecznictwo. NSA wskazuje, że „Rozpowszechnienie oznacza uczynienie czegoś znanym szerokiemu gronu odbiorców” (Wyrok WSA w Warszawie z dnia 30 sierpnia 2016 r., VI SA/Wa 455/16, LEX nr 2241303).

Dobrem chronionym jest sfera prywatności autora wypowiedzi obejmująca zarówno informacje odnoszące się do treści wypowiedzi, zwłaszcza jeśli dotyczą one faktów z życia prywatnego (rodzinnego, intymnego) autora, jak i dane identyfikujące autora lub czas, miejsce i okoliczności wypowiedzi⁶². Podstawę prawną ochrony wypowiedzi stanowią, na gruncie prawa krajowego, gwarancje zapewniające ochronę prywatności (art. 47 Konstytucji RP), tajemnicę komunikowania (art. 49 Konstytucji RP), a także autonomię informacyjną jednostki (art. 51 Konstytucji RP) oraz ochronę danych osobowych (art. 51 ust. 1 Konstytucji RP i postanowienia zawarte w RODO⁶³). Ochrona prywatności wypowiedzi została także przewidziana w przepisach szczególnych, w tym w art. 14 ust. 1 i 6, a także art. 14 a ustawy Prawo prasowe⁶⁴.

⁶² Przesłanki pozwalające na skuteczne powołanie się na ochronę prywatności zostały wypracowane przez ETPC w sprawach dotyczących Katarzyny von Hannover. Chodziło o publikację serii zdjęć przedstawiających księżniczkę m.in. w czasie jazdy konnej, w czasie zakupów, na nartach podczas wakacji, a także w towarzystwie księcia Ernesta Augusta von Hannover, kiedy wychodzi z domu, gra w tenisa, a także trzymających się za ręce w jednym z klubów w Monte Carlo. Wydawnictwo Burda, występujące jako interwenient w procesie wytoczonym przez księżniczkę Karolinę von Hannover, uzasadniało publikację jej zdjęć w magazynach kolorowych, wskazując, że jest ona osobą powszechnie znaną, pochodzi z rodziny królewskiej i po śmierci matki jest „pierwszą damą” w państwie, a zatem można przyjąć, że pełni funkcję publiczną; zdjęcia były wykonywane w miejscach publicznych i nie naruszały one godności księżniczki (zob. Wyrok ETPC z dnia 24 czerwca 2004 r. w sprawie von Hannover przeciwko Niemcom, skarga nr 59320/00 – dalej: Wyrok ETPC w sprawie von Hannover przeciwko Niemcom). Na gruncie orzeczeń w sprawie von Hannover za zasadne przyjęto uznawać, że tylko taka wypowiedź, która jednocześnie spełnia wszystkie kryteria prywatności (treść, miejsce wygłoszenia, adresat, brak związku z działalnością publiczną) może mieć charakter prywatny i nie powinna być publikowana.

⁶³ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. UE L Nr 119, s. 1 z późn. zm.).

⁶⁴ W art. 14 pr.pr. wskazany został katalog uprawnień, na które może powoływać się rozmówca, udzielając dziennikarzowi informacji. Może on zatem, po pierwsze, oczekiwać, że dziennikarz przed rozpowszechnieniem informacji utrwalonych za pomocą zapisów fonicznych i wizualnych uzyska zgodę na ich rozpowszechnienie (art. 14 ust. 1). W art. 14 ust. 3 pr.pr. przewidziano natomiast, że osoba udzielająca informacji może z ważnych powodów społecznych lub osobistych zastrzec termin i zakres jej opublikowania. W art. 14 ust. 5 pr.pr. ustawodawca postanowił, że dziennikarz nie może opublikować informacji, jeżeli osoba udzielająca jej zastrzegła to ze względu na tajemnicę zawodową. Natomiast w art. 14 ust. 6 pr.pr. zagwarantowano ochronę prywatności osób, których dotyczy wypowiedź prasowa. Dopuszczalność publikacji informacji dotyczącej prywatnej sfery życia jest dopuszczalna wówczas, gdy wiąże się to bezpośrednio z działalnością publiczną danej osoby.

Wywodzić ją należy także z przepisów prawa ponadnarodowego. Gwarancje ochrony prywatności zawiera art. 8 EKPC⁶⁵, jak również art. 7 KPP⁶⁶.

Zasadniczym celem art. 8 Konwencji jest ochrona jednostki przed arbitralną ingerencją władzy publicznej. Każda ingerencja na podstawie art. 8 musi być uzasadniona – w świetle drugiego ustępu – jako „zgodna z prawem” i „konieczna w demokratycznym społeczeństwie” dla osiągnięcia jednego z wyszczególnionych w tym przepisie celów⁶⁷. Zgodnie z utrwalonym orzecznictwem Trybunału, pojęcie konieczności implikuje, że taka ingerencja wynika z ważnej potrzeby społecznej oraz w szczególności, że pozostaje ona w odpowiedniej proporcji do jednego z uzasadnionych celów realizowanych przez władze⁶⁸.

Potrzeba zapewnienia ochrony prywatności jednostki pozostawała często w kolizji z prawem do realizacji swobody wypowiedzi. Oś sporu w takich sytuacjach koncentrowała się zazwyczaj na analizie treści wypowiedzi, a w szczególności zawartych w niej informacji obejmujących dane z życia prywatnego. Spór nie dotyczył zatem dopuszczalności rozpowszechnienia wypowiedzi ze względu na jej prywatny charakter, lecz ze względu na jej treść. Chodziło o ustalenie, czy istnieją – a jeśli tak, to jakie – okoliczności, które usprawiedliwiają ujawnienie treści wypowiedzi. Niezwykle rzadko przedmiotem sporu był sam charakter wypowiedzi, tj. jej przynależność do sfery prywatności (wypowiedź prywatna). Samo zatem ujawnienie istnienia wypowiedzi prywatnej bez ujawnienia jej treści nie stanowiło wystarczającej podstawy do występowania z roszczeniem o ochronę prywatności.

W art. 14 a pr.pr. ustawodawca zobowiązał dziennikarzy do autoryzowania wypowiedzi, jeśli miałyby one zostać wykorzystane w materiale prasowym w formie dosłownego cytatu.

⁶⁵ W myśl art. 8 EKPC „Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji (ust. 1). Niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa, z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób (ust. 2)”.

⁶⁶ Zgodnie z tym przepisem każdy ma prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się.

⁶⁷ Wyrok ETPC z dnia 16 lipca 2013 r. w sprawie Węgrzynowski i Smolczewski przeciwko Polsce, skarga nr 33846/07.

⁶⁸ Wyrok z dnia 24 marca 1988 r. w sprawie Olsson przeciwko Szwecji (nr 1), skarga nr 10465/83, § 67.

Ochrona prywatności jest poddawana obecnie, jak zauważył I.C. Kamiński, „waloryzacji”⁶⁹. Autor wskazuje, że ochrona prywatności w zetknięciu z wolnością wypowiedzi nabiera nowego, większego znaczenia, uzyskując prymat nad ochroną wolności wypowiedzi. W najnowszym orzecznictwie Trybunału widoczny jest coraz mocniej wątek równoważenia swobody wypowiedzi i „godnościowych racji”. Te ostatnie są łączone zwłaszcza z art. 8 Konwencji. Przepis ten gwarantuje jednostce prawo do życia prywatnego, które jest rozumiane szeroko, obejmując również tożsamość jednostki, nie tylko indywidualną, lecz także grupową⁷⁰. W konsekwencji istniałby pozytywny obowiązek zapewnienia poszanowania ochrony przed takimi aktami wypowiedzi, które naruszają godnościowy (równościowy) wymiar prywatności.

Pojęcie poszanowania życia prywatnego w rozumieniu art. 8 Konwencji dla celów określania pozytywnych obowiązków państwa nie ma wyraźnie wyznaczonych granic. W świetle różnorodności stosowanych praktyk i sytuacji panującej w umawiających się państwach, wymogi dotyczące tego pojęcia będą się znacznie różniły w zależności od sprawy. Tak więc jest to obszar, w którym umawiające się strony mają szeroki margines swobody w określaniu działań, jakie mają zostać podjęte w celu zapewnienia zgodności z Konwencją, przy uwzględnieniu potrzeb oraz zasobów społeczeństwa i jednostek⁷¹. Niemniej jednak art. 8, podobnie jak pozostałe postanowienia Konwencji i jej protokołów, muszą być interpretowane w sposób gwarantujący nie tyle prawa, które są teoretyczne i iluzoryczne, ale prawa, które są praktyczne i skuteczne⁷².

⁶⁹ Zob. I.C. Kamiński, „Mowa nienawiści” w orzecznictwie Europejskiego Trybunału Praw Człowieka, Raport z dnia 30.08.2023 r., CBPE, <https://cbpe.pl/2023/08/30/mowa-nienawisci-w-orzecznictwie-europejskiego-trybunalu-praw-czlowieka/> (dostęp: 15.02.2024).

⁷⁰ Tamże.

⁷¹ Realizacja przez państwo obowiązku zapewnienia „poszanowania” życia prywatnego może polegać – jak wskazał ETPC – na stosowaniu środków mających na celu zapewnienie poszanowania życia prywatnego nawet w sferze relacji pomiędzy jednostkami, co obejmuje zarówno zapewnienie regulacyjnych ram dla maszyny orzekającej i egzekucyjnej chroniącej prawa jednostek, jak i stosowanie, w uzasadnionych przypadkach, konkretnych środków (Wyroki ETPC: z dnia 26 marca 1985 r. w sprawie X i Y przeciwko Holandii, skarga nr 8978/80 oraz z dnia 26 maja 2011 r. w sprawie R.R. przeciwko Polsce, skarga nr 27617/04, §§ 183–184).

⁷² Wyroki ETPC: z dnia 25 listopada 2008 r. w sprawie Armoniené przeciwko Litwie, skarga nr 36919/02, § 38 oraz z dnia 25 listopada 2008 r. w sprawie Biriuk przeciwko Litwie, skarga nr 23373/03, § 37.

Ochrona godnościowych aspektów sfery życia prywatnego znajdująca podstawę w art. 8 EKPC może zatem stanowić podstawę do interpretacji konwencyjnego standardu wolności wypowiedzi w sposób zawężający zakres tej wolności. Zgodzić się należy ze stanowiskiem, że:

nie sposób obecnie rozstrzygnąć, czy i jak użycie art. 8 może spowodować rekonstrukcję i rewizję standardu swobody wypowiedzi wypracowanego w dotychczasowym orzecznictwie Trybunału. Jednym z kanonów tego standardu jest przecież, iż ochronie podlegają też wypowiedzi, które obrażają, oburzają lub wprowadzają niepokój. Dokonująca się „waloryzacja” art. 8, połączona też czasami z zastosowaniem zakazu dyskryminacji (art. 14), może tę tezę osłabiać⁷³.

Ochrona treści wypowiedzi ze względu na fakt ujawnienia w niej faktów ze sfery życia prywatnego może następować niezależnie od ochrony wypowiedzi ze względu na jej prywatny kontekst. Sąd Apelacyjny w Warszawie w wyroku z dnia 6 czerwca 2022 r. wyraził pogląd, zgodnie z którym podstępne nagranie prywatnej rozmowy godzi w konstytucyjną zasadę swobody i ochrony komunikowania się (art. 49 Konstytucji RP), a dowody uzyskane w sposób sprzeczny z prawem nie powinny być, co do zasady, dopuszczane w postępowaniu cywilnym⁷⁴. Podobne stanowisko zajmuje ETPC. Trybunał uznał za naruszające sferę życia prywatnego podsłuchiwanie rozmów⁷⁵, a także konfiskatę manuskryptu książki pisanej przez więźnia⁷⁶. Za rodzaj prywatnej

⁷³ Zob. I.C. Kamiński, „*Mowa nienawiści*”...

⁷⁴ Wyrok SA w Warszawie z dnia 6 czerwca 2022 r., I ACa 517/21, LEX nr 3440994; wcześniej takie samo stanowisko przedstawiono w wyroku z dnia 10 stycznia 2008 r. Sądu Apelacyjnego w Poznaniu (I ACa 1057/07).

⁷⁵ Trybunał uznał za naruszające sferę życia prywatnego podsłuchiwanie rozmów, jakie policjantka prowadziła ze swojego gabinetu z członkami rodziny. Trybunał nie miał także wątpliwości, że podsłuchiwanie rozmów prowadzonych z domowego aparatu telefonicznego stanowi ingerencję w sferę życia prywatnego oraz tajemnicę korespondencji (Wyrok ETPC z dnia 25 czerwca 1997 r. w sprawie Halford przeciwko Wielkiej Brytanii, skarga nr 20605/92).

⁷⁶ Więźniem był doktor nauk ekonomicznych i przedsiębiorca, który został skazany na 5 lat pozbawienia wolności za przestępstwa gospodarcze. W czasie jednego z widzeń z adwokatem dyrekcja wykorzystała jego nieobecność w celi i skonfiskowała manuskrypt, w którym opisywał swoje więzienne przeżycia oraz samo stosowanie procedury karnej oraz zachowanie przedstawicieli wymiaru sprawiedliwości (Wyrok ETPC z dnia

wypowiedzi Trybunał uznał także akcję zbierania podpisów pod petycją kierowaną do władz miasta⁷⁷, jak również wypowiedzi wygłaszane przez nauczycielkę w czasie zebrań partyjnych⁷⁸. Wypowiedź może zatem zostać objęta ochroną na podstawie regulacji gwarantujących ochronę prywatności nie tylko ze względu na jej treść, lecz także prywatny kontekst.

Zaklasyfikowanie wypowiedzi do sfery życia prywatnego rodzi określone konsekwencje. Treści zawarte w prywatnych wypowiedziach w żaden sposób nie rzutują bowiem na ocenę działalności publicznej osób je wypowiadających, nie stanowią elementu publicznej debaty ani, co do zasady, nie wywołują odpowiedzialności po stronie autorów wypowiedzi wówczas, gdy znamieniem występku lub deliktu jest „rozpowszechnienie” wypowiedzi. Z drugiej jednak strony nie korzystają one z ochrony, jaką Trybunał otoczył wypowiedzi publiczne. Co do zasady bowiem wypowiedzi prywatne nie mają znaczenia dla debaty publicznej, a ich wygłoszenie nie jest usprawiedliwione interesem publicznym. Wypowiedź prywatna nie może zatem być wygłaszana w dowolny sposób, w dowolnym miejscu i bliżej nieokreślonym czasie⁷⁹. Zarazem jednak wypowiedź osoby prywatnej, jeśli decydują się ona dobrowolnie na rozpowszechnienie swojego stanowiska, a temat wypowiedzi jest uzasadniony z uwagi na społeczne zainteresowanie, może nabrać charakteru publicznego⁸⁰.

Zarówno w ujęciu orzecznictwa krajowego, jak i w świetle postanowień ETPC ochrona prywatności zmierza w dwóch kierunkach – chroniąc informacje o sposobach przeżywania prywatności oraz chroniąc aktywność jednostki przez sam fakt jej przynależności do prywatnej sfery życia. Do sfery prywatności należy zatem nie tylko treść cudzej poufnie przekazanej wypowiedzi, lecz także samo jej wygłoszenie, a także miejsce, czas i adresat. Uznając bezprawność podsłuchiwanie prywatnych rozmów prowadzonych z miejsca pracy, Trybunał wskazał, że każda osoba ma prawo posiadać „uzasadnione

11 grudnia 2003 r. w sprawie Yankov przeciwko Bułgarii, skarga nr 39084/97 – dalej: Wyrok ETPC w sprawie Yankov przeciwko Bułgarii).

⁷⁷ Wyrok ETPC w sprawie Appleby przeciwko Wielkiej Brytanii.

⁷⁸ Wyrok ETPC z dnia 2 sierpnia 1995 r. w sprawie Vogt przeciwko Niemcom, skarga nr 17851/91 (dalej: Wyrok ETPC w sprawie Vogt przeciwko Niemcom).

⁷⁹ J. Taczkowska, *Autoryzacja wypowiedzi*, Warszawa 2008, s. 208.

⁸⁰ Wyrok ETPC w sprawie Fuentes Bobo przeciwko Hiszpanii; De Diego Nafria przeciwko Hiszpanii, a także: Appleby i in. przeciwko Wielkiej Brytanii; Wyrok ETPC z dnia 15 lutego 2005 r. w sprawie Steel i Morris przeciwko Wielkiej Brytanii, skarga nr 68416/01.

przekonanie”, że jej prywatna aktywność pozostaje pod ochroną prawa⁸¹. Prywatna jest zarówno informacja o intymności istniejącego związku pomiędzy dwojgiem ludzi, jak i sam fakt istnienia jakiegokolwiek związku. Postawa bądź działanie mają charakter prywatny niezależnie od tego, czy są prezentowane w miejscu publicznym, czy prywatnym⁸².

Prawo do prywatności obejmuje także ochroną wypowiedź anonimową, a zatem taką wypowiedź, której autor zdecydował o niepodawaniu do publicznej wiadomości swojej tożsamości, w szczególności imienia i nazwiska, albo wykorzystuje nieprawdziwe dane, także używając pseudonimu, w celu stworzenia pozorów jawnego działania, podczas gdy ustalenie jego prawdziwej tożsamości nie jest możliwe albo staje się poważnie utrudnione. Nie stanowi natomiast anonimowej wypowiedzi wypowiedź autora, którego dane zostały zastrzeżone do wiadomości określonego przez niego kręgu osób, a zatem w szczególności wówczas, gdy są objęte tajemnicą dziennikarską.

Wypowiedź anonimowa jedynie pozornie ma charakter wypowiedzi prywatnej. Intencją autora anonimowej wypowiedzi nie jest bowiem ochrona jej treści, lecz jej autorstwa. Autor anonimowej wypowiedzi jest zainteresowany, podobnie jak autor wypowiedzi prywatnej, ochroną prywatności, jednakże istotne są dla niego inne aspekty tej ochrony, w szczególności związane z tym, od kogo pochodzi wypowiedź, a nie czego ona dotyczy. Anonimowy charakter wypowiedzi nie stanowi zatem przeszkody do tego, by wypowiedź, ze względu na jej znaczenie i wagę dla interesu publicznego, stała się elementem debaty publicznej.

Rozwój jednolitego rynku cyfrowego skutkujący przeniesieniem do sfery cyfrowej wielu aktywności społecznych, w tym polegających na inicjowaniu i prowadzeniu debaty publicznej na forach i portalach społecznościowych z wykorzystaniem publicznie dostępnej sieci teleinformatycznej oraz komunikatorów internetowych, spowodował stworzenie forum wymiany opinii o zasięgu i pojemności na niespotykaną wcześniej skalę, zapewniając

⁸¹ Halford przeciwko Wielkiej Brytanii.

⁸² Rozpoznając skargę księżniczki Karoliny, Trybunał potwierdził, że nawet jeśli w publicznych miejscach, jakim była kawiarnia, objawia się prywatne życie – intymny związek – dwojga osób, to mają one prawo do jego ochrony na podstawie art. 8 Konwencji. Publikowanie zdjęć obrazujących takie zachowanie w miejscu publicznym stanowi naruszenie zasad Konwencji (zob. von Hannover przeciwko Niemcom).

nieograniczonej liczbie użytkowników nie tylko możliwość udziału w debacie publicznej, lecz także jej inicjowania i kształtowania. Stworzenie jednolitego rynku usług cyfrowych wyposażyło warunki rozwoju usług polegających na udzielaniu dostępu, przechowywaniu, przesyłaniu, a także umieszczaniu wypowiedzi (treści) w internecie. Drogą elektroniczną świadczone są najrozmaitsze usługi, zarówno takie, które ze względu na swój charakter wymagają znajomości i ujawnienia przez usługodawcę elektronicznego danych osobowych osób korzystających z tych usług (np. usługi zawierania różnego rodzaju umów sprzedaży), jak i usługi, których główną i charakterystyczną cechą jest anonimowość osób z nich korzystających, jak w przypadku nieodpłatnego udostępnienia dyskusyjnego portalu internetowego⁸³.

Prawo do anonimowej wypowiedzi, jako pochodna wolności słowa, co do zasady nie budzi kontrowersji w doktrynie⁸⁴, choć bywa kwestionowane w debacie publicznej⁸⁵. Obecnie żaden przepis prawa nie nakłada na usługodawców świadczących usługi pośrednictwa internetowego ani na usługodawców występujących w charakterze administratorów domen internetowych, forów dyskusyjnych i portali społecznościowych obowiązku zapewniania użytkownikom internetu narzędzi służących identyfikowaniu autorów wypowiedzi zamieszczonych w internecie. Usługodawca świadczący drogą elektroniczną usługi polegające na umożliwieniu bezpłatnego dostępu do utworzonego przez siebie internetowego portalu dyskusyjnego nie ma obowiązku zapewnienia możliwości identyfikacji usługobiorcy dokonującego wpisu na takim portalu⁸⁶. Obowiązku takiego nie można także wywodzić z powszechnie przyjętych zasad ogólnych, gdyż powszechnie przyjętą zasadą i istotą tego rodzaju usługi jest anonimowość usługobiorców korzystających z ogólnie dostępnych

⁸³ Wyrok SN z dnia 8 lipca 2011 r., IV CSK 665/10, OSNC 2012, nr 2, poz. 27.

⁸⁴ J. Kulesza, *Prawo do anonimowej wypowiedzi a prywatna cenzura Internetu w Polsce*, „Państwo i Prawo” 2012, nr 6, s. 35–48.

⁸⁵ Prezydent Francji E. Macron stwierdził, iż w demokratycznym społeczeństwie pojęcie anonimowości nie powinno istnieć. To samo ma dotyczyć się nie tylko fizycznego istnienia, ale również internetu oraz wszystkich jego użytkowników (zob. A. Piskorz, *Nadchodzi koniec anonimowości w sieci? To nowy pomysł Francji*, 19.04.2022, <https://geek.justjoin.it/koniec-anonimowosci-w-sieci/>, dostęp: 10.06.2024).

⁸⁶ Wyrok SN z dnia 8 lipca 2011 r., IV CSK 665/10, OSNC 2012, nr 2, poz. 27.

internetowych portali dyskusyjnych, zapewniająca wolność i swobodę wypowiedzi, co jest zasadniczym celem takich portali⁸⁷.

Pomimo istniejącej w doktrynie i orzecznictwie zgody co do tego, że anonimowość nie może chronić autorów szkodliwych treści elektronicznych przed odpowiedzialnością za wyrządzoną szkodę, to jednak, na gruncie zasad odpowiedzialności wskazanych w art. 12–14 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną⁸⁸, autor anonimowego wpisu może uchylić się od odpowiedzialności, a w jego miejsce odpowiadać za nadużycie będzie dostawca usługi, w szczególności pośrednik internetowy. Anonimowy charakter wypowiedzi stanowi zatem, pomimo krytyki takiego stanu rzeczy⁸⁹, przeszkodę w pociągnięciu do odpowiedzialności autorów wypowiedzi, które swoją treścią lub formą naruszyły prawo.

Z wykładni językowej art. 14 ust. 1 usude wynika, że nie ponosi odpowiedzialności:

ten, kto udostępniając zasoby systemu teleinformatycznego [...] nie wie o bezprawnym charakterze danych [...], a w razie otrzymania urzędowego zawiadomienia lub uzyskania wiarygodnej wiadomości o bezprawnym charakterze danych niezwłocznie uniemożliwi dostęp do tych danych.

Oznacza to, że uzyskanie wiedzy usługodawcy o bezprawnym charakterze danych wyłącza od tej chwili brak jego odpowiedzialności na gruncie tego unormowania za dalsze udostępnianie danych wpisów, bez względu na to, co jest źródłem tej wiedzy, tj. żądanie osoby dotkniętej takim bezprawnym wpisem czy też uzyskanie tej wiedzy przez administratora portalu

⁸⁷ Tamże.

⁸⁸ Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz.U. z 2020 r., poz. 344) – dalej: usude.

⁸⁹ J. Kulesza zauważa, że nie jest pożądana taka sytuacja, w której odpowiedzialność za udostępniane przez siebie treści cudzego autorstwa ponosiliby jedynie dostawcy usług elektronicznych. Autorka wskazuje, że niezbędne jest znalezienie satysfakcjonującego kompromisu między odpowiedzialnością samych autorów, a obowiązkami tych, którzy umożliwiają im praktykowanie wolności słowa online. Zakres odpowiedzialności dostawców usług za udostępniane przez nich cudze treści jest zbyt szeroki – kształt obecnej regulacji nakłada na usługodawców obowiązki, które skutkują *de facto* cenzurą treści elektronicznych (zob. J. Kulesza, *Prawo do...*, s. 35–48).

samoistnie np. na skutek działania moderatora lub nawet w inny sposób⁹⁰. W orzecznictwie zauważono zarazem, że administrator systemu teleinformatycznego nie ma prawa – a tym samym obowiązku – usunięcia danych z systemu, ponieważ nie jest on ich dysponentem, lecz ma możliwość ich zablokowania, co powinien uczynić⁹¹. Za treść anonimowej wypowiedzi, w razie braku zablokowania do niej dostępu, ponosi zatem odpowiedzialność, na gruncie usude, usługodawca (administrator systemu teleinformatycznego, pośrednik internetowy)⁹².

2. Treść i forma wypowiedzi

Wybór formy i treści wypowiedzi należy do autora wypowiedzi i stanowi element realizacji wolności wypowiedzi. Szczególnie wyraźnie ETPC – a także sądy krajowe – podkreślali istnienie tego elementu jako objętego gwarancjami ochronnymi na podstawie art. 10 EKPC w odniesieniu do działalności prasy⁹³. ETPC wskazywał wielokrotnie, że wybór gatunku dziennikarskiego, co przesądza o jej ocennym albo zobiektywizowanym, faktograficznym charakterze, a także forma prezentacji wypowiedzi (wypowiedź audiowizualna uprzednio zarejestrowana, a następnie odtworzona z nośnika, wypowiedź „na żywo” (ang. *live streaming*), wypowiedź na piśmie, drukowana) należy do swobodnej decyzji autora wypowiedzi.

⁹⁰ Wyrok SN z dnia 10 stycznia 2014 r., I CSK 128/13, LEX nr 1526612.

⁹¹ Wyrok Sądu Okręgowego w Warszawie z dnia 20 marca 2023 r., XXV C 1105/22, LEX nr 3550344.

⁹² W przypadku naruszenia dóbr osobistych wypowiedziami anonimowych internautów zamieszczonych na portalach internetowych odpowiedzialność administratora należy rozpatrywać na gruncie przepisu art. 24 § 1 KC w powiązaniu z przepisem art. 14 ust. 1 usude (Wyrok SN z dnia 30 września 2016 r., I CSK 598/15).

⁹³ W orzecznictwie wskazuje się, że ocena sposobu realizowania wolności wypowiedzi obejmuje zarówno treść, jak i formę przekazu, przy czym zasada ta dotyczy także prasy. Wolność mediów każdorazowo jest bowiem powiązana z odpowiedzialnością za treść i formę przekazu i wynikające z nich konsekwencje (Postanowienie SN z dnia 19 kwietnia 2022 r., I CSK 1217/22, LEX nr 3430673).

W orzecznictwie istnieje tendencja do obejmowania ochroną na podstawie art. 10 EKPC⁹⁴ wielu form wypowiedzi, w szczególności wypowiedzi niewerbalnych. W ujęciu Europejskiego Trybunału Praw Człowieka „wypowiedź” jest traktowana jako pojęcie o otwartym zakresie. Kolejne rozstrzygane przez Trybunał sprawy wciąż rozszerzają katalog werbalnych i niewerbalnych zachowań i prezentacji, które podlegają ochronie swobody wypowiedzi gwarantowanej w art. 10 Konwencji⁹⁵. Do form wypowiedzi objętych zakresem art. 10 EKPC Trybunał zaliczył m.in.: wygłoszoną opinię⁹⁶, opinię opublikowaną w prasie⁹⁷, publikację doniesienia o popełnieniu przestępstwa w formie pisma procesowego⁹⁸, poezję⁹⁹, opracowanie naukowe¹⁰⁰, publikację w formie informatora¹⁰¹, powieść¹⁰², biografię¹⁰³, manuskrypt¹⁰⁴, materiał reklamowy o charakterze politycznym¹⁰⁵ i religijnym¹⁰⁶, oświadczenie prasowe przygotowane przez

⁹⁴ Art. 10 – Wolność wyrażania opinii: „1. Każdy ma prawo do wolności wyrażania opinii. Prawo to obejmuje wolność posiadania poglądów oraz otrzymywania i przekazywania informacji i idei bez ingerencji władz publicznych i bez względu na granice państwowe. Niniejszy przepis nie wyklucza prawa Państw do poddania procedurze zezwoleń przedsięwzięciom radiowych, telewizyjnym lub kinematograficznym. 2. Korzystanie z tych wolności pociągających za sobą obowiązki i odpowiedzialność może podlegać takim wymogom formalnym, warunkom, ograniczeniom i sankcjom, jakie są przewidziane przez ustawę i niezbędne w społeczeństwie demokratycznym w interesie bezpieczeństwa państwowego, integralności terytorialnej lub bezpieczeństwa publicznego ze względu na konieczność zapobieżenia zakłóceniu porządku lub przestępstwu, z uwagi na ochronę zdrowia i moralności, ochronę dobrego imienia i praw innych osób oraz ze względu na zapobieżenie ujawnieniu informacji poufnych lub na zagwarantowanie powagi i bezstronności władzy sądowej”.

⁹⁵ J. Taczowska, *Autoryzacja wypowiedzi*, s. 204.

⁹⁶ Wyroki ETPC: w sprawie Jerusalem przeciwko Austrii; z dnia 21 marca 2000 r. w sprawie Wabl przeciwko Austrii, skarga nr 24773/94; z dnia 25 listopada 1999 r. w sprawie Nilsen i Johnsen przeciwko Norwegii, skarga nr 23118/93.

⁹⁷ Wyrok ETPC w sprawie Castells przeciwko Hiszpanii.

⁹⁸ Wyrok ETPC w sprawie Oberschlick przeciwko Austrii (nr 1).

⁹⁹ Wyrok ETPC z dnia 12 lipca 2001 r. w sprawie Feldek przeciwko Słowacji, skarga nr 29032/95 (dalej: Wyrok ETPC w sprawie Feldek przeciwko Słowacji).

¹⁰⁰ Wyrok ETPC z dnia 17 lipca 2001 r. w sprawie Ekin przeciwko Francji, skarga nr 39288/98.

¹⁰¹ Wyrok ETPC w sprawie Handyside przeciwko Wielkiej Brytanii.

¹⁰² Wyrok ETPC w sprawie Alinak przeciwko Turcji.

¹⁰³ Wyrok ETPC z dnia 28 września 1999 r. w sprawie Ozturk przeciwko Turcji, skarga nr 22479/93.

¹⁰⁴ Wyrok ETPC w sprawie Yankov przeciwko Bułgarii.

¹⁰⁵ Wyrok ETPC w sprawie VgT Verein Gegen Tierfabriken przeciwko Szwajcarii.

¹⁰⁶ Wyrok ETPC w sprawie Murphy przeciwko Irlandii.

członka partii politycznej¹⁰⁷, ulotkę informacyjną zawierającą fragmenty wypowiedzi kandydatów do parlamentu na temat aborcji rozdawaną w trakcie kampanii wyborczej¹⁰⁸, list otwarty¹⁰⁹, list jako dokument prywatny¹¹⁰, dokument urzędowy omawiający wyniki kontroli prowadzonej na zlecenie władz państwowych¹¹¹, zeznanie podatkowe prezesa fabryki Peugeot'a mające charakter poufnego dokumentu¹¹², fotografię przedstawiającą wizerunek¹¹³, karykaturę¹¹⁴, płacone ogłoszenie stanowiące obronę pamięci marszałka Pétaína potępionego za kolaborowanie z faszystami¹¹⁵, malowidło jako realizację wolności wypowiedzi artystycznej¹¹⁶, film¹¹⁷, żądanie dostępu informacji zebranych przez władze publiczne na temat osoby wnioskodawcy¹¹⁸, zachowanie w miejscu publicznym polegające na zakłóceniu przebiegu polowania na lisy¹¹⁹, zachowanie polegające na zbieraniu podpisów pod protestem przeciwko decyzjom władzy lokalnej¹²⁰, udział urzędników lokalnej administracji w działalności politycznej¹²¹, przynależność nauczycielki do organizacji o charakterze politycznym¹²².

¹⁰⁷ Wyrok ETPC z dnia 28 sierpnia 1992 r. w sprawie Schwabe przeciwko Austrii, skarga nr 13704/88 (dalej: Wyrok ETPC w sprawie Schwabe przeciwko Austrii).

¹⁰⁸ Wyrok z dnia 19 lutego 1998 r. w sprawie Bowman przeciwko Wielkiej Brytanii, skarga nr 24839/94.

¹⁰⁹ Wyrok ETPC w sprawie Thorgeir Thorgeirson przeciwko Islandii.

¹¹⁰ Wyrok ETPC z dnia 11 marca 2003 r. w sprawie Lešník przeciwko Słowacji, skarga nr 35640/97.

¹¹¹ Wyrok ETPC w sprawie Bladet Tromsø i Stensaas przeciwko Norwegii.

¹¹² Wyrok ETPC w sprawie Fressoz i Roire przeciwko Francji.

¹¹³ Wyroki ETPC: z dnia 13 lutego 2004 r. w sprawie News Verlag przeciwko Austrii, skarga nr 39394/98; w sprawie von Hannover przeciwko Niemcom.

¹¹⁴ Wyrok ETPC w sprawie Cumpăna i Mazăre przeciwko Rumunii.

¹¹⁵ Wyrok ETPC Lehideux przeciwko Francji.

¹¹⁶ Wyrok ETPC z dnia 24 maja 1988 r. w sprawie Muller i in. przeciwko Szwajcarii, skarga nr 10737/84.

¹¹⁷ Wyrok ETPC z dnia 25 listopada 1996 r. w sprawie Wingrove przeciwko Wielkiej Brytanii, skarga nr 17419/90.

¹¹⁸ Wyrok ETPC z dnia 23 czerwca 1989 r. w sprawie Gaskin przeciwko Wielkiej Brytanii, skarga nr 10454/83.

¹¹⁹ Wyrok ETPC z dnia 25 listopada 1999 r. w sprawie Hashman i Harrup przeciwko Wielkiej Brytanii, skarga nr 25594/94.

¹²⁰ Wyrok ETPC z dnia 6 maja 2003 r. w sprawie Appleby przeciwko Wielkiej Brytanii, skarga nr 44306/98.

¹²¹ Wyrok ETPC z dnia 2 września 1998 r. w sprawie Ahmed i in. przeciwko Wielkiej Brytanii, skarga nr 22954/93.

¹²² Wyrok ETPC w sprawie Vogt przeciwko Niemcom.

W orzecznictwie wskazuje się, że forma wypowiedzi ma oczywiście istotne znaczenie dla oceny granic tego, co uznaje się za dozwolone, dopuszczalne, mieszczące się ramach wyznaczanych przez prawa danego gatunku (danej formy). Zróżnicowane powinny być jednak kryteria oceny realizacji wolności wypowiedzi w obrębie poszczególnych form ekspresji, podyktowanych prawami gatunku uprawianej twórczości¹²³.

Element formy pozostaje zazwyczaj w związku znaczeniowym (semantycznym) z elementami treści wypowiedzi, co powoduje, że są one analizowane przez sądy łącznie jako nierozzerwalnie ze sobą współistniejące. Tak więc wyrażane przez EKPC oraz krajowe orzecznictwo poglądy dotyczące granic wolności wypowiedzi odnoszą się często jednocześnie do formy oraz treści wypowiedzi.

O ile ocena wymowy wypowiedzi, analizowana zarówno przez pryzmat jej formy, jak i treści, pozostaje niezakłócona w przypadku takich kategorii wypowiedzi jak w szczególności wypowiedź polityczna, komercyjna, reklamowa, dziennikarska¹²⁴, o tyle treść i forma mogą wymagać odrębnej oceny w odniesieniu do wypowiedzi artystycznych. Konflikt pomiędzy ochroną formy a ryzykiem odpowiedzialności za treść pojawia się np. w przypadku utworów literackich. Konieczne jest wówczas rozstrzygnięcie, czy w większym stopniu na ochronę zasługuje swoboda wypowiedzi artystycznej realizowana w ramach określonego gatunku twórczości, jak np. powieść z wątkami historycznymi, czy bardziej chronić należy inne dobra poprzez stosowanie ogólnych reguł odpowiedzialności odnoszących się do treści utworu. EKPC udzielił prymatu ochrony swobodzie artystycznej nad innymi dobrami¹²⁵.

¹²³ Postanowienie SN z dnia 1 lipca 2009 r., III KK 52/09, OSNKW 2010, nr 1, poz. 2.

¹²⁴ Odwołuję się w tym zakresie do sposobu kategoryzowania wypowiedzi dokonywanej przez ETPC i ustaleń poczynionych przez I.C. Kamińskiego (zob. I.C. Kamiński, *Ograniczenia swobody...*, s. 30 i n.).

¹²⁵ EKPC stanął na stanowisku, że wypowiedź artystyczna zasługuje na szczególną ochronę, gdy dotyczy publikacji książkowej o charakterze fikcji literackiej – szerszą, niż gdy chodzi o literaturę faktu. [...] Uznanie, że doszło do naruszenia art. 23 [k.c.], a więc, że naruszone zostały dobra osobiste, powinno bowiem być poprzedzone wnikliwą analizą danej książki, a poziom ochrony przyznanej autorowi powinien być na tyle wysoki, by możliwość orzeczenia o naruszeniu przez niego, w dziele fikcji, dóbr osobistych jednostki, miała charakter wyjątkowy, dotyczyła naruszeń ewidentnych i wręcz oczywistych (B. Rodak, *Naruszenie dobrego imienia osoby poprzez sportretowanie jej w powieści a prawo do poszanowania życia prywatnego. Glosa do decyzji ETPC z dnia 11 marca 2014 r.*, 47318/07, LEX/el. 2014).

Ocena dopuszczalności ingerencji w swobodę wypowiedzi artystycznej była niejednokrotnie przedmiotem oceny przez ETPC, który podkreślał szczególny charakter swobody wypowiedzi artystycznej, a w konsekwencji wskazywał na potrzebę odmiennego, bardziej elastycznego podejścia do ustalania jej granic¹²⁶. Jedną z form wypowiedzi artystycznej, której Trybunał poświęcił najwięcej uwagi, jest satyra. Satyra jest uznawana przez Trybunał za formę ekspresji artystycznej i komentarz społeczny, który – poprzez swoje nieodłączne cechy przesady i wypaczenia rzeczywistości – w sposób oczywisty ma na celu sprowokowanie i wzburzenie¹²⁷. W doktrynie podnoszone są postulaty, by ustalenia ETPC dotyczące satyry były stosowane także do innych gatunków twórczości¹²⁸.

Termin „forma wypowiedzi” jest najczęściej odnoszony do wypowiedzi werbalnych, w szczególności wówczas, kiedy mają charakter nadmiarowy, a w konsekwencji stają się narzędziem naruszenia dóbr osobistych nie ze względu na ich informacyjny charakter, ale ze względu na zawartość w wypowiedzi i intensywność elementów niezracjonalizowanych oraz nasycenie wypowiedzi kontekstem emocjonalnym, który uzupełnia wypowiedź, ujawniając intencje jej autora w szczególności artykułu prasowego prezentującego istotne wydarzenia lub postępowanie określonych osób, reportażu, recenzji czy felietonu¹²⁹. W orzecznictwie ETPC rzadko obecne było rozróżnienie form dziennikarskiej twórczości. ETPC posługiwał się zwykle pojęciami

¹²⁶ Przyjmuje się, że „Obszar twórczości artystycznej, będący owocem wyobraźni twórcy, jest objęty reżimem wzmoczonej wolności po to, żeby nie wyposażać sędziego we władzę cenzorską, która byłaby wykonywana w imię nieodmiennie subiektywnej moralności o charakterze ograniczającym środki wyrazu, które, chociaż często mniejszościowe, są zarazem odzwierciedleniem żywego społeczeństwa i które mają swoje miejsce w demokracji” (zob. M. Górski, *Test prawideł kanonu artystycznego. Glosa do wyroku s. apel. z dnia 18 lutego 2016 r.*, „Europejski Przegląd Sądowy” 2019, nr 3, s. 43–47).

¹²⁷ Wyrok ETPC w sprawie Ziemiński przeciwko Polsce, pkt 45 i cytowane tam orzecznictwo.

¹²⁸ M. Górski dokonując analizy wyroku Sądu Apelacyjnego w Wersalu (Wyrok Sądu Apelacyjnego w Wersalu, *Cour d'appel de Versailles*, z dnia 18 lutego 2016 r., przeciwko Aurélienowi Pascalowi X, 15/02687) i porównując wyrażone w nim stanowisko ze stanowiskiem EKPC, zauważa, że „tak jak satyra musi być oceniana »na swoich, szczególnych prawach«, tak i innego rodzaju nurty artystyczne, których wyodrębnienie następuje np. na podstawie określonej tematyki i przyjętej konwencji, powinny być oceniane w kontekście »swoich szczególnych praw«, czyli kanonu reguł właściwych dla danego nurtu sztuki” (M. Górski, *Test prawideł...*, s. 47).

¹²⁹ Postanowienie SN z dnia 1 lipca 2009 r., III KK 52/09, OSNKW 2010, nr 1, poz. 2.

najbardziej pojemnymi. W przypadku prasy drukowanej Trybunał używa określeń: „artykuł prasowy”¹³⁰, „reportaż” bądź „wywiad”¹³¹. W odniesieniu do radia i telewizji posługuje się natomiast pojęciami „audycja”¹³² lub „magazyn”, jednocześnie charakteryzując ich tematykę, np. „audycja podejmująca problematykę ochrony środowiska”¹³³ albo „magazyn o charakterze informacyjnym”¹³⁴. Z punktu widzenia ochrony swobody wypowiedzi Trybunał oceniał także treść i sposób formułowania przez dziennikarza pytań. Można więc przyjąć, że również pytania stawiane w trakcie wywiadu bądź audycji stanowią rodzaj dziennikarskiej wypowiedzi¹³⁵.

Kluczowe dla wytyczenia ram wolności wypowiedzi jest potwierdzenie przez Trybunał w sprawie Handyside przeciwko Wielkiej Brytanii, a następnie wielokrotnie powtarzanego stanowiska, zgodnie z którym gwarancje zawarte w art. 10 EKPC znajdują zastosowanie nie tylko do „informacji” i „poglądów”, które są dobrze przyjmowane lub postrzegane jako nieszkodliwe lub obojętne, lecz także do tych wypowiedzi, które są obraźliwe, szokują lub przeszkadzają państwu lub jakiejkolwiek grupie społecznej. Takie są bowiem wymogi pluralizmu, tolerancji i otwartości, bez których nie ma „społeczeństwa demokratycznego”¹³⁶. W kolejnych orzeczeniach Trybunał spostrzegł, że wypowiedzi mogą przybierać postać zracjonalizowanych twierdzeń odnoszących się do faktów, a także mogą mieć charakter niezracjonalizowanych,

¹³⁰ Wyroki ETPC: w sprawie Bergens Tidende przeciwko Norwegii; w sprawie Cumpănă i Mazăre przeciwko Rumunii; w sprawie Oberschlick przeciwko Austrii (nr 1), w sprawie Oberschlick przeciwko Austrii (nr 2); w sprawie Lingens przeciwko Austrii; w sprawie Dalban przeciwko Rumunii.

¹³¹ Wyroki ETPC: w sprawie Jersild przeciwko Danii; z dnia 20 kwietnia 2004 r. w sprawie Amihalachioaie przeciwko Mołdawii, skarga nr 60115/00; w sprawie Özgür Gundem przeciwko Turcji.

¹³² Wyrok ETPC w sprawie Pedersen i Baadsgaard przeciwko Danii.

¹³³ Wyrok ETPC z dnia 29 marca 2001 r. w sprawie Toma przeciwko Luksemburgowi, skarga nr 38432/97.

¹³⁴ Wyrok ETPC z dnia 30 marca 2004 r. w sprawie Radio France i in. przeciwko Francji, skarga nr 53984/00.

¹³⁵ Wyroki ETPC: z dnia 6 lutego 2001 r. w sprawie Tammer przeciwko Estonii, skarga nr 41205/98; w sprawie Jersild przeciwko Danii; w sprawie Pedersen i Baadsgaard przeciwko Danii.

¹³⁶ Wyrok ETPC w sprawie Handyside przeciwko Wielkiej Brytanii; podobnie Wyrok ETPC z dnia 25 stycznia 2007 r. w sprawie Vereinigung Bildender Künstler przeciwko Austrii, skarga nr 68354/01, LEX nr 212105 i inne.

subiektywnych opinii (ocen)¹³⁷. Zdaniem Trybunału, podczas gdy istnienie faktów można wykazać, to już prawdziwość ocen nie podlega udowodnieniu. Wymóg udowodnienia prawdziwości sądu wartościującego jest niemożliwy do spełnienia i dlatego też narusza sam w sobie zasadę wolności wyrażania opinii, która stanowi fundamentalną część praw chronionych na podstawie artykułu 10 Konwencji.

Konsekwencją powyższego ustalenia jest zastosowanie bardziej rygorystycznych wymagań w stosunku do autorów wypowiedzi o faktach, ponieważ ich prawdziwość należy dowieść w procesie, w stosunku do wymagań adresowanych wobec autorów opinii (ocen). Ustalenie bezprawności wypowiedzi wymaga zatem w pierwszej kolejności zweryfikowania jej charakteru jako opinii albo twierdzenia o faktach¹³⁸. Chociaż w praktyce rzadko dana wypowiedź przybiera jednoznaczną postać: oceną lub informacyjną, albowiem najczęściej występują w niej – w różnym natężeniu – elementy faktyczne i ocenne, jednak stopień ich natężenia oraz proporcje, w jakich występują, stanowią podstawę przyjęcia określonego charakteru wypowiedzi. W takich wypadkach, jak podkreśla się w orzecznictwie, należy zbadać, czy w wypowiedzi można wyodrębnić elementy poddające się testowi według kryterium prawda/fałsz oraz konsekwentnie taki test przeprowadzić¹³⁹.

Trudność dotycząca rozdzielenia wypowiedzi ocennych od twierdzeń o faktach ma charakter metodologiczny. Zważywszy na nieograniczoną i zróżnicowaną liczbę stanów faktycznych związanych z kreatywnym często użyciem kontekstów językowych, nadawaniem wyrażeniom nowych znaczeń i tworzeniem neologizmów, wydaje się, że nie jest możliwe ustalenie metodyki pozwalającej na kwalifikowanie wypowiedzi do jednej z dwóch kategorii, tj.; ocen lub twierdzeń o faktach. Okoliczność ta powoduje, że ustalenia dokonywane przez sądy mają charakter intuicyjny, a przez to uznaniowy.

Rozgraniczenie wypowiedzi ocennych od twierdzeń o faktach wywołuje skutki procesowe i materialnoprawne. Skutkiem procesowym jest ustalenie charakteru i rodzaju dowodów, jakich przeprowadzenie jest konieczne,

¹³⁷ Wyroki ETPC: z dnia 19 maja 2005 r. w sprawie Turhan przeciwko Turcji, skarga nr 48176/99; w sprawie Jerusaleń przeciwko Austrii, z dnia 6 maja 2003 r. w sprawie Perna przeciwko Włochom, skarga nr 48898/99; w sprawie Feldek przeciwko Słowacji.

¹³⁸ Wyrok SA w Warszawie z dnia 5 września 2013 r., I ACa 244/13, LEX nr 1400489.

¹³⁹ Wyrok SN z dnia 18 stycznia 2013 r., IV CSK 270/12, OSNC 2013, nr 7–8, poz. 94.

w szczególności obowiązek przeprowadzenia dowodu prawdy. Skutkiem materialnoprawnym jest treść wydanego przez sąd rozstrzygnięcia defini tywnego normującego sytuację prawną stron.

Sąd nie ma obowiązku uprzedzenia stron o tym, w jaki sposób kwali fikuje sporne wypowiedzi. Tymczasem zastosowana przez sąd kwalifika cja determinuje sposób i zakres prowadzenia postępowania dowodowego. Jeśli zatem wypowiedzi zostaną zakwalifikowane jako twierdzenia o faktach, to naruszytel ma obowiązek dowieść prawdziwości tych faktów. Pod tym bowiem warunkiem może dopiero uchylić się od odpowiedzialności. Jeśli jednak wypowiedzi zostaną zakwalifikowane jako opinie, to wystarczające dla uniknięcia odpowiedzialności będzie wykazanie, że autor przy formułowaniu tych opinii nie nadużył prawa. Brak precyzyjnie określonej metodyki pozwalają cej na rozgraniczenie wypowiedzi ocennych od twierdzeń o faktach poszerza zakres dyskrejonalnej władzy sądu, a zarazem wprowadza element niepew ności po stronie uczestników postępowania, co nie służy realizacji celów procesu tak karnego, jak i cywilnego, w szczególności obowiązkowi ustalenia prawdy materialnej (art. 3 k.p.c. i art. 7 k.p.k.).

Dostrzeżenie wskazanych powyżej mankamentów spowodowało, że sta nowisko judykatury, a w tym także EKPC, ewoluowało. Trybunał początkowo twierdził, że związek między sądem wartościującym i podpierającymi opinię faktami może być, według Trybunału, różny w zależności od okoliczności. Nie może być to jednak związek luźny, a „dostateczny”, czyli mający uzasad nione podstawy. Jednakże aż do rozstrzygnięcia w sprawie Feldek przeciwko Słowacji¹⁴⁰, na co zwrócił uwagę Sąd Najwyższy¹⁴¹, tylko bardzo poważne racje bądź pilna potrzeba społeczna mogła uzasadniać postawienie ochrony dóbr osobistych osoby pełniącej funkcję publiczną ponad wolność słowa. Wskazywano, że tylko bardzo poważne racje mogą ograniczyć wolność słowa w debacie politycznej¹⁴². Dopiero w orzeczeniu dotyczącym Lubomira Feldeka, poety, pisarza i publicysty, którego słowackie sądy skazały w związku z krytycznymi publikacjami pod adresem Dušana Slobodnika, Europejski Trybunał stwierdził, że sąd wartościujący nie podlega wprawdzie udowodnieniu,

¹⁴⁰ Wyrok ETPC w sprawie Feldek przeciwko Słowacji.

¹⁴¹ Postanowienie SN z dnia 1 lipca 2009 r., III KK 52/09, OSNKW 2010, nr 1, poz. 2.

¹⁴² Tamże.

ale można wymagać, aby wyrażona opinia miała dostateczną podstawę faktyczną, gdyż bez niej dochodzi do nadużycia wolności słowa. Podkreślono przy tym, że konieczny związek między sądem wartościującym i popierającymi opinię faktami jest różny w poszczególnych przypadkach i zależy od okoliczności¹⁴³. Trybunał podkreślił, że od autora sądu wartościującego nie można wymagać, aby udowodnił jego prawdziwość. Można jednak sprawdzić, czy jego opinia ma dostateczną podstawę faktyczną, gdyż bez niej dochodzi do nadużycia wolności słowa¹⁴⁴. Nie należy przy tym dokonywać rygorystycznej interpretacji użytych słów prowadzącej bądź do uznania, że wypowiedź jest stwierdzeniem faktów, bądź do odrzucenia przedstawionych dowodów¹⁴⁵.

Możliwość badania, czy opinia była oparta na wystarczającej podstawie faktycznej, dotyczy takich wypowiedzi ocennych, w których można wyodrębnić elementy poddające się testowi według kryterium prawdy lub fałszu. ETPC w odniesieniu do wypowiedzi o charakterze ocennym dopuścił możliwość badania, czy „fakty, na podstawie których skarżący sformułował swoją ocenę, były zasadniczo prawdziwe”, bądź – inaczej ujmując – czy wyrażone sądy korzystały z „wystarczającej podstawy faktycznej”¹⁴⁶. Ujemne wypowiedzi ocenne nie podlegają testowi prawdy i uznaje się je za dopuszczalne, jeżeli krytyka leży w interesie publicznym i jest rzetelna. Wypowiedź wartościująca może zostać w danych okolicznościach uznana za przekraczającą granice krytyki możliwej do zaakceptowania, jako nieznajdująca dostatecznej podstawy faktycznej. Manipulowanie prawdą o rzeczywistości nie może być zaakceptowane¹⁴⁷.

Wypowiedzi ocenne pozbawione wystarczającej podstawy faktycznej oraz nieprawdziwe twierdzenia mogą być eliminowane z obiegu publicznego wówczas, gdy pozwalają na identyfikację osób, których dotyczą. Szczególne rygory dokonywania takiej oceny, w tym prowadzące do zastosowania najdalej

¹⁴³ I.C. Kamiński: *Swoboda wypowiedzi...*, s. 93–105.

¹⁴⁴ Wyrok ETPC w sprawie Feldek przeciwko Słowacji.

¹⁴⁵ Wyrok ETPC w sprawie Jerusalem przeciwko Austrii; I.C. Kamiński: *Swoboda wypowiedzi...*, s. 12.

¹⁴⁶ Wyroki ETPC: w sprawie Schwabe przeciwko Austrii, w sprawie Jerusalem przeciwko Austrii i w sprawie Feldek przeciwko Słowacji.

¹⁴⁷ Wyrok SA w Warszawie z dnia 22 lipca 2021 r., I ACa 401/21, LEX nr 3240353; podobnie Wyroki Sądu Najwyższego z dnia 9 czerwca 2005 r., III CK 622/04, nie publik., z dnia 23 września 2009 r., I CSK 346/08, OSNC 2010, nr 3 poz. 48, z dnia 28 stycznia 2010 r., I CSK 217/09, OSNC 2010, nr 6 poz. 94, czy wskazany już wyżej wyrok IV CSK 270/12.

idącego – jak się wydaje – środka ochrony, tj. nakazanie usunięcia informacji lub danych z przestrzeni publicznej, znajdują zastosowanie w przypadku, gdy pokrzywdzony powołuje się na element prywatności, jakim są jego dane osobowe, wskazując na potrzebę usunięcia nieprawdziwej o nim informacji. Nurt w orzecznictwie potwierdzający tę optykę został zapoczątkowany w 2014 r. orzeczeniem Trybunału Sprawiedliwości UE w sprawie Mario Costeja González przeciwko Google Spain (C-131/12)¹⁴⁸, kiedy TSUE uznał, że na operatorach wyszukiwarek internetowych ciąży obowiązek usunięcia nieprawdziwych informacji, o ile zawierają one dane osobowe pozwalające na identyfikowanie osoby, której dotyczy informacja¹⁴⁹. Wskazany powyżej wyrok został wydany na gruncie prawa UE, w szczególności dyrektywy 95/46 w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych¹⁵⁰ uchylonej następnie w 2016 r. rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO)¹⁵¹. Konsekwencją wyrażonego wówczas przez TSUE stanowiska było przyjęcie na gruncie RODO rozwiązania, zgodnie z którym osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe w szczególności wówczas, gdy „osoba, której

¹⁴⁸ W ramach sporu, jaki zaistniał pomiędzy Google Spain SL (dalej: Google Spain) i Google Inc. a Agencia Española de Protección de Datos (hiszpańską agencją ochrony danych, dalej: AEPD) i M. Costeją Gonzálezem w przedmiocie wydanej przez tę agencję decyzji uwzględniającej wniesioną przez M. Costeję Gonzálezę skargę na te dwie spółki i nakazującej Google Inc. przyjęcie środków koniecznych do usunięcia danych osobowych dotyczących M. Costeji González z jej indeksu oraz uniemożliwienie dostępu do tych danych w przyszłości. Google Inc. zwróciło się do TS o wydanie rozstrzygnięcia prejudycjalnego (Wyrok TS z dnia 13 maja 2014 r. w sprawie Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mario Costeja González, C-131/12, poz. I-317, dalej: Wyrok TS w sprawie Google Spain przeciwko González).

¹⁴⁹ Tamże.

¹⁵⁰ Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. UE L Nr 281, s. 31 z późn. zm.).

¹⁵¹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. UE L Nr 119, s. 1 z późn. zm.).

dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania (art. 17 ust. 1 lit. c RODO).

Powyżej wskazane orzeczenie znacząco wpłynęło nie tylko na sposób dokonywania wykładni prawa do prywatności, ale także ustalania przesłanek odpowiedzialności podmiotów, które co prawda nie są autorami wypowiedzi, ale ze względu na charakter swojej działalności przyczyniają się do jej rozpowszechnienia. Chodzi zatem o pośredników internetowych, których działania i zaniechania mogą stanowić przedmiot oceny sądów także wówczas, gdy pośrednicy nie ingerują w treść przekazywanej wiadomości. Zasygnalizować w tym miejscu wypada, co będzie przedmiotem pogłębionej analizy w kolejnych fragmentach pracy, że w późniejszych orzeczeniach TSUE wydawanych na gruncie RODO, a także w judykatach ETPC wydawanych na gruncie art. 10 w zw. z art. 8 EKPC zarysowały się odmienne stanowiska dotyczące usuwania z internetu nieprawdziwych informacji¹⁵², przy czym ETPC przyznał szczególny status internetowym archiwom prasowym, wskazując, że archiwa internetowe objęte są ochroną przewidzianą w art. 10 EKPC¹⁵³. Trybunał podkreślił znaczący wkład archiwów internetowych w proces przechowywania i udostępniania wiadomości i informacji. Archiwa takie są ważnym źródłem edukacji i wiedzy historycznej, zwłaszcza że są łatwo dostępne dla szerokiego ogółu i generalnie są bezpłatne. ETPC wskazał, że chociaż w demokracji zasadniczym celem prasy jest pełnienie funkcji stróża publicznego „public watchdog”, to jednak ma ona także do spełnienia drugą rolę, polegającą na prowadzeniu i udostępnianiu szerokiemu ogółowi archiwów zawierających opublikowane już wcześniej wiadomości¹⁵⁴.

¹⁵² O ile zatem prawo do bycia zapomnianym uzyskało na gruncie RODO znaczenie samoistne, a zatem objęte ochroną niezależnie od ochrony udzielonej innym wartościom, o tyle na gruncie ETPC, jak zauważa W. Wator, „nie ukonstytuowało się prawo do bycia zapomnianym *per se*. To ewolucyjna interpretacja EKPC 21 pozwoliła na zakwalifikowanie kontroli nad danymi osobowymi jako komponentu prawa do poszanowania życia prywatnego” (W. Wator, *Prawo do bycia zapomnianym a swoboda wypowiedzi. Glosa do wyroku ETPC z dnia 28 czerwca 2018 r.*, „Europejski Przegląd Sądowy” 2019, nr 5, s. 46–50). Usunięcie danych osobowych „może spoczywać bezpośrednio na operatorach wyszukiwarek internetowych, bez konieczności usuwania tych danych ze strony internetowej, na której się one znajdują, zwłaszcza w sytuacji, gdy zachowanie tych informacji na tej stronie ma za podstawę przepis prawa”.

¹⁵³ Sprawa *Times Newspapers Ltd*, powołana wyżej, § 27.

¹⁵⁴ Tamże.

Utrzymywanie archiwalnych zbiorów w internecie jest kluczowym aspektem tej roli¹⁵⁵. Wyrażone przez ETPC stanowisko w wyroku w sprawie Węgrzynowski i Smolczewski przeciwko Polsce ma istotne konsekwencje dla oceny zakresu obowiązku wyszukiwarek internetowych. Wyraźnie wybrzmiało bowiem stanowisko, zgodnie z którym obowiązek usunięcia danych osobowych może, co prawda, spoczywać bezpośrednio na operatorach wyszukiwarek internetowych, jednakże na wyszukiwarkach nie ciąży obowiązek usuwania tych danych ze strony internetowej, na której się one znajdują, zwłaszcza w sytuacji, gdy zachowanie tych informacji na tej stronie ma za podstawę przepis prawa.

Usunięcie informacji z przestrzeni publicznej z powyżej wskazanych przyczyn oznacza, że informacje te mogą zostać skategoryzowane jako „nielegalnych treści”. Zgodnie z motywem 12 AUC:

pojęcie to [nielegalne treści – dop. J.T.O.] należy rozumieć w szczególności jako odnoszące się do informacji, niezależnie od ich formy, które zgodnie z obowiązującym prawem są albo same w sobie nielegalne, takich jak nielegalne nawoływanie do nienawiści lub treści o charakterze terrorystycznym i niezgodne z prawem treści dyskryminujące, albo które stają się nielegalne na mocy obowiązujących przepisów ze względu na fakt, iż odnoszą się one do nielegalnych działań.

Podsumowując, treść i forma wypowiedzi mają rozstrzygające znaczenie nie tylko w toku dokonywania przez sądy zindywidualizowanej oceny ich znaczenia dla debaty publicznej, ale mogą być wykorzystywane w celu wyodrębnienia kategorii wypowiedzi, które w pakiecie cyfrowym (AUC, ARC) zostały ujęte w zbiorczej kategorii: „nielegalnych treści”. Zaliczenie wypowiedzi do tej kategorii może mieć charakter pierwotny albo wtórny. Wtórnie nielegalny charakter mają te wypowiedzi, które korzystają, co do zasady, z ochrony zagwarantowanej na podstawie art. 10 EKPC i przepisów prawa krajowego, jednakże mają charakter nadmiarowy, stanowiąc nadużycie tej wolności, a w konsekwencji, w wyniku kontroli następczej, konieczne stało

¹⁵⁵ Wyrok ETPC z dnia 16 lipca 2013 r. w sprawie Węgrzynowski i Smolczewski przeciwko Polsce, skarga nr 33846/07.

się zrekompensowanie wynikłej z ich rozpowszechnienia krzywdy lub szkody. Pierwotnie nielegalny charakter mają natomiast te wypowiedzi, które na skutek zmiany wykładni¹⁵⁶ albo zmiany prawa i wejścia w życie nowych przepisów wyłączających *explicite* ochronę niektórych kategorii wypowiedzi (mechanizm gilotyny) nie są uznawane za realizację wolności wypowiedzi i – właśnie z tego powodu – nie podlegają ochronie, a ich rozpowszechnienie staje się podstawą do ścigania *ex officio*, przy czym wszczęcie i prowadzenie postępowania przeciwko autorom nielegalnych treści ma stanowić – w myśl nowych regulacji (AUC i ARC) – pozytywny obowiązek państwa.

3. Autor wypowiedzi – zakresy odpowiedzialności

Za wzmacnianiem ochrony swobody wypowiedzi może również przemawiać sprawowanie przez osobę lub inny podmiot roli określanej mianem „publicznego kontrolera” (ang. *public watchdog*, fr. *chien de garde*). Taką funkcję Trybunał pierwotnie łączył z dziennikarzami oraz mediami¹⁵⁷, ale następnie poszerzył ją na organizacje pozarządowe¹⁵⁸ i bloggerów aktywnych

¹⁵⁶ Istotne znaczenie ma w odniesieniu do realizacji wolności wypowiedzi nie tylko wykładnia art. 10 EKPC, ale obecnie także coraz częściej art. 17 EKPC. Trybunał sięgając do tego instrumentu, nie tylko wypowiada stanowisko w przedmiocie odmowy udzielenia ochrony określonym rodzajom wypowiedzi, ale także usprawiedliwia, zachęca, a nawet oczekuje i domaga się aktywności ze strony państwa, którego roli Trybunał upatruje w takim stanowieniu i stosowaniu prawa, które napiętnuje wypowiedzi niemieszczące się w standardzie. I.C. Kamiński zauważa, że w strasburskim orzecznictwie dała się nawet zauważyć gotowość, by rezygnować z traktowania art. 17 jako „normatywnej gilotyny”, a korzystać z niego jako przepisu identyfikującego „wzmocnione” uprawnienie państwa do dokonania ingerencji, czy też konieczność ingerencji, którą państwo musi wykazać ze względu na treść art. 10 ust. 2 (trójelementowy test zgodności ingerencji z Konwencją); zob. I.C. Kamiński, „Mowa nienawiści”...

¹⁵⁷ Symboliczne zadośćuczynienie w wysokości jednego franka zasądzone w postępowaniu cywilnym: Wyrok ETPC z dnia 24 lutego 1997 r. w sprawie De Haes i Gijssels przeciwko Belgii, skarga nr 19983/92. Po raz pierwszy w: Wyrok ETPC w sprawie Barthold przeciwko Niemcom, § 58.

¹⁵⁸ Wyrok ETPC z dnia 27 maja 2004 r. w sprawie Vides Aizsardzības Klubs przeciwko Łotwie, skarga nr 57829/00, § 42.

w internecie¹⁵⁹. Istotny będzie też kontekst wyborczy, w odniesieniu do którego strasburscy sędziowie podkreślali, że wszelkie informacje oraz oceny niezbędne w celu podjęcia przemyślanej decyzji powinny być w okresie przedwyborczym dopuszczalne i swobodnie dostępne¹⁶⁰.

4. Graniczne formy wolności wypowiedzi

Ewolucja standardu wolności wypowiedzi nie musi oznaczać zmiany jego treści, ale może sprowadzać się do definiowania na nowo kryteriów, w oparciu o które standard ten jest budowany. Nie chodzi zatem jedynie o sposób wykładni przesłanek ochrony i oznaczanie granic ingerowania w wolność wypowiedzi z powołaniem na przysługujący państwom margines uznania, ale o ustalenie i zdefiniowanie nowej koncepcji ochrony wolności wypowiedzi, w której uwzględnia się, z jednej strony realizację celów politycznych UE, a z drugiej nowe uwarunkowania techniczne i technologiczne, determinujące sposób korzystania z wolności wypowiedzi. W rezultacie następuje zalegalizowanie nowego, dychotomicznego podziału na wypowiedzi, które pozostają pod ochroną prawa oraz te, którym odmawia się ochrony, zaliczając je do kategorii „nielegalnych treści”. Zmiana podejścia uwidacznia się przede wszystkim w definiowaniu roli państwa, które stając na straży realizacji polityki antydyskryminacyjnej i równościowej, ma być nie tylko – jak dotychczas – gwarantem wolności i praw, ale powinno *de facto* je kształtować w szczególności poprzez czynne zaangażowanie w zwalczanie nielegalnych treści i przeciwdziałanie ich rozpowszechnieniu.

Granica wolności wypowiedzi przebiega zatem nie tyle pomiędzy prawem osobistym do swobody wypowiedzi a prawami osobistymi osób, których wypowiedź dotyczy, lecz jest wytyczana przez swoiście rozumianą koncepcję

¹⁵⁹ Wyrok ETPC w sprawie Falzon przeciwko Malcie, § 47.

¹⁶⁰ I.C. Kamiński, *Pojęcie „mowy nienawiści” w orzecznictwie Europejskiego Trybunału Praw Człowieka*, [w:] *Kwalifikacja prawna mowy nienawiści – krajowe i europejskie uwarunkowania normatywne, społeczne i obyczajowe nadużycia wolności wypowiedzi*, J. Tackowska-Olszewska (red.), Warszawa 2024.

ochrony interesu publicznego, którego konkretyzację stanowić ma przeciwdziałanie dyskryminacji i przemocy werbalnej. Oznacza to, że na gruncie nowego standardu ingerencja w wolność wypowiedzi staje się nie tylko usprawiedliwiona, ale jest uznawana za konieczną, co oznacza *a contrario*, że sprzeczny z istotą ochrony wolności i praw staje się brak ingerencji stanowiący niezgodne z prawem europejskim zaniechanie ze strony państwa członkowskiego. Co prawda w dokumentach programowych UE zauważa się, że „pomiędzy walką z mową nienawiści a cenzurą istnieje cienka granica”¹⁶¹, a także wyraża się przekonanie, że „nie uregulujemy skrajnej mowy politycznej. Domeną państw członkowskich pozostanie to, w jaki sposób będą one określały swobodę wypowiedzi”¹⁶², to – jak się wydaje – tym bardziej skłania europejskie organy prawodawcze do tego, by „narzucić unijne standardy walki ze zjawiskiem werbalnej i fizycznej nienawiści”¹⁶³. Wyrazem realizacji powyższej koncepcji kształtowania nowego standardu wolności wypowiedzi jest inicjatywa Komisji Europejskiej zmierzająca do poszerzenia katalogu tzw. europrzestępstw o mowę nienawiści i przestępstwa z nienawiści (art. 83 TFUE).

Komisja Europejska postuluje poszerzenie dziedzin przestępczości wymienionych w art. 83 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) o nową dziedzinę, tj. przestępstwa z nienawiści i mowę nienawiści. Komisja Europejska wnosi, by „nienawiść wobec osób lub grup posiadających (lub postrzeganych jako posiadające) cechy objęte ochroną oraz nawoływanie do nienawiści i przestępstwa z nienawiści uznać za dziedzinę przestępczości w rozumieniu art. 83 ust. 1 TFUE”¹⁶⁴. Realizacja tego postulatu oznacza poszerzenie katalogu tzw. europrzestępstw o nową dziedzinę, a w konsekwencji umożliwi instytucjom UE wydawanie aktów prawnych ustanawiających normy minimalne odnoszące się do określania znamion typów i kategorii

¹⁶¹ Opinia Europejskiego Komitetu Regionów – Poszerzenie katalogu unijnych przestępstw o mowę nienawiści i występkę nią powodowane (2023/C 79/03), pkt 39, <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52022IR1407&from=EN> (dostęp: 10.06.2024).

¹⁶² Tamże, pkt 41.

¹⁶³ Tamże, pkt 41.

¹⁶⁴ Komunikat Komisji do Parlamentu Europejskiego i Rady z dnia 9 grudnia 2021 r.: Bardziej inkluzywna i bezpieczna Europa: rozszerzenie wykazu przestępstw UE o nawoływanie do nienawiści i przestępstwa z nienawiści, <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52021DC0777&from=IT> (dostęp: 10.06.2024).

przestępstw z nienawiści i mowy nienawiści oraz dokonywanie kwalifikacji określonych zachowań jako wyczerpujących znamiona przestępstw, a także ustalania rozmiaru kar, jakie grożą za ich popełnienie i określania środków ochrony służących pokrzywdzonym i ofiarom tych przestępstw. Nadto do kompetencji organów stanowiących UE należałoby przesądzenie o zamkniętym albo otwartym katalogu grup podmiotów, których prawa zostaną poddane ochronie oraz ustalenie przesłanek ochrony. Projektowane rozwiązania, ze względu na przedmiot i proponowaną metodę regulacji, legitymizują działania organów UE w zakresie, w jakim będą one mogły skutecznie oddziaływać na ustalanie granic swobody wypowiedzi.

Kontrola legalności wypowiedzi w świetle opisanych powyżej mechanizmów wymagałaby przeprowadzenia swoistego przedsądu, którego rezultatem miałyby być ustalenie, czy wypowiedź będąca przedmiotem kontroli stanowi realizację wolności wypowiedzi, a w konsekwencji czy może korzystać z ochrony. Dopiero udzielenie twierdzącej odpowiedzi pozwalałoby na merytoryczne rozstrzygnięcie w przedmiocie dopuszczalności ingerencji w wolność wypowiedzi przy zastosowaniu tzw. testu szkodliwości. Jeśli jednak na etapie przedsądu polegającego na poszukiwaniu kwalifikacji prawnej, która miałaby stanowić podstawę merytorycznego rozstrzygnięcia w przedmiocie dopuszczalności ingerencji w wolność wypowiedzi uprawniony organ dojdzie do wniosku, że autor wypowiedzi jedynie dla pozoru powołuje się na realizację swobody wypowiedzi, podczas gdy w rzeczywistości zmierza do osiągnięcia celu sprzecznego z wartościami chronionymi w Konwencji, to nie jest możliwe przyznanie autorowi wypowiedzi ochrony na gruncie art. 10 EKPC i art. 11 KPP. W tej sytuacji należy odmówić udzielenia ochrony, a nawet konieczne jest podjęcie ścigania i zastosowanie sankcji wobec autora, którego działanie narusza porządek konwencyjny (także traktatowy), co oznacza, że jego działanie nie tylko nie może być uzasadnione realizacją usprawiedliwionego interesu indywidualnego lub publicznego, ale jako pozostające z nimi w kolizji zasługuje na napiętnowanie¹⁶⁵. Wypowiedź nielegalna jest zatem *per se* karygodna, a rola państwa polega na jej wyeliminowaniu z przestrzeni publicznej i przeciwdziałaniu jej rozpowszechnieniu w przyszłości.

Zaproponowany w niniejszej dysertacji termin „graniczne formy wolności wypowiedzi” odnosi się do tych wypowiedzi, które ubiegają się o udzielenie

¹⁶⁵ Wyrok ETPC w sprawie Zemmour przeciwko Francji.

ochrony na gruncie konwencyjnego standardu (art. 10 EKPC), jednakże ze względu na ich treść (przedmiot) oraz intensywność pierwiastka ocennego, w szczególności natężenie pejoratywnego, wymagają zastosowania przedsądu. W ramach przedsądu ustaleniu podlega to, czy dana wypowiedź jest do pogodzenia z konwencyjnymi wartościami i nie stoi w sprzeczności z porządkiem demokratycznym, a nadto – czy autor wypowiedzi powołując się na realizację wolności wypowiedzi, nie zmierza w rzeczywistości do osiągnięcia celu, który jest nie do pogodzenia z tymi wartościami. Negatywny wynik przedsądu eliminuje wypowiedź z debaty i usprawiedliwia, co jest jak się wydaje najistotniejsze, zastosowanie najdalej idących środków, jak w szczególności usunięcie treści lub jej zablokowanie oraz zakazanie jej rozpowszechniania w przyszłości.

Zastosowany mechanizm oddzielenia wypowiedzi legalnych od nielegalnych oraz poddanie ocenie treści i formy wypowiedzi przy zastosowaniu odrębnych, różnych podstaw, a w konsekwencji także przesłanek oceny, wywołuje skutek prewencyjny – skłaniając uczestników debaty do zaniechania wypowiadania się w podobny sposób i w podobnych sprawach ze względu na ryzyko spotkania się z odmową udzielenia ochrony i zastosowaniem sankcji wobec autora wypowiedzi. Zastosowanie przedsądu wywołuje także skutek następczy polegający na zastosowaniu środków najbardziej dolegliwych dla autora wypowiedzi, takich jak – w szczególności – nakaz usunięcia jego wypowiedzi z przestrzeni publicznej, ale także na nałożenie na niego sankcji karnej.

Graniczne formy wypowiedzi to formy ekspresji wykorzystywane w sposób instrumentalny w celu oddzielenia wypowiedzi mieszczących się w tzw. europejskim standardzie wolności wypowiedzi i tych, którym odmawia się ochrony. W orzecznictwie ETPC wskazano bowiem, że kateryczne wypowiedzi atakujące lub oczerniające całe grupy, czy to etniczne, religijne, czy inne, zasługują na bardzo ograniczoną ochronę na mocy art. 10 Konwencji w związku z art. 17 EKPC¹⁶⁶ lub na taką ochronę nie zasługują wcale¹⁶⁷. Stanowisko to EKPC uzasadnia potrzebą realizacji zobowiązania z art. 14 EKPC

¹⁶⁶ Wyroki ETPC: w sprawie Seurot przeciwko Francji; Wyrok ETPC w sprawie Soulas przeciwko Francji, §§ 40 i 43–44; z dnia 20 kwietnia 2010 r. w sprawie Le Pen przeciwko Francji (grudzień), skarga nr 18788/09, które dotyczą ogólnych wypowiedzi wrogich muzułmanom we Francji.

¹⁶⁷ Wyrok ETPC w sprawie Norwood przeciwko Wielkiej Brytanii, w związku z oświadczeniami łączącymi muzułmanów w Zjednoczonym Królestwie z atakami terrorystycznymi z 11 września 2001 r.

do zwalczania dyskryminacji rasowej¹⁶⁸. Przyjmuje się jednak, że art. 17 ma zastosowanie tylko w wyjątkowych okolicznościach i skrajnych przypadkach. W sprawach dotyczących art. 10 Konwencji należy go stosować tylko wtedy, gdy jest całkowicie jasne, że zakwestionowane uwagi miały na celu odwrócenie uwagi od jego rzeczywistego celu poprzez wykorzystanie prawa do wolności wypowiedzi w celach oczywiście sprzecznych z wartościami Konwencji¹⁶⁹.

Graniczne formy wypowiedzi stały się materia dysputy orzeczniczej, co doprowadziło ostatecznie do wypracowania przez judykaturę stanowiska o potrzebie rozdzielenia wypowiedzi „legalnych”, a więc dających się pogodzić z europejskim standardem, od wypowiedzi „nielegalnych”, które nie tyle naruszają europejski standard, co w ogóle – ze względu na ekstensywny charakter tych wypowiedzi – nie mogą być na jego tle oceniane, albowiem naruszają wartości, na których budowana jest wspólnota państw europejskich i są wobec tego *per se* niezgodne z europejskim prawem.

Od państwa, członka RE lub UE, oczekuje się, by wdrożyło skuteczne rozwiązania zarówno na płaszczyźnie prawa cywilnego karnego, jak i administracyjnego, których skutkiem jest wyeliminowanie nielegalnych treści. Termin „nielegalne treści” został zdefiniowany w art. 3 lit. h AUC i oznacza:

informacje, które same w sobie lub przez odniesienie do działania, w tym sprzedaży produktów lub świadczenia usług, nie są zgodne z prawem Unii lub z prawem jakiegokolwiek państwa członkowskiego, które jest zgodne z prawem Unii, niezależnie od konkretnego przedmiotu lub charakteru tego prawa¹⁷⁰.

¹⁶⁸ Wyrok ETPC z dnia 16 lutego 2021 r. w sprawie Budinova i Chaprazov przeciwko Bułgarii, skarga nr 12567/13, § 94 i przytoczone tam odesłania.

¹⁶⁹ Wyrok ETPC w sprawie Perinçek przeciwko Szwajcarii.

¹⁷⁰ W Zaleceniu CM/Rec (2022)16 Komitetu Ministrów do państw członkowskich w sprawie walki z mową nienawiści, że na państwach członkowskich ciąży obowiązek zapewnienia zarówno na gruncie prawa karnego, cywilnego, jak i administracyjnego skutecznych mechanizmów walki z mową nienawiści. W zakresie prawa karnego obowiązek ten obejmuje w szczególności zdefiniowanie występku „mowy nienawiści”, a następnie sankcjonowanie co najmniej takich zachowań, jak: a) publiczne podżeganie do popełniania ludobójstwa, zbrodni przeciwko ludzkości lub zbrodni wojennych; b) publiczne podżeganie do nienawiści, przemocy lub dyskryminacji; c) rasistowskie, ksenofobiczne, seksistowskie i LGBTI-fobiczne groźby; d) rasistowskie, ksenofobiczne, seksistowskie i LGBTI-fobiczne obelgi publiczne na takich warunkach, jak te określone specjalnie dla obelg internetowych w Protokole Dodatkowym do Konwencji o cyberprzestępczości

Kwalifikowaną formą nielegalnych treści jest mowa nienawiści. Mowa nienawiści, jak zauważa ustawodawca europejski, co potwierdza doktryna i orzecznictwo, nie stanowi obecnie kategorii normatywnej. Nie istnieje akt prawny ani na płaszczyźnie krajowej, ani ponadnarodowej, który przesądzałby o zakresie treściowym tego pojęcia. Także w przedstawionym przez Komisję Europejską projekcie Decyzji Rady UE z dnia 9 grudnia 2021 r. w sprawie dodania nawoływania do nienawiści i przestępstw z nienawiści do dziedzin przestępczości określonych w art. 83 ust. 1 TFU pojęcie mowy nienawiści nie zostało zdefiniowane¹⁷¹. W dokumencie tym wskazano co prawda, że pojęcie mowy nienawiści było wielokrotnie używane w aktach prawnych organizacji międzynarodowych, jednak nie doprowadziło to do ustalenia jego jednolitej definicji.

Na konstrukcję pojęcia „mowy nienawiści” składają się elementy ocenne odwołujące się do subiektywnych odczuć i wrażliwości, a w konsekwencji wymagające zaangażowania innych niż obiektywnie sprawdzalne i poddające się logicznej weryfikacji przesłanki. Po raz pierwszy posłużono się tym pojęciem w Zaleceniu Komitetu Ministrów Rady Europy z 1997 r.¹⁷². Mowę nienawiści ujęto w niej jako:

obejmujący wszelkie formy wypowiedzi, które szerzą, wzniecają, promują lub usprawiedliwiają nienawiść rasową, ksenofobię, antysemityzm lub inne formy nienawiści opartej na nietolerancji, w tym: nietolerancję wyrażoną przez agresywny nacjonalizm, etnocentryzm, dyskryminację oraz wrogość wobec mniejszości, imigrantów i osób o pochodzeniu imigranckim.

dotyczących kryminalizacji aktów o charakterze rasistowskim i ksenofobicznym popełnionych za pośrednictwem systemów komputerowych (ETS nr. 189); e) publiczne zaprzeczanie, trywializacja i akceptacja ludobójstwa, zbrodnie przeciwko ludzkości lub zbrodnie wojenne; f) celowe rozpowszechnianie materiałów, które zawierają takie przejawy mowy nienawiści (wymienionych wyżej), w tym idei opartych na wyższości rasowej lub nienawiści (pkt 11 projektu dyrektywy). W zakresie prawa cywilnego i administracyjnego zaordynowano, by organy publiczne lub instytucje publiczne zostały zobowiązane do aktywnego zapobiegania i zwalczania mowy nienawiści oraz ich rozpowszechniania oraz promowania (pkt 15); zob. Zalecenie CM/Rec (2022)16 Komitetu Ministrów do państw członkowskich w sprawie walki z mową nienawiści, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680a67955#_ftn1 (dostęp: 10.06.2024).

¹⁷¹ Komunikat Komisji do Parlamentu Europejskiego i Rady „Bardziej inkluzywna....

¹⁷² Zalecenie nr R (97) 20 dla państw członkowskich w sprawie „mowy nienawiści”.

W 2015 r. w zaleceniu Europejskiej Komisji przeciwko Rasizmowi i Nietolerancji (ECRI) Rady Europy zdefiniowano mowę nienawiści jako:

popieranie lub promowanie w jakiejkolwiek formie oczerniania lub szkalowania osoby lub grupy osób lub nienawiści do takiej osoby lub grupy osób bądź podżeganie do tego, a także wszelkie molestowanie, znieważanie, negatywną stereotypizację, stygmatyzację lub groźby wobec takiej osoby lub grupy osób oraz uzasadnianie wszystkich tych wspomnianych rodzajów wypowiedzi względami związanymi z rasą, kolorem skóry, pochodzeniem lub przynależnością narodową lub etniczną, wiekiem, niepełnosprawnością, językiem, religią lub przekonaniami, płcią, tożsamością płciową, orientacją seksualną i innymi cechami osobistymi lub statusem osobistym¹⁷³.

Organizacja Bezpieczeństwa i Współpracy w Europie (OBWE) określa przestępstwa z nienawiści jako „przestępstwa popełnione z powodu uprzedzeń w stosunku do określonej grupy społecznej”. Jest to definicja operacyjna stosowana przez OBWE w jej sprawozdaniach dotyczących „przestępstw z nienawiści” oparta na decyzji Rady Ministerialnej OBWE nr 9/09 z dnia 2 grudnia 2009 r. w sprawie zwalczania przestępstw z nienawiści¹⁷⁴. Do celów zalecenia CM/Rec (2022)16 mowa nienawiści została zdefiniowana jako:

wszystkie rodzaje ekspresji, które podżegają, promują, szerzą lub usprawiedliwiają przemoc, nienawiść lub dyskryminację osoby lub grupy osób, lub które je oczerniają, ze względu na ich rzeczywiste lub przypisane cechy osobiste lub status, takie jak „rasa”, język, religia, narodowość, pochodzenie narodowe lub etniczne, wiek, niepełnosprawność, płeć, tożsamość płciowa i orientacja seksualna¹⁷⁵.

¹⁷³ Zalecenie nr 15 dotyczące ogólnej polityki ECRI w sprawie zwalczania mowy nienawiści, s. 3.

¹⁷⁴ Decyzja Rady Ministerialnej OBWE nr 9/09 z dnia 2 grudnia 2009 r. w sprawie zwalczania przestępstw z nienawiści, uzgodniona w drodze konsensusu przez wszystkie państwa OBWE, w tym wszystkie państwa członkowskie UE; zob. Office for Democratic Institutions and Human Rights, *Hate Crime Laws – A Practical Guide*, Warszawa 2009.

¹⁷⁵ Załącznik do zalecenia CM/Rec (2022)16.

Określenie „mowa nienawiści” pojawia się wielokrotnie w orzecznictwie ETPC rozstrzygającego na podstawie Europejskiej Konwencji Praw Człowieka. Jak należy pamiętać, w myśl art. 52 Karty praw podstawowych¹⁷⁶ Europejska Konwencja Praw Człowieka stanowi źródło „wspólnego europejskiego standardu prawnego”. I.C. Kamiński podkreśla, że pojęcie mowy nienawiści stosowane w orzecznictwie Trybunału jest wielowątkowe i występuje w kontekście kilku przepisów Konwencji: swobody wypowiedzi (art. 10), zakazu nadużycia prawa (art. 17), prawa do prywatności (art. 8), zakazu złego traktowania (art. 3) oraz zakazu dyskryminacji (art. 14)¹⁷⁷. Wskazanie na mowę nienawiści pojawiło się już wielokrotnie w orzecznictwie Europejskiego Trybunału Praw Człowieka (m.in. mowa nienawiści jako okoliczność uprawniająca państwo do posłużenia się sankcją pozbawienia wolności w reakcji na przekroczenia granic swobody wypowiedzi, konieczność zapewnienia ochrony jednostki ze względu na art. 8 EKPC – prawo do prywatności, którego częścią jest ochrona „integralności jednostki”). Konstrukcję mowy nienawiści Trybunał stosuje do wielu treści. I.C. Kamiński zauważa, że – w świetle orzecznictwa ETPC – „mowa nienawiści może zarówno stanowić wypowiedź wymierzoną w demokratyczną formę władzy, wypowiedź stanowiącą wyraz nienawiści lub wezwanie do nienawiści albo do nietolerancji ze względu na rasę, narodowość, przynależność etniczną, religijną, orientację seksualną, jak też wypowiedź oznaczającą negację bądź pochwalanie zbrodni przeciwko ludzkości lub zbrodni wojennej, wypowiedź będącą wezwaniem do przemocy lub jej pochwalaniem. Czasami w takich wypowiedziach można bez trudu zidentyfikować nienawiść lub wezwane do niej albo obecność podobnego elementu, np. nietolerancji lub dyskryminacji. W innych sytuacjach mamy już do czynienia z inferencją czy przypisaniem¹⁷⁸.

Orzeczniczy standard ETPC jest bardzo daleki od precyzyjności, spójności i przewidywalności. Przykładem braku precyzji i niezdecydowania ETPC

¹⁷⁶ Zgodnie z treścią art. 52 ust. 3 Karty praw podstawowych w zakresie, w jakim niniejsza Karta zawiera prawa, które odpowiadają prawom zagwarantowanym w europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności, ich znaczenie i zakres są takie same jak praw przyznanych przez tę konwencję.

¹⁷⁷ I.C. Kamiński, *Mowa nienawiści...*

¹⁷⁸ Tamże.

jest wyrok Vejdeland przeciwko Szwecji¹⁷⁹). Chociaż ETPC jednogłośnie nie dopatrzył się naruszenia art. 10, do wyroku dołączono trzy zdania odrębne do uzasadnienia, sporządzone łącznie przez sześciu sędziów, co oznacza, że argumentacja zawarta w wyroku wyraża stanowisko *de facto* jednego sędziego. Dołączone zdania odrębne identyfikują jednocześnie odmienne (i wykluczające się) stanowiska prawne: rygorystyczne i wąskie ujmowanie mowy nienawiści; konieczność analizy kontekstowej, która prowadzi do akceptacji ingerencji w pewnych okolicznościach/miejscach, ale już nie w innych); szerokie rozumienie mowy nienawiści połączone z pozbawieniem jej w ogóle ochrony ze względu na art. 17 EKPC).

Na płaszczyźnie nauk prawnych definiowanie „mowy nienawiści” było przedmiotem wielu wypowiedzi, przede wszystkim ujmujących mowę nienawiści w aspekcie realizacji swobody wypowiedzi¹⁸⁰. Zważywszy, że polskie prawo karne posiada instrumenty reakcji karnoprawnej (art. 119 § 1 k.k.; art. 256 § 1 k.k.; art. 257 k.k.) na przestępcze zachowania polegające na stosowaniu przemocy werbalnej, w tym także motywowane przesłankami

¹⁷⁹ Wyrok ETPC z dnia 9 lutego 2012 r. Vejdeland i inni przeciwko Szwecji, skarga nr 1813/07. ETPC stanął na stanowisku, że rozpowszechnianie informacji, które mają charakter dyskryminacji ze względu na orientację seksualną, nie jest przedmiotem ochrony wolności wypowiedzi. Wyrok dotyczył grupy Szwedów, którzy w szkole średniej rozprowadzali ulotki nazywające homoseksualizm dewiacyjną skłonnością seksualną. W ulotkach wskazywano na destrukcyjny wpływ homoseksualizmu na moralność społeczną i obarczano homoseksualistów winą za rozprzestrzenianie się HIV i AIDS. Oskarżono w nich także „homoseksualne lobby” o pomniejszanie znaczenia pedofilii (K. Warecka, *Strasburg: sankcja karna za obrazę homoseksualistów nie narusza wolności słowa. Vejdeland i inni przeciwko Szwecji – wyrok ETPC z dnia 9 lutego 2012 r., skarga nr 1813/07, LEX/el. 2014*).

¹⁸⁰ I.C. Kamiński, *Ograniczenia swobody wypowiedzi...*; J. Sobczak, *Swoboda wypowiedzi w orzecznictwie Trybunału Praw Człowieka w Strasburgu*, cz. II, „Ius Novum” 2007, nr 4; I.C. Kamiński, *Europejski Trybunał Praw Człowieka w roku 2014: czy to jeszcze ten sam trybunał?*, „Polski Rocznik Praw Człowieka i Prawa Humanitarnego” 2015, nr 6; A. Śledzińska-Simon, *Decyzja ramowa w sprawie zwalczania pewnych form i przejawów rasizmu i ksenofobii jako trudny kompromis wobec mowy nienawiści w Unii Europejskiej*, [w:] *Mowa nienawiści a wolność słowa. Aspekty prawne i społeczne*, R. Wieruszewski (red.), Warszawa 2010; A. Łukaszczyk, *Mowa nienawiści w stosunku do mniejszości rasowych, narodowych i etnicznych jako granica wolności wypowiedzi. Uwagi na tle wybranych orzeczeń Europejskiego Trybunału Praw Człowieka*, „Przegląd Prawa Konstytucyjnego” 2021, nr 5; D. Bychawska-Siniarska, *Ochrona prawa do wolności wyrażania opinii na mocy Europejskiej Konwencji Praw Człowieka*, Strasburg 2018; A. Bodnar, A. Gliszczyńska-Grabias, R. Wieruszewski, M. Wyrzykowski, *Mowa nienawiści a wolność słowa. Aspekty prawne i społeczne*, Warszawa 2010.

dyskryminacyjnymi ze względu na kryterium mniejszościowe, zjawisko „mowy nienawiści” było analizowane na gruncie nauki prawa karnego¹⁸¹. Znamieniem przedmiotowym działania przestępnego polegającego na stosowaniu mowy nienawiści jest stosowanie przez sprawcę przemocy. Znamień podmiotowe odnosi się natomiast do intencjonalności i stopnia zawinienia, co w odniesieniu do omawianej kategorii przestępstwa wymaga zweryfikowania pobudek (nienawistności), jakimi kierował się sprawca.

W decyzji Ramowej Rady UE 2008/913/WSiSW z dnia 28 listopada 2008 r. w sprawie zwalczania pewnych form i przejawów rasizmu i ksenofobii za pomocą środków prawnokarnych¹⁸² termin „nienawiść” zdefiniowano „jako odnoszący się do nienawiści okazywanej ze względu na rasę, kolor skóry, religię, pochodzenie lub przynależność narodową lub etniczną”. W projekcie dyrektywy Parlamentu Europejskiego i Rady w sprawie zwalczania przemocy wobec kobiet i przemocy domowej¹⁸³ zdefiniowane zostało natomiast pojęcie „cyberprzemoc”, które oznacza każdy akt przemocy popełniony, wspomagany lub zintensyfikowany częściowo lub w całości przy użyciu technologii informacyjno-komunikacyjnych (art. 4 lit. d). Ustawodawca europejski dokonuje w nim także opisu znamion takich czynów jak cyberstalking (art. 8) oraz cybernękanie (art. 9), a także udostępnianie bez zgody treści intymnych lub zmanipulowanych (art. 7). Przyjmuje jednocześnie, że „konieczne jest zapewnienie zharmonizowanych definicji przestępstw i kar w odniesieniu do określonych form cyberprzemocy” (motyw 17) oraz zakłada, że „cyberprzemoc jest w szczególności skierowana przeciwko polityczkom,

¹⁸¹ *Komentarz do art. 256 Kodeksu karnego*, [w:] A. Marek, *Kodeks karny. Komentarz*, Lex; M. Mozgawa, *Komentarz do art. 256 Kodeksu Karnego*, [w:] M. Mozgawa, *Kodeks karny. Komentarz*, Lex; Z. Cwiakalski, *Komentarz do art. 117–277 k.k.*, [w:] G. Bogdan, *Kodeks karny. Część szczególna*, t. 2, A. Zoll (red.); R. Guzik, *Wolność słowa a mowa nienawiści. Analiza karnoprawna*, Warszawa 2021; L. Gardocki, *Zagadnienia teorii kryminalizacji*, Warszawa 1990; M. Dąbrowska-Kardas, *Analiza dyrektywalna przepisów części ogólnej kodeksu karnego*, Warszawa 2012.

¹⁸² Decyzja Ramowa Rady UE z dnia 28 listopada 2008 r. w sprawie zwalczania pewnych form i przejawów rasizmu i ksenofobii za pomocą środków prawnokarnych, motyw 9, <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32008F0913> (dostęp: 10.06.2024).

¹⁸³ Projekt Dyrektywy Parlamentu Europejskiego i Rady w sprawie zwalczania przemocy wobec kobiet i przemocy domowej z dnia 8 marca 2022 r., <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52022PC0105> (dostęp: 10.06.2024) – dalej: dyrektywa przemocowa.

dziennikarkom i obrończyniom praw człowieka i dotyka je w szczególnym stopniu” (motyw 17). Opisy znamion wyżej wskazanych czynów, które – jak się postuluje w treści projektu dyrektywy – mają stanowić przestępstwa, nie zawsze są konkretne, a w konsekwencji ich zastosowanie w sprawach o zbliżonych okolicznościach faktycznych może być dalece zróżnicowane. Przykładowo jedną z form cyberstalkingu jest – jak zaproponowano w art. 8 lit. c – „udostępnianie wielu użytkownikom końcowym treści zawierających dane osobowe innej osoby, bez jej zgody, za pomocą technologii informacyjno-komunikacyjnych w celu nakłonienia tych użytkowników końcowych do wyrządzenia tej osobie szkody fizycznej lub znacznej szkody psychicznej”. Cybernękanie z kolei to:

inicjowanie ataku z udziałem osób trzecich na inną osobę przez udostępnianie wielu użytkownikom końcowym za pomocą technologii informacyjno-komunikacyjnych treści zawierających groźby lub zniewagi, czego skutkiem jest wyrządzenie zaatakowanej osobie znacznej szkody psychicznej.

Nie wdając się w szczegółową analizę opisów znamion stalkingu i cybernękania, z których pierwszy ma charakter bezskutkowy, a drugi wymaga dowiedzenia wystąpienia skutku w postaci „znacznej szkody psychicznej”, charakterystyczne jest posłużenie się pojemnymi terminami jak „inicjowanie ataku”; „szkoda psychiczna”; „wielu użytkowników”, „technologie informacyjno-komunikacyjne”; „udostępnienie treści”. Ustawodawca europejski próbuje doprecyzować niektóre z terminów, wskazując np., że termin „wielu” „należy rozumieć jako odnoszący się do dotarcia do znacznej liczby użytkowników końcowych przedmiotowych technologii, co umożliwia szeroki dostęp do tych treści oraz ich potencjalne dalsze rozpowszechnianie (motyw 18). Wyjaśnienie to w istocie ma charakter opisu *ignotum per ignotum*. Nadal bowiem nie jest jasne, co oznaczają pojęcia „znaczna liczba użytkowników”, „szeroki dostęp do treści” ani „potencjalne dalsze rozpowszechnienie”. Powyższy sposób definiowania przestępstwa cybernękania może zatem prowadzić do wniosku, że każda niemal wypowiedź krytyczna umieszczona na portalu społecznościowym ze względu na „wielu użytkowników”, „potencjalne dalsze

rozpowszechnienie” i „szeroki dostęp do treści” może oznaczać „wyrządzenie znacznej szkody psychicznej”.

Wszystkie wskazane powyżej pojęcia charakteryzuje duża intuicyjność oraz niejednoznaczność treści. Źródłem braku jednolitego znaczenia nadawanego pojęciu „mowy nienawiści” oraz konstruujących ten termin pojęć: przemoc, podżeganie do przemocy – jest nie tylko jego nieuchwytność, lecz także wielowymiarowość kontekstów interpretacyjnych wynikająca z różnorodności kulturowej, obyczajowej oraz historycznej państw członkowskich UE.

Istnieje zauważalny związek pomiędzy zaproponowanymi w dyrektywie rozwiązaniami służącymi zwalczaniu form cyberprzemocy a pojęciem nielegalnych treści oraz zasadami ich zwalczania opisanymi w pakiecie cyfrowym. W akcie o usługach cyfrowych określono bowiem horyzontalne ramy nadzoru regulacyjnego, rozliczalności i przejrzystości dostawców usług online, w szczególności pośredników internetowych, podczas gdy w projekcie dyrektywy przemocowej opisano znamiona czynów, które stanowią konkretyzację terminu „nielegalne treści” użytego w rozporządzeniach cyfrowych. Komisja Europejska wskazała w kierowanym do PE wniosku o przyjęcie dyrektywy, że zaproponowane w dyrektywie rozwiązania prawne:

zwiększają skuteczność aktu o usługach cyfrowych w dwóch kluczowych aspektach tj. po pierwsze, akt o usługach cyfrowych określa obowiązki w zakresie należytej staranności spoczywające na niektórych dostawcach usług pośrednich i dotyczące zwalczania nielegalnych treści w internecie.

Zauważono bowiem, że wniosek uzupełnia akt o usługach cyfrowych dzięki uwzględnieniu norm minimalnych dotyczących przestępstw cyberprzemocy. Po drugie, w dyrektywie przemocowej:

zapewnia się, aby krajowe organy sądowe były uprawnione do wydawania dostawcom usług pośrednich nakazów podjęcia działań przeciwko określonym rodzajom nielegalnych treści stanowiących cyberprzemoc, objętych niniejszym wnioskiem¹⁸⁴.

¹⁸⁴ Tamże, s. 7.

Akt o usługach cyfrowych zawiera szereg rozwiązań nakładających na podmioty świadczące usługi cyfrowe obowiązki w zakresie monitorowania, moderowania oraz usuwania nielegalnych treści. Na dostawcach usług ciążyć ma *de facto* obowiązek monitorowania i usuwania treści. Przez monitorowanie ustawodawca europejski rozumie działania – bez względu na to, czy są one zautomatyzowane – podejmowane przez dostawców usług pośrednich, których celem jest, w szczególności, wykrywanie, identyfikowanie i zwalczanie nielegalnych treści. Skutkiem wykrycia nielegalnej treści lub informacji ma być działanie polegające na stopniowaniu jej dostępności, widoczności i osiągalności, np. depozycjonowanie takich treści lub informacji, demontyzacja, uniemożliwienie dostępu do nich lub ich usunięcie, lub wpływające na możliwość przekazywania takich informacji przez odbiorców usługi, np. zamknięcie lub zawieszenie konta odbiorcy (art. 3 lit. t).

W prawie krajowym zasady ponoszenia odpowiedzialności za rozpowszechnianie bezprawnych wypowiedzi zostały uregulowane w ustawie o świadczeniu usług drogą elektroniczną (*usude*)¹⁸⁵. Należy podkreślić jednak, że ustawa ta nie reguluje podstaw odpowiedzialności usługodawców, lecz jedynie określa przesłanki, których spełnienie zwalnia ich z odpowiedzialności. Art. 14 ust. 1 *usude* przewiduje, że usługodawca nie ponosi odpowiedzialności, jeżeli nie wiedział o bezprawnym charakterze danych, a w razie powzięcia wiarygodnej wiadomości o bezprawnym charakterze danych, niezwłocznie uniemożliwił dostęp do nich¹⁸⁶. Przed wejściem w życie pakietu cyfrowego na gruncie krajowej wykładni ustawy o świadczeniu usług elektronicznych dominował pogląd, zgodnie z którym rozpowszechnienie wypowiedzi za pośrednictwem internetu, w szczególności na forach i portalach społecznościowych, należało wiązać ze szczególną konwencją takiej wypowiedzi, skrótowością i uproszczeniem, a przez to większą wyrazistością albo ostrością wypowiedzi, co w orzecznictwie uznawano za usprawiedliwione. Sąd Najwyższy wskazał, że nie można pomijać, iż wypowiedź została zamieszczona na forum internetowym. Właściwości takiego dyskursu i charakter jego ekspresji uzasadniają większe niż przeciętne przyzwolenie na ostrzejsze, często skrótowe, dobitne i przejawiskawione opinie, co oczywiście nie usuwa potrzeby udzielania ochrony przed naruszeniami

¹⁸⁵ *Usude*.

¹⁸⁶ Wyrok SN z dnia 18 stycznia 2013 r., IV CSK 270/12, OSNC 2013, nr 7–8, poz. 94.

dóbr osobistych przez wypowiedzi niemieszczące się w dopuszczalnej formule, do których często w tym dyskursie dochodzi¹⁸⁷. Jednakże specyfika tego forum polega przede wszystkim na stworzeniu szerokiej możliwości otwartej oraz nieskrępowanej wymiany poglądów i ocen. Gdy chodzi o oceny, są one obecnie w internecie tak rozpowszechnione, że dotyczą wszystkich przejawów życia społecznego i możliwych sfer działalności, poczynając od politycznej, przez społeczną, artystyczną, zawodową, do gospodarczej. Sąd Najwyższy podkreślał, że swoboda wypowiedzania opinii, której znaczenie we współczesnym społeczeństwie ma – pomimo związanych z nią zagrożeń – niezaprzeczalną wartość, uzasadnia powoływanie się na realizację ważnego interesu publicznego lub prywatnego. Niemożliwa do obrony, jak stwierdził Sąd Najwyższy, jest taka koncepcja wolności wypowiedzi, która odrzuca wszystko, co zawiera elementy krytyczne i negatywne. Opinie i sądy krytyczne mieszczą się bowiem w ramach chronionego prawem uprawnienia do wyrażenia ujemnej oceny. Należy przy tym podkreślić, że opinie, czyli wypowiedzi wartościujące, stanowią wyraz subiektywnego punktu widzenia ich autora i mieszczą się w granicach dopuszczalnej krytyki, nawet jeżeli jest ona niesprawiedliwa¹⁸⁸.

Przytoczone powyżej stanowisko, jak należy przypuszczać, pozostanie aktualne na gruncie rozwiązań zawartych w AUC i ARC w tej części, w jakiej odnosi się do wypowiedzi, które mieszczą się w europejskim standardzie (legalne treści), a także w odniesieniu do tych form ekspresji, które obejmują wypowiedzi offline. Zmianie może ulec natomiast model dokonywania oceny wypowiedzi rozpowszechnianych za pośrednictwem internetu (online), w szczególności ze względu na nową rolę i nowe narzędzia, w jakie wyposażone zostały podmioty świadczące usługi pośrednictwa internetowego.

Usługi pośrednictwa internetowego¹⁸⁹ należą do kategorii usług społeczeństwa informacyjnego, obejmujących szeroki zakres rodzajów działalności gospodarczej prowadzonych w trybie online. Takie rodzaje działalności mogą w szczególności polegać na sprzedaży towarów online; nie zaliczają się do nich rodzaje działalności takie jak dostawa towarów jako taka lub

¹⁸⁷ Wyroki Sądu Najwyższego z dnia 8 lipca 2011 r., IV CSK 665/10, OSNC 2012, nr 2, poz. 27 i z dnia 8 marca 2012 r., V CSK 109/11, OSNC 2012, nr 10, poz. 119.

¹⁸⁸ Wyrok SN z dnia 18 stycznia 2013 r., IV CSK 270/12, OSNC 2013, nr 7 – 8, poz. 94.

¹⁸⁹ Szczegółowo status pośredników internetowych zostanie omówiony w kolejnych częściach pracy.

świadczenie usług offline. Usługi społeczeństwa informacyjnego nie ograniczają się wyłącznie do usług dających sposobność do zawierania umów online, ale – o ile stanowią one działalność gospodarczą – dotyczą także usług, które nie są wynagradzane przez tych, którzy je otrzymują, takie jak usługi polegające na oferowaniu informacji online lub informacji handlowych, lub zapewniających narzędzia umożliwiające szukanie, dostęp oraz pozyskiwanie danych. W usługach społeczeństwa informacyjnego mieszczą się także usługi, które polegają na przekazywaniu informacji poprzez sieć komunikacyjną, na zapewnianiu możliwości dostępu do sieci komunikacyjnej lub na hostingu informacji przekazywanych przez usługobiorcę¹⁹⁰. Usługi te są objęte zbiorczą nazwą usług pośrednictwa internetowego. Do dostawców usług pośrednich, w szczególności usług pośrednich polegających na świadczeniu usług znanych jako usługi „zwykłego przekazu”, „cachingu” i „hostingu”, zastosowanie znajduje obecnie akt o usługach cyfrowych¹⁹¹.

Kluczowym pojęciem, jakim operuje ustawodawca europejski na gruncie aktu o usługach cyfrowych¹⁹² i aktu o rynkach cyfrowych¹⁹³, jest termin „nielegalne treści”. Powyższe spostrzeżenie dowodzi, że przyjęcie przez Parlament Europejski pakietu cyfrowego i jego wdrożenie jest wyrazem zaaprobowania przez organy UE potrzeby zreformowania konwencyjnego standardu wolności wypowiedzi. Reforma ta zakłada zatem, choć nie zostało to wyraźnie wskazane w treści żadnego z wniosków ustawodawczych¹⁹⁴, że istnieje kategoria wypowiedzi, które – jako *per se* nielegalne – nie mogą korzystać z ochrony

¹⁹⁰ Motyw 18 dyrektywy 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (Dz.U. UE L Nr 178, s. 1 z późn. zm.).

¹⁹¹ Zgodnie z art. 2 ust. 1 rozporządzenia w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych) (Dz.U. UE L Nr 277, s. 1 z późn. zm.) rozporządzenie to ma zastosowanie do usług pośrednich, które są oferowane odbiorcom mającym siedzibę lub znajdującym się w Unii, niezależnie od miejsca siedziby dostawców tych usług pośrednich.

¹⁹² Tamże.

¹⁹³ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie kontestowanych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828 (akt o rynkach cyfrowych) (Dz.U. UE L Nr 265, s. 1).

¹⁹⁴ Chodzi o wnioski Komisji Europejskiej do Parlamentu Europejskiego i Rady o przyjęcie rozporządzeń składających się na pakiet cyfrowy, tj. Wniosek ARC oraz Wniosek AUC.

prawa, a w konsekwencji konieczne jest ich wyeliminowanie z debaty publicznej, przeciwdziałanie ich rozpowszechnianiu zarówno online, jak i offline oraz uzasadnione jest napiętnowanie autorów tychże wypowiedzi. Wypowiedzi te, jako – co do zasady – nielegalne, są treściami niechcianymi, a przeciwdziałanie ich powstawaniu może następować w szczególności poprzez zastosowanie efektu mrożącego (ang. *chilling effect*).

O ile adresatami obowiązków opisanych w pakiecie cyfrowym są przede wszystkim pośrednicy internetowi, w tym bardzo duże platformy internetowe i bardzo duże wyszukiwarki internetowe, o tyle w projekcie dyrektywy przemocowej, w której – jak wskazano powyżej – zdefiniowane zostały cyberprzestępstwa popełniane z wykorzystaniem wypowiedzi jako narzędzia wskazanych tam typów przestępstw, adresatem obowiązków są państwa członkowskie UE. W dyrektywie nałożono na państwa członkowskie obowiązek zapewnienia, by ich ustawodawstwo zawierało opisy typów występów polegających na stosowaniu mowy nienawiści, przy czym państwa powinny zapewnić karalność mowy nienawiści zarówno wówczas, gdy pojawia się w trybie offline, jak też w internecie. Oczekuje się, że państwo będzie posiadało „jasne i przewidywalne przepisy dotyczące szybkiego i skutecznego usuwania mowy nienawiści w internecie, która jest zakazana na mocy prawa karnego, cywilnego lub administracyjnego”¹⁹⁵.

Zważywszy, że w dyrektywie przemocowej znajdują się odesłania do definicji, mechanizmów i instytucji opisanych w konwencji stambulskiej¹⁹⁶, wskazanej jako „ważny punkt odniesienia”¹⁹⁷, w myśl zawartych w tych aktach prawnych postanowień za nielegalne treści uchodzić będą wypowiedzi, które „mogą prowadzić do fizycznej, seksualnej, psychologicznej lub ekonomicznej szkody lub cierpienia”¹⁹⁸ ze względu na płeć, przy czym płeć rozumie się jako „płeć społeczno-kulturową”. Pojęcie to oznacza „społecznie skonstruowane role, zachowania, działania i atrybuty, które dane społeczeństwo uznaje za odpowiednie dla kobiet lub mężczyzn”¹⁹⁹. Należy zwrócić uwagę na istniejącą

¹⁹⁵ Projekt dyrektywy przemocowej, pkt 16.

¹⁹⁶ Konwencja Rady Europy o zapobieganiu i zwalczaniu przemocy wobec kobiet i przemocy domowej (Seria Traktatów Rady Europy nr 210).

¹⁹⁷ Dyrektywa przemocowa, s. 4.

¹⁹⁸ Art. 3 lit. a Konwencji stambulskiej.

¹⁹⁹ Art. 3 lit. c Konwencji stambulskiej.

w obrębie Konwencji stambulskiej niespójność terminologiczną, która – być może – została zamierzona przez jej twórców. O ile bowiem konwencja zmierza – jak wynika *explicite* z jej preambuły, a także art. 1 lit. a – do „ochrony kobiet przed wszystkimi formami przemocy”, to cel i przedmiot Konwencji przestają być czytelne w zetknięciu z definicją płci społeczno-kulturowej. Nie jest zatem jasne, czy dalej idąca ochrona ma zostać zapewniona na gruncie Konwencji wyłącznie tym osobom, które określą się jako kobiety, czy też także innym osobom, które – co prawda – nie będą chciały uchodzić za kobiety, niemniej pełnić będą ich role w społeczeństwie. Czy zatem osoba o homofoobicznym usposobieniu niebędąca kobietą, ale wypełniająca w życiu prywatnym i zawodowym tę rolę może cieszyć się dobrodziejstwem ochrony konwencyjnej, czy też nie jest możliwe powołanie się przez nią na postanowienia Konwencji?

Wydaje się, że zamysłem twórców Konwencji było udzielenie ochrony przedstawicielom każdej płci społeczno-kulturowej. Stanowisko to potwierdza także treść wniosku KE w sprawie przyjęcia dyrektywy przemocowej²⁰⁰, a także art. 4 lit. b projektu dyrektywy. W świetle wskazanych w tych dokumentach postanowień „przemoc domowa może dotyczyć wszystkich ludzi, w tym mężczyzn, osób młodszych lub starszych, dzieci i osób LGBTIQ²⁰¹”. Wobec powyższego wypowiedzi, „które prowadzą lub mogą prowadzić do fizycznej, seksualnej, psychologicznej lub ekonomicznej szkody lub cierpienia”²⁰², co wynika z zawartej w tych aktach definicji „przemocy wobec kobiet” i „przemocy domowej”, uchodzić będą za treści nielegalne. W dyrektywie przemocowej przesądzono *de facto* o karygodności każdej pejoratywnej lub powodującej dolegliwość wypowiedzi, która dotyczyć będzie tożsamości płciowej i to niezależnie od tego, czy autor wypowiedzi będzie odnosił ją do konkretnej osoby, czy do całego środowiska osób transpłciowych lub homo albo heteroseksualnych. Ochrona przed takimi wypowiedziami ma polegać w szczególności na wydawaniu przez właściwe organy sądowe, na wniosek ofiary, wiążących nakazów prawnych skierowanych do odpowiednich dostawców usług pośrednich i zobowiązujących ich do usunięcia takich treści lub uniemożliwienia dostępu do nich²⁰³. Nakazy, w tym usunięcia treści lub

²⁰⁰ Dyrektywa przemocowa, s. 4.

²⁰¹ Lesbijki, geje, osoby biseksualne, transpłciowe, interseksualne i queer.

²⁰² Dyrektywa przemocowa, art. 4 lit. a.

²⁰³ Art. 25 ust. 1 projektu dyrektywy przemocowej.

zablokowania dostępu, mają być wydawane nie tylko w drodze merytorycznego rozstrzygnięcia, lecz także w toku postępowań zabezpieczających²⁰⁴.

Skuteczność nowych rozwiązań zwalczających nielegalne treści ma zostać zapewniona dwiema drogami. Po pierwsze mają ją zapewnić rozwiązania przyjęte w pakiecie cyfrowym, w szczególności legalizujące proceder monitorowania, weryfikowania i kontrolowania przez pośredników internetowych rozpowszechnianych treści, a w następstwie dokonanych przy użyciu tych metod ustaleń, depozycjonowania treści, blokowania dostępu, zawieszania kont użytkownikom internetu lub usuwania treści. Po drugie występkę polegającą na rozpowszechnianiu nielegalnych treści i stosowaniu mowy nienawiści, jak wynika, z proponowanych rozwiązań zawartych w Komunikacie KE do PE i Rady: Bardziej inkluzywna i bezpieczna Europa²⁰⁵, mają trafić do katalogu europrzestępstw, co zapewniłoby im ściganie i ustalanie wymiaru kary na poziomie ogólnoeuropejskim z wyłączeniem przepisów krajowych. Jak bowiem wcześniej wskazano, Parlament Europejski i Rada mogą na podstawie art. 83 ust. 1 TFUE ustanowić normy minimalne odnoszące się do określania przestępstw oraz kar w dziedzinach szczególnie poważnej przestępczości o wymiarze transgranicznym, wynikające z rodzaju lub skutków tych przestępstw lub ze szczególnej potrzeby wspólnego ich zwalczania.

Podsumowując, stwierdzić należy, że w świetle nowych regulacji prawnych zmiana standardu wolności wypowiedzi jest nieuchronna. Stanowi ona konsekwencję zaaprobowanej przez organy ustawodawcze UE koncepcji, w myśl której należy odmówić ochrony niektórym kategoriom wypowiedzi, uznając je za szkodliwe, a w konsekwencji nielegalne. Sposób definiowania nielegalnych treści oraz metody przeciwdziałania rozpowszechnieniu nielegalnych treści wskazują, że zmiana koncepcji dotyczy także nowego kontekstu normatywnego, który pozwala na udzielenie prymatu ochronie prawa do prywatności, w tym prawa do tożsamości (np. płciowej, wyznaniowej, rasowej) oraz ochrony praw równościowych nad ochroną wolności wypowiedzi. Sygnalizuje to zarazem nowe podejście przez organy UE do budowania wspólnoty europejskiej, która przestaje być wspólnotą państw i narodów, a staje się wspólnotą mniejszości religijnych i wspólnotą osób reprezentujących różnorodne,

²⁰⁴ Tamże, art. 25 ust. 2.

²⁰⁵ Komunikat KE do PE i Rady z dnia 09.12.2021 r. Bardziej inkluzywna...

aczkolwiek mniejszościowe orientacje. Zmiana ta następuje zarówno na płaszczyźnie prawa UE, jak i regulacji przyjmowanych w Radzie Europy²⁰⁶. Udzielenie ochrony mniejszościom następuje poprzez odwołanie się do równościowych koncepcji, a następnie, w imię realizacji takich wartości jak ochrona równości i przeciwdziałanie dyskryminacji, stworzony zostaje system prawnej kontroli dystrybucji treści w środowisku cyfrowym. Treści nielegalne, w rozumieniu dokumentów wypracowanych w Komisji Europejskiej i Parlamencie jako niezasługujące na ochronę, są w konsekwencji eliminowane z przestrzeni publicznej.

²⁰⁶ I.C. Kamiński zauważa, że w 2022 r. Komitet Ministrów przyjął nową rekomendację w sprawie zwalczania mowy nienawiści (Rekomendacja z dnia 20 maja 2022 r. w sprawie zwalczania mowy nienawiści, *Combating hate speech*). Odwołuje się ona do poprzedniego dokumentu (Rekomendacja z dnia 30 października 1997 r. w sprawie „mowy nienawiści”), ale posługuje się już inną perspektywą normatywną. Podczas gdy pierwsza rekomendacja koncentrowała się na swobodzie wypowiedzi, druga akcentuje potrzebę budowania równowagi różnych gwarancji Konwencji, a więc uwzględnienia prawa do życia prywatnego (art. 8, który chroni tożsamość jednostki) oraz zakazu dyskryminacji (art. 14). Co więcej, z art. 8 i 14 wynika pozytywny obowiązek państwa do zabezpieczenia jednostki przed mową nienawiści oraz stworzenia adekwatnego reagowania na taką mowę. Rekomendacja z 2022 r. powtarza, jak rekomendacja z roku 1997, że ograniczenia wolności słowa muszą być wąsko interpretowane i stosowane, a art. 10 chroni też wypowiedzi, które obrażają, oburzają lub wprowadzają niepokój. Zauważony zostaje również art. 17, ale w preambule, i to na jej początku (drugi motyw), znalazło się wskazanie na nowy strasburski wątek. Tworzenie i egzekwowanie polityk i ustawodawstwa dotyczących mowy nienawiści wymaga starannego ważenia i równoważenia swobody wypowiedzi z prawem do poszanowania życia prywatnego i rodzinnego (art. 8) oraz zakazem dyskryminacji (art. 14). Punktem wyjścia przestaje więc być art. 10 Konwencji (z tradycyjną regułą, iż swoboda wypowiedzi to zasada, a jej ograniczenie to wyjątek wymagający przekonującego i precyzyjnego uzasadnienia (Wyrok ETPC w sprawie *The Sunday Times* przeciwko Wielkiej Brytanii (nr 1), § 65), a centralnym staje się zadanie polegające na jednoczesnym uwzględnieniu i „wypośrodkowaniu” różnych gwarancji konwencyjnych (zob. I.C. Kamiński, *Mowa nienawiści...*, s. 68 i n.).

III. Wolność wypowiedzi na rynku usług cyfrowych

1. Harmonizacja prawa – zastępowalność standardu

Wolność komunikowania i wymiany informacji w internecie są objęte ochroną na podstawie art. 10 EKPC i art. 11 Karty praw podstawowych, co wielokrotnie potwierdził Europejski Trybunał Praw Człowieka, a także Trybunał Sprawiedliwości UE. Zgodnie z orzecznictwem Europejskiego Trybunału Praw Człowieka, art. 10 EKPC gwarantuje każdemu wolność wypowiedzi i informacji i dotyczy nie tylko treści informacji, lecz także środków ich rozpowszechniania, a wszelkie ograniczenia tych środków wpływają na prawo do otrzymywania i przekazywania informacji. Jak zauważył ETPC, internet jest obecnie jednym z głównych środków, za pomocą których jednostki korzystają z prawa do wolności wypowiedzi i informacji. Strony internetowe, a zwłaszcza platformy udostępniania treści online, dzięki ich dostępności oraz zdolności do przechowywania i rozpowszechniania dużej ilości danych, przyczyniają się w dużej mierze do zwiększania dostępu ogółu społeczeństwa do aktualnych wiadomości i w sposób ogólny do ułatwiania przekazywania informacji, gdyż możliwość wypowiadania się przez jednostki w internecie stanowi bezprecedensowe narzędzie umożliwiające korzystanie z wolności wypowiedzi¹. Trybunał podkreślił konieczność należytego uwzględnienia szczególnego znaczenia internetu dla wolności wypowiedzi i informacji,

¹ Wyroki ETPC: w sprawie Cengiz przeciwko Turcji, § 52; w sprawie Kharitonov przeciwko Rosji, § 33 i przytoczone tam orzecznictwo.

zagwarantowanej w art. 11 Karty, a tym samym zapewnienia poszanowania tego prawa podstawowego przy wdrażaniu tego systemu².

Potwierdzenie przez TSUE i ETPC, że gwarancje wolności wypowiedzi zawarte w KPP i EKPC odnoszą się nie tylko do tradycyjnych środków komunikowania, ale w takim samym stopniu znajdują zastosowanie do aktywności w internecie, nie przesądza jeszcze o tym, że mechanizm kreowania standardu wolności wypowiedzi, jego utrzymania i gwarantowania jest w internecie taki sam jak poza nim. Zważywszy na podjęte przez Komisję Europejską i Parlament Europejski inicjatywy ustawodawcze i ich zakres, zasadne wydaje się postawienie tezy przeciwnej. Przyjąć zatem można, że standard wolności wypowiedzi wypracowany na gruncie EKPC i KPP w odniesieniu do sfery cyfrowej tylko formalnie pozostał taki sam. Faktycznie jednak uległ zmianie przede wszystkim dlatego, że w jego konstruowanie włączyły się podmioty świadczące usługi transmisji danych, przechowywania i udzielania do nich dostępu, nazywane w aktach prawnych regulujących sferę usług cyfrowych pośrednikami internetowymi³. Pośrednicy internetowi stali się, obok nadawców i odbiorców, uczestnikami procesu komunikowania. Pomimo że działalność pośredników internetowych jest w aktach prawnych charakteryzowana jako bierne, zautomatyzowane świadczenie usług bez ingerowania w ich treść, to jednak pośrednik internetowy faktycznie dysponuje takim arsenałem narzędzi, środków technicznych i metod, które wyposażają go w realne władztwo nad przepływem informacji w internecie i uzyskuje on realny wpływ na zakres realizacji swobody wypowiedzi.

Status pośredników internetowych został pierwotnie uregulowany na gruncie dyrektywy o handlu elektronicznym, a przede wszystkim art. 12–14 tej dyrektywy. Przepisy te zawierają przesłanki umożliwiające uchylenie się pośrednika internetowego od odpowiedzialności prawnej za naruszenie prawa spowodowane treścią lub formą transmitowanych (art. 12 usługa zwykłego przekazu) lub przechowywanych danych (art. 14 usługa hostingu), a także z tytułu ułatwiania (przyspieszania) do nich dostępu (art. 13 usługa cachingu). Potwierdzenie statusu pośrednika internetowego TSUE uzależniał

² Wyrok z dnia 22 czerwca 2021 r. w sprawie YouTube i Cyando, C-682/18 i C-683/18, pkt 64, 65, 113.

³ Chodzi o takie akty prawa europejskiego, jak dyrektywa o handlu elektronicznym, a także AUC oraz ARC.

od wykazania neutralności działania pośrednika. Działalność tego usługodawcy powinna mieć „charakter czysto techniczny, automatyczny i bierny, co oznacza, że nie posiada on wiedzy na temat informacji przekazywanych lub przechowywanych przez jego klientów ani kontroli nad nimi oraz że nie odgrywa on aktywnej roli poprzez umożliwienie tym klientom optymalizacji ich działalności polegającej na sprzedaży online”⁴.

Prawa i obowiązki pośredników internetowych zostały wskazane w dwóch rozporządzeniach Parlamentu Europejskiego, tj. akcie w sprawie usług cyfrowych (AUC) oraz akcie w sprawie kontestowalnych i uczciwych rynków cyfrowych (ARC)⁵. Akt o usługach cyfrowych to inicjatywa horyzontalna dotycząca w szczególności kwestii takich jak odpowiedzialność pośredników internetowych za treści osób trzecich, bezpieczeństwo użytkowników w internecie lub asymetryczne obowiązki w zakresie należytej staranności dotyczące poszczególnych dostawców usług społeczeństwa informacyjnego w zależności od charakteru zagrożeń społecznych, jakie mogą powodować takie usługi. Akt o rynkach cyfrowych dotyczy natomiast zakłóceń równowagi ekonomicznej, nieuczciwych praktyk handlowych ze strony strażników dostępu i ich niekorzystnych skutków, takich jak osłabienie kontestowalności rynków platform.

O ile istotą usługi pośrednictwa internetowego jest zautomatyzowana transmisja i przechowywanie nieingerujące w treść wiadomości, to jednak sposób wykonywania usług pośrednictwa wpływa na zakres korzystania z wolności wypowiedzi przez użytkowników internetu, w szczególności wówczas, gdy pośrednik ogranicza, spowolnia lub odmawia wykonania usługi, pozbawiając *de facto* odbiorcę możliwości uzyskania dostępu do informacji albo jej przekazania innym osobom. Rola pośredników internetowych jest

⁴ Wyrok TS z dnia 7 sierpnia 2018 r. w sprawie Coöperatieve Vereniging SNB-RE-ACT U.A. przeciwko Deepakowi Mehcie, C-521/17, nr 8, poz. I-639; podobnie Wyrok TS z dnia 11 września 2014 r. w sprawie Sotiris Papasavvas przeciwko O Fileleftheros Dimosia Etaireia Ltd. i in., C-291/13, nr 9, poz. I-2209 (dalej: Wyrok TS w sprawie Sotiris Papasavvas przeciwko O Fileleftheros Dimosia Etaireia Ltd.); a także Wyrok TS z dnia 15 września 2016 r. w sprawie Tobias Mc Fadden przeciwko Sony Music Entertainment Germany GmbH, C-484/14, nr 9, poz. I-689 (dalej: Wyrok TS w sprawie Tobias Mc Fadden przeciwko Sony Music Entertainment Germany GmbH).

⁵ ARC, s. 1.

zatem znacząca, a normowanie ich praw i obowiązków bezpośrednio rzutuje na kształt wolności wypowiedzi.

Obecność pośredników i ich potencjalny wpływ na sposób i zakres korzystania z wolności wypowiedzi wymagały odmiennego podejścia nie tylko do normowania zasad aktywności podmiotów prywatnych w internecie, ale także ustalania obowiązków podmiotów publicznych oraz redefiniowania statusu państw. Istotne stało się ustalenie roli państw członkowskich UE, a przede wszystkim określenie ich miejsca w stosunkach z pośrednikami internetowymi.

Jeśli zatem przyjąć, że sposób świadczenia usług pośrednictwa może determinować zakres korzystania z wolności wypowiedzi to, w następstwie tego, należy także stwierdzić, że na treść standardu wolności wypowiedzi wpływać będzie sposób ustalenia praw i obowiązków ciążących na tych podmiotach. Odpowiedzi wymagało zatem pytanie dotyczące zarówno zakresu, rodzaju i sposobu normowania obowiązków pośredników internetowych, jak też konieczne stało się wskazanie podmiotów odpowiedzialnych za kontrolę i nadzór nad wykonaniem tych obowiązków.

Dla modelu wolności wypowiedzi nie jest bowiem bez znaczenia, komu i jakie uprawnienia zostały przyznane, a nadto, jakie mechanizmy wyłączenia odpowiedzialności będą istnieć w przypadku wkroczenia pośredników internetowych w sferę praw podstawowych, w tym wobec naruszenia przez pośredników wolności wypowiedzi użytkowników internetu. Istotne jest także ustalenie, w jakim zakresie państwa członkowskie UE mogą wpływać na budowanie standardu wolności wypowiedzi w internecie. O ile bowiem mogły one poza sferą cyfrową, na gruncie wypracowanego przez TSUE i ETPC standardu, powoływać się na margines swobody przy rozstrzyganiu w przedmiocie dopuszczalności ograniczania wolności wypowiedzi, o tyle w przestrzeni cyfrowej mechanizm ten może okazać się niewystarczający, nieskuteczny albo nieodpowiedni (nieadekwatny).

Koncepcja regulacyjna, w tym decyzje dotyczące przyznania albo odmowy przyznania wybranym podmiotom w sferze wolności wypowiedzi kompetencji regulacyjnych, kontrolnych i nadzorczych, a także kompetencji prawotwórczych, będzie zatem przesądzać o treści standardu wolności wypowiedzi w internecie. Jeśli więc na gruncie art. 10 EKPC i art. 11 KPP standard wolności wypowiedzi został wypracowany przy zastosowaniu tzw. trójelementowego testu (testu szkodliwości), to przeniesienie tego standardu na grunt cyfrowy

również wymaga – jak założono w niniejszej pracy – jego zastosowania. W pierwszej kolejności zatem ograniczenia (wymogi formalne, warunki, sankcje) muszą spełniać wymaganie legalności formalnej. Działania władzy publicznej, których skutkiem jest ograniczenie wolności wypowiedzi, muszą zatem opierać się na podstawie wynikającej z prawa krajowego – w polskich warunkach konstytucyjnych musi to być podstawa o randze ustawowej, chyba że wyprowadzać się ją będzie z prawa unijnego bądź prawa międzynarodowego. Podstawa ta musi być ujęta w sposób odpowiadający „wymaganiom jakościowym”, tzn. dostępności i przewidywalności, istnieć również muszą gwarancje proceduralne chroniące przed arbitralnymi działaniami władzy⁶. Naruszenie tych wymagań stanowi wystarczającą przesłankę dla stwierdzenia naruszenia art. 10 EKPC i nie ma wówczas potrzeby podejmowania oceny legalności materialnej czy proporcjonalności ingerencji. Ograniczenia muszą następnie spełniać wymaganie legalności materialnej, więc ich zastosowanie musi służyć realizacji jednego z „celów prawowitych” wskazanych w art. 10 ust. 2 EKPC. Ponadto znaczenie podstawowe ma ocena, czy ograniczenie wolności wyrażania opinii było „niezbędne w społeczeństwie demokratycznym”⁷.

Ustalenie standardu wolności wypowiedzi w internecie będzie wymagało zatem rozstrzygnięcia, czy test szkodliwości znajduje zastosowanie i jeśli tak, czy w odniesieniu do wszystkich aktywności, a zatem także w odniesieniu do pośredników internetowych, a nadto, co oznaczają, ze względu na przejętą w UE metodę regulacyjną sfery praw i wolności wykonywanych w internecie, poszczególne zawarte w tej treści przesłanki tj.: 1) legalności ingerencji; 2) proporcjonalności; 3) pilnej społecznie potrzeby. Nie jest zarazem bez znaczenia, jaki organ lub podmiot zostanie (został) wyposażony w kompetencje do wydawania rozstrzygnięć w tym zakresie oraz okoliczność, czy dopuszczalne jest ograniczenie wypowiedzi *ex ante*, tj. jeszcze przed jej pierwszym publicznym udostępnieniem, oraz ustalenie, jaką rolę w tym systemie odgrywać będą suwerenne państwa i prawo przez nie stanowione. Powziąć można bowiem wątpliwości także co do tego, że nadal efektywnie będą stosowane instytucje i koncepcje wypracowane przez ETPC i TSUE organizujące proces

⁶ Wyrok ETPC z dnia 13 lipca 1995 r. w sprawie Tolstoy Miloslavsky przeciwko Wielkiej Brytanii, skarga nr 18139/91, LEX nr 80421.

⁷ Wyrok SO w Krakowie z dnia 28 grudnia 2018 r., I C 2007/13, LEX nr 2729385.

komunikowania, do których wielokrotnie odwołuje się orzecznictwo, takie jak potrzeba przeciwdziałania „mrozącemu efektowi” (ang. *chilling effect*); możliwość korzystania przez państwa z marginesu swobody przy dokonywaniu oceny dopuszczalności ograniczeń; koncepcja prasy jako „psa stróżującego” (ang. *watchdog*) czy „grubej skóry” w odniesieniu do osób pełniących funkcje publiczne, których działalność została poddana krytyce.

Komisja i Parlament Europejski zdecydowały się na przyjęcie metody pełnej harmonizacji w dziedzinie usług pośrednictwa internetowego. KE uznała, że aby uniknąć fragmentacji prawnej, konieczne jest przyjęcie aktu prawnego rangi rozporządzenia⁸. Ponieważ internet z natury ma charakter transgraniczny, działania legislacyjne na szczeblu krajowym, jak wskazano w AUC, utrudniają świadczenie i odbiór usług na terytorium całej Unii i są nieskuteczne, jeżeli chodzi o zapewnienie bezpieczeństwa i jednakowego poziomu ochrony praw obywateli Unii⁹.

Jako podstawę prawną tej decyzji wskazano art. 114 TFUE¹⁰, który przewiduje ustanowienie środków mających na celu zapewnienie funkcjonowania rynku wewnętrznego¹¹. W uzasadnieniu przyjętej metody regulacyjnej wskazano, że służy ona zapewnieniu prawidłowego funkcjonowania rynku wewnętrznego, w szczególności pod względem świadczenia transgranicznych usług cyfrowych (w szczególności usług pośrednich). Podkreślono, że metoda ta jest konieczna ze względu na potrzebę:

usunięcia przeszkód i zapobieżenia pojawianiu się przeszkód w prowadzeniu takiej działalności gospodarczej wynikających z różnic w sposobie,

⁸ Wniosek AUC, s. 3.

⁹ Tamże, s. 7.

¹⁰ Traktat Ustanawiający Europejską Wspólnotę Gospodarczą (Dz.U. z 2004 r. Nr 90, poz. 864/2 z późn. zm.).

¹¹ P. Polański zauważa, że art. 114 TFUE stanowi ogólną podstawę prawną do wprowadzania harmonizacji, przy czym dla uchwalenia środka harmonizującego wystarczy większość głosów (zob. P. Polański, *Europejskie prawo handlu elektronicznego. Mechanizmy regulacji usług społeczeństwa informacyjnego*, Warszawa 2014, s. 245). Zgodnie z art. 114 TFUE, z zastrzeżeniem, że Traktaty nie stanowią inaczej, Parlament Europejski i Rada, stanowiąc zgodnie ze zwykłą procedurą ustawodawczą i po konsultacji z Komitetem Ekonomiczno-Społecznym, przyjmują środki dotyczące zbliżenia przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich, które mają na celu ustanowienie i funkcjonowanie rynku wewnętrznego.

w jaki opracowywane są przepisy krajowe, uwzględniając fakt, że szereg państw członkowskich przyjęło lub zamierza przyjąć przepisy dotyczące takich kwestii, jak usuwanie nielegalnych treści w internecie, należyta staranność, procedury zgłaszania i działania oraz przejrzystość¹².

Pozostawienie możliwości regulowania działalności pośredników internetowym państwom członkowskim oceniono, wskazując, że „działania legislacyjne na szczeblu krajowym [...] utrudniają świadczenie i odbiór usług na terytorium całej Unii i są nieskuteczne [...]”¹³. Wybór rozporządzenia jako instrumentu regulacji uzasadniono, wskazując, że:

Komisja podjęła decyzję o przedstawieniu wniosku dotyczącego rozporządzenia w celu zapewnienia spójnego poziomu ochrony w całej Unii i uniknięcia rozbieżności utrudniających swobodne świadczenie odnośnych usług na rynku wewnętrznym, a także w celu zagwarantowania jednakowej ochrony praw oraz jednakowych obowiązków przedsiębiorstw i konsumentów na całym rynku wewnętrznym. Jest to konieczne do zapewnienia pewności prawa i przejrzystości¹⁴.

Ta sama podstawa prawna została wskazana przez Komisję w odniesieniu do pełnej harmonizacji przepisów prawa dotyczących bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych. Powołując art. 114 FFUE jako podstawę prawną wyboru rozporządzenia i metody harmonizacji pełnej, Komisja Europejska w uzasadnieniu wniosku kierowanego do Parlamentu Europejskiego w sprawie przyjęcia aktu o rynkach cyfrowych wskazała, że państwa członkowskie, działając samodzielnie, nie mogą osiągnąć celu, jakim jest zapewnienie wszystkim przedsiębiorstwom kontestowalnych i uczciwych rynków w sektorze cyfrowym w całej Unii¹⁵. Przyjęto, że zidentyfikowane problemy można rozwiązać wyłącznie za pomocą aktu ustawodawczego. Rozporządzenie jest ponadto niezbędne ze względu na fakt, że ma ono zastosowanie bezpośrednio w państwach członkowskich, ustanawia

¹² Wniosek AUC, s. 6.

¹³ Tamże, s. 7.

¹⁴ Tamże, s. 8.

¹⁵ Wniosek ARC, s. 6.

ten sam poziom praw i obowiązków dla podmiotów prywatnych, a także umożliwia spójne i skuteczne stosowanie przepisów w transgranicznym, z zasady, pośrednictwie handlowym online. Rozporządzenie jest najbardziej odpowiednim sposobem rozwiązywania zidentyfikowanych problemów dotyczących uczciwości i kontestowalności oraz przeciwdziałania fragmentacji jednolitego rynku podstawowych usług platformowych świadczonych lub oferowanych przez strażników dostępu¹⁶.

Zastosowana metoda harmonizacji pełnej oznacza, że państwa członkowskie nie mogą ustanawiać krajowych przepisów prawnych przewidujących wyższy albo niższy poziom ochrony. Pełna harmonizacja oznacza zupełność przyjętego środka harmonizującego, co oznacza utratę przez państwa członkowskie możliwości podejmowania własnych działań w obszarze objętym harmonizacją¹⁷.

Pełna harmonizacja dotyczy w szczególności obowiązków w zakresie należytej staranności dostawców usług pośrednich (motyw 40 AUC). Należy przez to rozumieć, że ocena adekwatności środków stosowanych przez pośredników internetowych, takich jak w szczególności filtrowanie, blokowanie treści, ograniczanie dostępu w celu zapobieżenia naruszeniom prawa, w tym także zapobieżeniu rozpowszechnianiu treści nielegalnych, powinna w całej Unii opierać się na takich samych przesłankach i prowadzić do jednolitego rezultatu, niezależnie od tego, w jakim państwie dokonywana jest ocena. Zharmonizowane wymogi dotyczą także zasad moderowania treści (motyw 49 AUC), a także mechanizmu „zgłaszania i działania” (art. 16 AUC) oraz stosowania przez sądy krajowe przepisów dotyczących pośredników internetowych, „by ich decyzje nie były sprzeczne z decyzją przyjętą przez Komisję na podstawie rozporządzenia” (motyw 147 AUC).

W motywie 156 AUC ustawodawca europejski deklaruje, że rozporządzenie (AUC) nie narusza praw podstawowych uznanych w Karcie ani praw podstawowych stanowiących ogólne zasady prawa Unii. W związku z tym rozporządzenie – w myśl zawartej w nim dyspozycji – powinno być interpretowane i stosowane zgodnie z tymi prawami podstawowymi, w tym dotyczącymi wolności wypowiedzi i informacji oraz wolności i pluralizmu mediów. Wykonując

¹⁶ Tamże, s. 8.

¹⁷ P. Polański, *Europejskie prawo handlu...*, s. 248.

uprawnienia określone w rozporządzeniu, wszystkie zaangażowane organy publiczne powinny dążyć – w sytuacjach, w których występuje konflikt odpowiednich praw podstawowych – do osiągnięcia właściwej równowagi między danymi prawami zgodnie z zasadą proporcjonalności (motyw 153 AUC).

W sferze deklaracji (oświadczeń, zobowiązań) formalnych, w szczególności zawartych w rozporządzeniach regulujących usługi i rynki cyfrowe, przyjęte rozwiązania nie powinny naruszać wypracowanego i istniejącego poza internetem standardu wolności wypowiedzi. Trudno jednakże z całą pewnością orzec, że ze względu na specyfikę działania internetu i szczególnie sposób aktywności i zapewniania widoczności w internecie oraz wyższą – jak się wydaje – wrażliwość na ingerencje, wypracowany poza internetem standard wolności wypowiedzi będzie do utrzymania także w internecie.

2. Standard negocjowany – rola państw członkowskich

Ocena dopuszczalności ingerencji w wolność wypowiedzi, o ile dotyczy sfery pozacyfrowej, stanowi wypadkową, z jednej strony, wytyczenia granic swobody działania państwa (margines swobody państwa) w zakresie, w jakim państwo może poprzez swe organy ustawodawcze, wykonawcze i sądownicze ingerować w realizację wolności wypowiedzi przysługującej jednostce oraz, z drugiej strony, jest wynikiem wykładni „granicy wolności wypowiedzi” dokonywanej na gruncie art. 10 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności (standard konwencyjny). ETPC dokonując wykładni granicy wolności wypowiedzi, uwzględnia nie tylko treść art. 10 EKPC, lecz także waży potrzeby zapewnienia ochrony gwarantowanej w nim wolności z potrzebą ochrony równoważnych konwencyjnych wartości, jak w szczególności prywatność (art. 8 EKPC) i prawo do równego traktowania (art. 14 EKPC). Trybunał (ETPC) ustalając zakres swobody wypowiedzi, dokonuje indywidualizacji oceny dopuszczalności ingerencji w wolność wypowiedzi, uwzględniając zarówno okoliczności konkretnej sprawy (status autora wypowiedzi, charakter, treść i cel wypowiedzi), jak i uwarunkowania systemowe, społeczne i historyczne państwa, przeciwko któremu skierowana została skarga.

ETPC dopuszcza zatem, by państwo dysponowało pewnym zakresem swobody (margines swobody działania państwa) w zakresie ustalania granic ingerencji w wolność wypowiedzi. Uprawnienia państwa do stosowania środków prawnych ograniczających wolność wypowiedzi wpływają, w ocenie ETPC, nie tylko z treści art. 10 EKPC, który to przepis pozwala przy dokonywaniu oceny dopuszczalności ingerencji w wolność wypowiedzi na uwzględnienie szczególnych uwarunkowań społecznych, kulturowych lub historycznych istniejących w państwie, ale także z treści art. 17 EKPC, który nakłada na państwo pozytywny obowiązek przeciwdziałania rozpowszechnianiu treści nielegalnych, stanowiących mowę nienawiści, które nie korzystają z ochrony konwencyjnej (mechanizm gilotyny). Zgodnie z treścią art. 17 EKPC na ochronę nie zasługują te akty, które „zmierzają do zniweczenia praw i wolności wymienionych w konwencji”. W takim zatem zakresie, w jakim przyznanie ochrony danej wypowiedzi prowadziłoby do „zniweczenia praw i wolności” gwarantowanych w konwencji, Trybunał przyjmuje, że niezbędne jest, by państwo przedsięwzięło środki konieczne do eliminowania takich wypowiedzi z przestrzeni publicznej i przeciwdziałania pojawieniu się ich w przyszłości¹⁸. Art. 17 ma jednak zastosowanie tylko w wyjątkowych okolicznościach i skrajnych przypadkach. W sprawach dotyczących art. 10 Konwencji należy go stosować tylko wtedy, gdy jest całkowicie jasne, że zakwestionowane uwagi miały na celu odwrócenie uwagi od jego rzeczywistego celu poprzez wykorzystanie prawa do wolności wypowiedzi w celach oczywiście sprzecznych z wartościami Konwencji¹⁹.

¹⁸ Kategoryczne wypowiedzi atakujące lub oczerniające całe grupy, czy to etniczne, religijne, czy inne, zasługują na bardzo ograniczoną ochronę na mocy art. 10 Konwencji w związku z art. 17 (zob. podobnie Seurot przeciwko Francji, Soulas przeciwko Francji, §§ 40 i 43–44, wyrok ETPC z dnia 20 kwietnia 2010 r. w sprawie Le Pen przeciwko Francji, skarga nr 18788/09, które dotyczą ogólnych wypowiedzi wrogich muzułmanom we Francji) lub wcale nie zasługują na ochronę (zob. w szczególności Wyrok ETPC w sprawie Norwood przeciwko Wielkiej Brytanii, w związku z oświadczeniami łączącymi muzułmanów w Zjednoczonym Królestwie z atakami terrorystycznymi z 11 września 2001 r.). Stanowisko to jest rezultatem wykładni art. 10 w zw. z art. 14 EKPC i przyjętym na gruncie Konwencji zobowiązaniem do zwalczania dyskryminacji rasowej (zob. Wyrok ETPC z dnia 16 lutego 2021 r. w sprawie Budinova i Chaprazov przeciwko Bułgarii, skarga nr 12567/13, § 94 i przytoczone tam odesłania).

¹⁹ Wyrok ETPC w sprawie Perinçek przeciwko Szwajcarii, §§ 78, 79, 114.

Wobec uwzględnienia przez ETPC, że ustalane na gruncie systemów prawnych poszczególnych państw zakresy wolności wypowiedzi mogą się od siebie różnić, a istnienie tych różnic nie uchyla, co do zasady, istnienia tzw. europejskiego standardu wolności wypowiedzi, zasadne jest stosowanie terminu „standard negocjowany”. Zarazem jednak ze względu na to, że ETPC – powołując się na treść art. 17 EKPC – odmawia rozpoznania skarg na naruszenie art. 10 EKPC w odniesieniu do tych wypowiedzi, które ze względu na ich treść lub formę zmierzają, w ocenie Trybunału, do zniweczenia konwencyjnych wartości, konieczne jest wyodrębnienie tych kategorii, które nie tylko nie mieszczą się w „europejskim standardzie wolności wypowiedzi” i nie podlegają ochronie na gruncie postanowień konwencji, ale – jak sugeruje Trybunał – powinny być zwalczane z tego powodu, że stanowią, w ogólności, zagrożenie dla innych konwencyjnych wartości (mechanizm gilotyny). W odniesieniu do autorów takich wypowiedzi państwo (strona konwencji) nie tylko może podejmować adekwatne środki korzystając z przysługującego mu marginesu swobody, ale ma obowiązek działania w sposób i w zakresie przez nie swobodnie wybranym i niepodlegającym kontroli ze strony Trybunału.

A. Margines swobody państwa

Termin „swobody uznania”, tożsamy znaczeniowo z wyrażeniem „margines swobody państwa”, stanowi konstrukcję, która ze względu na przypisaną mu w orzecznictwie ETPC wagę, stała się nośnikiem treści normatywnych, pomimo że termin ten do 1 sierpnia 2021 r. nie występował w treści europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności. Konstrukcja marginesu uznania państwa została wypracowana przez ETPC na gruncie Konwencji, w szczególności w świetle art. 10 ust. 2, a obecnie została inkorporowana na podstawie Protokołu nr 15²⁰ do preambuły Konwencji²¹. Protokół został przyjęty w 2013 r. i od tego czasu czekał na ratyfikację przez

²⁰ Protokół nr 15 zmieniający konwencję o ochronie praw człowieka i podstawowych wolności, sporządzony w Strasburgu dnia 24 czerwca 2013 r. (Dz.U. z 2021 r., poz. 1879).

²¹ W piśmiennictwie podkreśla się, że koncepcja marginesu oceny w całości została ukształtowana w orzecznictwie Trybunału w wyniku interpretacji postanowień Konwencji (zob. Z. Kotuła, *Protokół 15 do europejskiej konwencji...*, s. 87).

państwa strony Konwencji. Ostatnim krajem, który wyraził zgodę na ratyfikację, były w kwietniu 2021 r. Włochy. Celem wprowadzenia Protokołu było wzmocnienie standardów ochrony praw człowieka²².

Zgodnie z art. 1 Protokołu nr 15, który wszedł w życie dnia 1 sierpnia 2021 r., do tekstu preambuły Konwencji dodano nowy ustęp w następującym brzmieniu: „potwierdzając, że Wysokie Układające się Strony, zgodnie z zasadą subsydiarności, ponoszą główną odpowiedzialność za zapewnienie praw i wolności określonych w niniejszej Konwencji i jej Protokołach oraz że korzystają przy tym z marginesu oceny, pod kontrolą Europejskiego Trybunału Praw Człowieka ustanowionego niniejszą Konwencją”. W ten sposób wpisano do EKPC zasadę subsydiarności i zatwierdzono stosowaną w orzecznictwie konstrukcję marginesu swobody (oceny)²³. Margines oceny odnosi się do zakresu swobody państwa w interpretowaniu postanowień Konwencji, która to swoboda jest jednak ograniczona ze względu na kontrolę sprawowaną przez ETPC nad treścią, wynikiem i sposobem dokonywania wykładni przez krajowe organy wymiaru sprawiedliwości. Zakres i intensywność oraz rezultat kontroli sprawowanej przez ETPC zależy od okoliczności faktycznych sprawy, charakteru danego prawa i braku jego jednolitej wykładni na poziomie europejskim²⁴. Subsydiarność oznacza z kolei, że obowiązek ochrony praw człowieka spoczywa w pierwszej kolejności na państwach, a ETPC powinien być angażowany wyłącznie, gdy nie wypełniają one tego obowiązku lub robią to nieprawidłowo²⁵.

Po raz pierwszy²⁶ termin „margines uznania” został użyty w 1958 r. w raporcie Europejskiej Komisji Praw Człowieka w sprawie Grecja przeciwko Wielkiej Brytanii, która dotyczyła naruszenia praw człowieka podczas wojny partyzanckiej na Cyprze²⁷. W odniesieniu do ustalania granic wolności wypowiedzi

²² S. Kolarz, *Reforma Europejskiego Trybunału Praw Człowieka*, „Biuletyn Polski Instytut Praw Międzynarodowych” 2021, nr 155, s. 1.

²³ W orzecznictwie ETPC, także ze względu na różnorodność tłumaczenia tekstów wydawanych przez ETPC orzeczeń, zamiennie stosowane są także terminy „margines uznania”, „margines oceny”.

²⁴ S. Kolarz, *Reforma Europejskiego Trybunału...*, s. 1.

²⁵ Tamże, s. 1.

²⁶ Z. Kotuła, *Protokół 15 do europejskiej konwencji...*, s. 87.

²⁷ Wyrok ETPC z dnia 17 września 1997 r. w sprawie Grecja przeciwko Wielkiej Brytanii, skarga nr 176/56.

i swobody dokonywania oceny dopuszczalności ingerencji przez organy krajowe państwa strony Konwencji, Trybunał wypowiedział się w sprawie Handyside przeciwko Zjednoczonemu Królestwu²⁸. Wskazano wówczas, że zadaniem Trybunału nie jest w żadnym razie zastępowanie właściwych sądów krajowych, lecz kontrola na podstawie art. 10 orzeczeń wydanych przez nie w ramach przysługującego im uprawnienia do oceny. Jednakże kontrola Trybunału okazywałaby się na ogół iluzoryczna, gdyby ograniczał się on do zbadania tych orzeczeń w oderwaniu od innych, w szczególności wydanych na gruncie EKPC. Trybunał powinien zatem, jak zauważono w uzasadnieniu do orzeczenia w sprawie Handyside, rozpatrywać je w świetle całości sprawy, w tym analizowanej wypowiedzi oraz argumentów i dowodów przedstawionych przez skarżącego w krajowym porządku prawnym, a następnie na szczeblu międzynarodowym. Trybunał musi rozstrzygnąć, na podstawie różnych dostępnych mu danych, czy powody podane przez władze krajowe w celu uzasadnienia podejmowanych przez nie konkretnych środków „ingerencji” są „istotne i wystarczające” w świetle art. 10 ust. 2²⁹. Co do zasady zadaniem Trybunału nie jest porównywanie różnych decyzji wydanych przez organy ścigania i sądy, nawet w pozornie podobnych okolicznościach; i musi on, podobnie jak pozwany rząd, szanować niezawisłość sądów. Co więcej, przede wszystkim Trybunał nie ma do czynienia z rzeczywiście analogicznymi

²⁸ Wyrok ETPC w sprawie Handyside przeciwko Wielkiej Brytanii. Skarżący Richard Handyside był właścicielem wydawnictwa Stage 1 w Londynie, które otworzył w 1968 r. Opublikował on między innymi *The Little Red Schoolbook* (dalej: *Podręcznik Szkolny*). Brytyjskie sądy uznały, że konwencja książki rozpatrywanej jako całość prowadzi do wniosku, że poczucie pewnej odpowiedzialności za wspólnotę – a także za siebie samego – jest, jeśli nie całkowicie nieobecne, to podporządkowane subiektywnie pojmowanemu samorozwojowi dziecka. Dostrzeżono w tym przejaw skłonności do deprawacji i demoralizacji. Za niewłaściwe uznano także, że w podręczniku nie było żadnej wzmianki o nielegalności palenia marihuany. Podobnie w książce nie ma żadnego konkretnego zapisu o nielegalności współżycia seksualnego chłopca, który osiągnął wiek czternastu lat, i dziewczynki, która nie ukończyła jeszcze szesnastego roku życia. Trzeba było pamiętać, że *Podręcznik szkolny* był opracowany w ten sposób, że szukało się części dotyczącej konkretnego zagadnienia, co nie wymuszało czytania go jako całości. Na gruncie EKPC Komisja wyraziła opinię – stosunkiem głosów osiem do pięciu, przy jednym głosie wstrzymującym się – że Sądy krajowe nie naruszyły art. 10 Konwencji. Zatem ani tymczasowe zajęcie, ani przepadek i zniszczenie *Podręcznika* (dziewięć głosów za, cztery przeciwko, jeden wstrzymujący się) nie naruszyły EKPC (pkt 38).

²⁹ Punkt 50 uzasadnienia ETPC w sprawie Handyside przeciwko Wielkiej Brytanii.

sytuacjami³⁰. Rola Trybunału jest dalej idąca niż ustalenie, że w razie ingerencji w wolność wypowiedzi środki zastosowane przez państwo były „przewidziane przez prawo” w rozumieniu Konwencji³¹. Trybunał musi zbadać, czy władze krajowe „musiały” skorzystać ze środków, które zastosowały do osiągnięcia celu, oraz czy nie przekroczyły one krajowego marginesu uznania, co w konsekwencji naruszyło wspólny standard gwarantowany przez autonomiczną koncepcję. W orzeczeniu podkreślono, że funkcje nadzorcze Trybunału zobowiązują go do zwracania najwyższej uwagi na zasady charakteryzujące „społeczeństwo demokratyczne”. Trybunał uznał, że „władze państwowe są, co do zasady, w lepszej pozycji niż sędzia międzynarodowy przy formułowaniu opinii [...] w przedmiocie »niezbędności« »ograniczeń« i »sankcji«” oraz wprost wskazał, że:

art. 10 ust. 2 Konwencji pozostawia jej stronom margines swobody uznania. Margines ten przysługuje zarówno krajowej władzy legislacyjnej [...], jak i organom, w tym organom władzy sądowniczej, których zadaniem jest interpretacja i stosowanie obowiązującego prawa³².

Od momentu wydania wyroku w sprawie Handyside przedstawione w nim tezy dotyczące doktryny marginesu swobody uznania są powtarzane i rozwijane w orzecznictwie Trybunału. Doktryna ta opiera się na założeniu, że sądy krajowe są w stanie lepiej wyważyć będące względem siebie w opozycji interes publiczny i interes jednostki³³. K. Orzeszyna zauważa, że:

u podstaw koncepcji marginesu oceny leżą dwie zasady ogólne prawa międzynarodowego praw człowieka: zasada subsydiarności oraz zasada sytuacyjności³⁴. Zgodnie z pierwszą z nich, funkcją ochrony międzynarodowej jest wspomaganie ochrony krajowej. Sędzia krajowy powinien

³⁰ Tamże, pkt. 56.

³¹ Opinia odrębna sędziego Moslera sporządzona w sprawie Handyside przeciwko Wielkiej Brytanii.

³² Pkt. 48 uzasadnienia ETPC w sprawie Handyside przeciwko Wielkiej Brytanii.

³³ Z. Kotula, *Protokół 15 do europejskiej konwencji...*, s. 85.

³⁴ K. Orzeszyna, *Recenzja monografii A. Wiśniewskiego: Margines oceny w orzecznictwie Europejskiego Trybunału Praw Człowieka*, „Roczniki Nauk Prawnych KUL” 2010, nr 1, s. 244.

więc porównywać regulacje krajowe z międzynarodowymi i stosować te, które gwarantują najszerszy zakres ochrony. Zasada sytuacyjności oznacza z kolei uwzględnianie warunków danego kraju i konkretnych okoliczności. To właśnie z niej wynikają granice korzystania z praw człowieka. Margines oceny pozwala Trybunałowi na elastyczność konieczną dla zachowania równowagi między suwerennością państw a ich obowiązkami wynikającymi z Konwencji³⁵.

Odwoływanie się w orzecznictwie do marginesu uznania prowadziło Trybunał do przeciwnych wniosków, tj. niekiedy Trybunał uznawał, że stosowanie przez państwo środków ingerujących w wolność mieściło się w granicach swobody uznania, podczas gdy innym razem Trybunał dochodził do wniosku, że państwo wykroczyło poza przyznany mu margines swobody oceny, a w konsekwencji zastosowana przez państwo ingerencja była nie do pogodzenia z „europejskim standardem wolności wypowiedzi”³⁶. Czynnikiem warunkującym szerokość krajowego marginesu uznania jest istnienie bądź brak jednolitego standardu (konsensusu) w określonej kwestii³⁷. Istnienie europejskiego standardu, jak w przypadku tzw. europejskiego standardu wolności wypowiedzi zawęża dopuszczalność powoływania się przez państwo na margines uznania w zakresie wydawania rozstrzygnięć obejmujących realizację danego prawa lub wolności. Gdy taki standard istnieje – lub Trybunał oznajmia, że istnieje – zakres krajowych uprawnień ocennych ulega redukcji³⁸

³⁵ Tamże.

³⁶ Zwraca się uwagę, że znaczna liczba i zróżnicowanie kryteriów uwzględnianych przy ustalaniu istnienia i zakresu marginesu swobody uznania w danej sprawie utrudnia – a niekiedy wręcz uniemożliwia – przewidzenie rozstrzygnięcia Trybunału. Ze względu na to, że okoliczności każdego przypadku oraz działania podjęte przez państwa są badane przez Trybunał *ex post*, nie zawsze wiadomo, jak w danych okolicznościach faktycznych powinno zachować się państwo, aby spełnić warunki określone w Konwencji (zob. J. Kratochvíl, *The Inflation of the Margin of Appreciation by the European Court of Human Rights*, „Netherlands Quarterly of Human Rights” 2011, nr 29/3, s. 330, cyt. za: Z. Kotuła, *Protokół 15 do europejskiej konwencji...*, s. 94).

³⁷ H. Wiczanańska, *Oddziaływanie doktryny marginesu uznania na rozstrzyganie konfliktu pomiędzy wolnością wypowiedzi a wolnością sumienia i wyznania w praktyce orzeczniczej Europejskiego Trybunału Praw Człowieka*, „Przegląd Europejski” 2020, nr 2, s. 90.

³⁸ I.C. Kamiński, *Ograniczenia swobody wypowiedzi...*, s. 801.

Zauważa się, że konstrukcja marginesu uznania służyła *de facto* rozstrzygnięciu fundamentalnego dla współczesnych czasów problemu antynomii uniwersalizm–relatywizm³⁹. Pozwalała ona Trybunałowi, w braku oczywistego naruszenia norm Konwencji, dążyć do wyważenia między europejskimi standardami praw człowieka a kulturowymi, społecznymi i religijnymi preferencjami państw i demokratycznej większości ich obywateli⁴⁰.

Odwołanie się przez Trybunał do kompetencji obejmującej ustalanie zakresu, z jakiego może korzystać państwo w ramach marginesu swobody i skonkretyzowanie jego treści w okolicznościach konkretnych, rozstrzyganych przez ETPC spraw, wymusiło na Trybunale dbałość o spójność i niesprzeczność tej koncepcji⁴¹. W konsekwencji wypowiedziom Trybunału dotyczącym marginesu uznania państwa przydaje się niekiedy status doktryny⁴². Przy czym koncepcja marginesu uznania jest równolegle uznawana za metodę interpretacji dopuszczalnych ograniczeń w korzystaniu z praw człowieka⁴³. Wskazuje się, że stanowi ona „specyficzną regułę wykładni Konwencji, która uzupełnia, a nawet modyfikuje klasyczne dyrektywy interpretacyjne”⁴⁴. Metoda ta pozwala na wyznaczenie granicy pomiędzy tym, „co powinno pozostawać w gestii lokalnych społeczności, a tym, co bezwzględnie powinno obowiązywać wszystkie państwa strony”⁴⁵.

³⁹ K. Orzeszyna, *Recenzja monografii...*, s. 244.

⁴⁰ Tamże, s. 245.

⁴¹ Koncepcja marginesu uznania jest rozumiana jako forma oceny i rozstrzygnięcia, w której Trybunał uznaje dyskrejonalność władz krajowych w zakresie sprawowania wymiaru sprawiedliwości na płaszczyźnie wewnętrznej, uwzględniając ją przy wykonywaniu nadzoru nad realizacją przez państwa strony ich zobowiązań wynikających z Konwencji (zob. A. Wiśniewski, *Margines oceny w orzecznictwie Europejskiego Trybunału Praw Człowieka*, Gdańsk 2008, s. 34).

⁴² J. Skrzydło definiuje margines uznania państwa jako zakres swobody zagwarantowany organom krajowym, po wyznaczeniu przez Trybunał standardu kontrolnego właściwego dla okoliczności danej sprawy (zob. J. Skrzydło, *Wolność słowa w orzecznictwie Sądu Najwyższego Stanów Zjednoczonych i Europejskiego Trybunału Praw Człowieka. Analiza porównawcza*, Toruń 2013, s. 115).

⁴³ K. Orzeszyna, *Recenzja monografii...*, s. 244.

⁴⁴ A. Ciżyńska-Pałosz, *Wpływ Europejskiego Trybunału Praw Człowieka na porządek prawny państw-stron Europejskiej Konwencji Praw Człowieka, a koncepcja marginesu oceny. Analiza ze szczególnym uwzględnieniem wyroku Europejskiego Trybunału Praw Człowieka w sprawie Hirst przeciwko Zjednoczonemu Królestwu*, „Przegląd Prawno-Ekonomiczny” 2020, nr 1, s. 10.

⁴⁵ L. Garlicki, *Zakres zobowiązań państwa w świetle orzecznictwa Europejskiego Trybunału Praw Człowieka*, [w:] *Stosowanie prawa międzynarodowego i wspólnotowego*

Znaczenie normatywne koncepcji marginesu uznania ujawnia się zatem zarówno na płaszczyźnie materialnoprawnej, jak i formalnej, przesądzając tak o treści, jak również o sposobie dokonywania ustaleń dotyczących samodzielności (dyskrecjonalności) państw stron Konwencji sprawujących jurysdykcję w zakresie rozstrzygania o prawach i wolnościach człowieka.

Konstrukcja marginesu uznania ujmowana w charakterze doktryny jest opisywana jako „wyraz subsydiarności materialnej, przeciwstawianej subsydiarności proceduralnej, której gwarancją jest z kolei przede wszystkim przesłanka wyczerpania środków krajowych wyrażona w art. 35 Konwencji”⁴⁶. Koncepcja marginesu swobody służy więc także rozgraniczeniu zakresów kompetencji Trybunału i państw stron Konwencji⁴⁷. Istotą zasady subsydiarności jest natomiast zrównoważenie swobody, która przysługuje państwu w zakresie kształtowania własnych stosunków z podlegającymi jego jurysdykcji jednostkami i wynika z przynależnej mu suwerenności.

Zwraca uwagę fakt, że inkorporowanie do preambuły EKPC zasady subsydiarności i marginesu uznania spotkało się z wyraźnym sprzeciwem organizacji pozarządowych. Wyraziły one obawy, czy takie wyróżnienie omawianych zasad spośród innych reguł interpretacyjnych nie doprowadzi do sytuacji, w której państwa, zwłaszcza w kontrowersyjnych pod względem światopoglądowym sprawach, będą powoływać się w postępowaniu przed Trybunałem na zasadę subsydiarności i swobodę uznania, chcąc uniknąć rozstrzygnięcia co do meritum⁴⁸. Niepokój ten wzmacnia poczynione w doktrynie spostrzeżenie, że zakres krajowego marginesu uznania jest determinowany rodzajem dobra uzasadniającego ingerencję, co zdaniem licznych przedstawicieli doktryny stanowi słabość systemu strasburskiego⁴⁹. Skoro rodzaj dobra może rozstrzygać o dopuszczalności albo braku dopuszczalności oparcia się przez Trybunał na jurysdykcji krajowej, to potwierdzone zostaje w ten sposób przekonanie o braku zobiektywizowanych przesłanek ingerencji w wolność wypowiedzi. Brak takich przesłanek z kolei generuje

w *wewnętrznym porządku prawnym Francji i Polski*, M. Granat (red.), Warszawa 2007, s. 4; podobnie: J. Kapelańska-Pręgowska, *Koncepcja tzw. marginesu oceny w orzecznictwie ETPC*, „Państwo i Prawo” 2007, nr 12, s. 87.

⁴⁶ Z. Kotuła, *Protokół 15 do europejskiej konwencji...*, s. 89.

⁴⁷ Tamże, s. 89.

⁴⁸ Tamże, s. 93.

⁴⁹ J. Skrzydło, *Wolność słowa...*, s. 350.

stan niepewności i nieufności wobec systemu prawa, w tym wobec organów sprawujących wymiar sprawiedliwości⁵⁰.

Koncepcja marginesu swobody pozwala w praktyce ETPC na realizację kilku funkcji, stanowiąc *de facto* instrument służący uzasadnianiu dynamicznej, a niekiedy prawotwórczej wykładni postanowień Konwencji⁵¹. Spełnia zarazem funkcję podobną do regulacji o charakterze blankietowym, albowiem w praktyce odsyła do prawa krajowego. Nadto zapewnia trwałość (stabilność) idei (ideologii), utrwalając w państwach Rady Europy przekonanie o niezmienności oraz niezawodności demokratycznego systemu sprawowania rządów. Margines uznania pozwala w ujęciu materialnoprawnym na uwzględnienie przepisu prawa krajowego i jego wykładni, a w ujęciu formalnym na przyjęcie reguł interpretacyjnych zapewniających utrzymanie ciągłości tzw. europejskich standardów, w tym standardu wolności wypowiedzi. I.C. Kamiński zauważa, że margines swobody ocen stanowi „być może najważniejszą konstrukcję związaną z konwencją”⁵². Zarazem zwraca uwagę, że konstrukcja ta „nie odnosi się do metody wykładni konwencji, lecz określa regułę przeglądu, jaką instytucje strasburskie stworzyły w celu ustalenia zakresu oraz intensywności swej kontroli”⁵³.

O ile w doktrynie nie budzi wątpliwości, że ocena dopuszczalności ingerencji w wolność wypowiedzi jest uzależniona od ustalenia przez Trybunał, czy w odniesieniu do konkretnej wypowiedzi, przy uwzględnieniu jej treści, formy, celu oraz okoliczności, w jakich została rozpowszechniona, mogą znaleźć zastosowanie wskazane w art. 10 ust. 2 EKPC klauzule limitacyjne,

⁵⁰ Zwraca się uwagę nie tylko na słabość koncepcji marginesu uznania, lecz także na niefunkcjonalność klauzuli limitacyjnej zawartej w art. 10 ust. 2 EKPC. Trybunał strasburski, jak się wskazuje, w większości przypadków skłonny był zaakceptować krajową kwalifikację celu bądź zgodne stanowisko stron w tej sprawie, ewentualnie dokonać zabiegu polegającego na przesunięciu istoty problemu w kierunku innych elementów klauzuli limitacyjnej (zob. H. Wiczanowska, *Oddziaływanie doktryny...*, s. 89).

⁵¹ Potwierdzeniem prawotwórczego skutku wykładni dokonywanej przez ETPC jest treść Protokołu nr 15, który inkorporuje do preambuły Konwencji zasadę subsydiarności i konstrukcję marginesu uznania. I.C. Kamiński zauważa, że „doktryna marginesu swobody ocen miała być taktycznym posunięciem Trybunału, by nie straszyć państw członkowskich rozszerzaniem przez strasburskich sędziów swoich kontrolnych uprawnień” (zob. I.C. Kamiński, *Ograniczenia swobody wypowiedzi...*, s. 800).

⁵² Tamże, s. 800.

⁵³ Tamże, s. 800.

o tyle sporne pozostawały i nadal pozostają granice dyskrejonalności państwa w sferze limitowania wolności wypowiedzi.

Inkorporowanie konstrukcji marginesu uznania do preambuły Konwencji nie zawsze powinno być postrzegane jako wzmocnienie pozycji państw stron Konwencji. Państwa mogą także, powołując się na konstrukcję marginesu uznania w jej powiązaniu z zasadą subsydiarności, oczekiwać od Trybunału zastępowania w ich kompetencjach normotwórczych. Niemniej prawdopodobne jest także, że dla państw nowe brzmienie Konwencji może stanowić zachętę do podważania jurysdykcji ETPC w toczących się przeciw nim postępowaniach⁵⁴. Może jednak być i tak, że to Trybunał upatrując na gruncie zasady subsydiarności przede wszystkim ciężącego na państwie obowiązku działania (obowiązek pozytywny), w mniejszym stopniu niż dotychczas będzie podejmował aktywność w kierunku budowania europejskich standardów. I.C. Kamiński dostrzegł, na wiele lat przed ratyfikacją Protokołu nr 15, że konstrukcja marginesu swobody oceny jest narzędziem przejściowym, wskazując, że jej zastosowanie jest uzasadnione tylko wówczas, gdy tzw. europejski standard ochrony danej wolności nie został jeszcze wypracowany⁵⁵. Zarazem jednak istnieć mogą takie okoliczności, w szczególności takie rodzaje wypowiedzi, wobec których Trybunał odmówi dokonywania ich oceny, przenosząc obowiązek reagowania na państwa strony Konwencji.

Na tle powyższych spostrzeżeń nie jest bez znaczenia treść zdania pierwszego zawartego w art. 1 Protokołu nr 15, w którym podkreślone zostały obowiązki (a nie uprawnienia) Wysokich Układających się Stron. W zdaniu pierwszym wskazano, że zgodnie z zasadą subsydiarności to właśnie państwa „ponoszą główną odpowiedzialność za zapewnienie praw i wolności określonych w niniejszej Konwencji”. Skoro państwa mają zapewnić realizację wolności i praw, to – *a minori ad maius* – tym bardziej są one zobowiązane do tego, by reagować na zachowania, w tym rozpowszechniane wypowiedzi, które nie tylko nie mieszczą się w standardzie, ale w ogóle nie pozostają pod ochroną Konwencji. W odniesieniu do wolności wypowiedzi chodzi zatem o takie jej rodzaje, które nie tylko nie odpowiadają europejskiemu standardowi, ale – co więcej – są sprzeczne z Konwencją i nie są objęte ochroną

⁵⁴ S. Kolarz, *Reforma Europejskiego Trybunału...*, s. 3.

⁵⁵ I.C. Kamiński, *Ograniczenia swobody wypowiedzi...*, s. 809.

konwencyjną. W takiej sytuacji konstrukcja marginesu swobody nie znajduje zastosowania, albowiem to nie organy konwencyjne, lecz państwo staje się podmiotem wyłącznie odpowiedzialnym za zapewnienie ochrony wartości konwencyjnych. Państwo ma zatem obowiązek działania (obowiązek pozytywny) i nie może być zastępowane w wykonywaniu tego obowiązku przez system organów konwencyjnych.

Konstrukcja marginesu uznania jest – jak celnie spostrzegł I.C. Kamiński – narzędziem przejściowym. Dodać należy, że narzędzie to jest wykorzystywane na etapie nie tylko – na co zwraca uwagę I.C. Kamiński – dochodzenia do europejskiego standardu ochrony (budowanie standardu), ale także ustalania, że ocena na gruncie Konwencji nie jest w ogóle możliwa z tego powodu, że stałaby ona w sprzeczności z wartościami chronionymi w Konwencji, a zatem samo przeprowadzenie oceny stanowiłoby naruszenie istoty chronionych w Konwencji wartości i praw.

Odnosząc powyższe spostrzeżenia do sfery realizacji wolności wypowiedzi, należy zwrócić uwagę, że ETPC stanął na stanowisku, zgodnie z którym nie wszystkie rodzaje wypowiedzi zasługują na ochronę konwencyjną⁵⁶. Na taką ochronę nie zasługują – co do zasady – treści nielegalne, a pośród nich tzw. mowa nienawiści. W orzecznictwie Europejskiego Trybunału Praw Człowieka mowa nienawiści – jak zauważa I.C. Kamiński – staje się nową kategorią wypowiedzi służącą do podjęcia wstępnej decyzji klasyfikacyjnej (identyfikacyjnej), kluczowej dla dalszej analizy ingerencji i finalnie oceny, czy doszło do naruszenia chroniącego swobodę wypowiedzi art. 10 EKPC, a nadto, czy wypowiedź w ogóle podlega ochronie konwencyjnej. Zakwalifikowanie wypowiedzi jako mowy nienawiści ma olbrzymie konsekwencje. Nie tylko pozbawia znaczenia działające na rzecz ochrony wątki i konteksty, ale te przekształcają się w swoiste okoliczności obciążające⁵⁷.

Zastosowana w orzecznictwie EKPC konstrukcja marginesu uznania, a następnie inkorporowanie jej do preambuły Konwencji, co nie tylko potwierdziło jej normatywny charakter, ale zobowiązało Trybunał do jej uwzględniania w przyszłym orzecznictwie, nie stanowi dowodu na stabilizowanie

⁵⁶ Decyzja ETPC w sprawie Belkacem przeciwko Belgii, podobnie Decyzja ETPC w sprawie M'Bala M'Bala przeciwko Francji.

⁵⁷ I.C. Kamiński, *Mowa nienawiści...*, s. 89.

europejskich standardów, w tym standardu wolności wypowiedzi, lecz – przeciwnie – pozwala na dokonywanie ich modyfikacji. Odesłanie do konstrukcji marginesu uznania i powiązanie jej z obowiązkami państw stron konwencji w zakresie zapewnienia ochrony konwencyjnym prawom i wolnościom prowadzą do współdzielenia się przez Trybunał odpowiedzialnością także za kształt standardu wolności wypowiedzi, a w konsekwencji zapowiada (albo co najmniej dopuszcza zmianę) nowe podejście do zasad ochrony wolności, jaką stanowi swoboda wypowiedzi.

Nowość w tym podejściu ujawnia się przede wszystkim w tym, że umawiające się strony, ratyfikując Protokół nr 15, wyraziły zgodę na wzmocnienie roli państw w odniesieniu do normowania praw i wolności, w tym także w sferze oddziaływania na zakres wolności wypowiedzi. Wzmocnienie to nie oznacza jednak ograniczenia kontroli Trybunału w wykonywaniu jego kompetencji kontrolnych w odniesieniu do rozpowszechniania wypowiedzi, które, co do zasady, korzystają z ochrony konwencyjnej, lecz dotyczy przeniesienia na państwa obowiązku reagowania na te wypowiedzi, które nie mieszczą się w tzw. europejskim standardzie oraz obowiązku działania w celu ich wyeliminowania z obiegu publicznego. Chodzi zatem o te wypowiedzi, którym Trybunał odmawia na podstawie art. 17 EKPC udzielenia ochrony, odrzucając przyjęcie sprawy do rozpoznania. Trybunał stoi bowiem na stanowisku, że rozpoznanie sprawy stanowiłoby potwierdzenie prawa autora wypowiedzi „do uczestniczenia w działalności lub popełnienia czynu mającego na celu zniweczenie któregośkolwiek z praw i wolności wskazanych w Konwencji”⁵⁸. Odmowa Trybunału wywołuje ten skutek, że ciężar działania zostaje przeniesiony w całości na państwo stronę konwencji. O ile zatem na gruncie EKPC konstrukcja marginesu uznania uruchamia mechanizm negocjowania z państwem kształtu, *in concreto*, standardu wolności wypowiedzi w danej sprawie, o tyle decyzja o odmowie na podstawie art. 17 EKPC przyjęcia przez Trybunał sprawy do rozpoznania przenosi na państwo obowiązek zastosowania środków służących reagowaniu i eliminowaniu nieobjętych ochroną konwencyjną wypowiedzi, generując po stronie państwa obowiązki pozytywne.

Zasadniczą funkcją konstrukcji marginesu uznania niezależnie od powyżej wskazanych, jest uzasadnienie zastosowania dychotomicznego podziału

⁵⁸ Decyzja ETPC w sprawie M'Bala M'Bala przeciwko Francji.

na sferę wypowiedzi objętych ochroną konwencyjną i rozróżnienie jej od wypowiedzi nieobjętych taką ochroną, a zatem tzw. nielegalnych treści.

Wskazać należy w tym miejscu w celu uchylenia ewentualnych zarzutów dotyczących mieszania porządków prawnych, tj. porządku przyjętego na gruncie Rady Europy i porządku prawnego UE, że Unia przejęła jako własny dorobek strasburskiego Trybunału wypracowany na gruncie europejskiej Konwencji o ochronie praw człowieka i obywatela. W preambule Karty Praw Podstawowych⁵⁹ stanowiącej załącznik nr 1 do Traktatu z Lizbony⁶⁰ wskazano, że „Karta potwierdza, przy poszanowaniu kompetencji i zadań Unii oraz zasady pomocniczości, prawa wynikające zwłaszcza z tradycji konstytucyjnych i zobowiązań międzynarodowych wspólnych Państwom Członkowskim, a także europejskiej Konwencji”. W art. 52 ust. 3 KPP postanowiono, że „W zakresie, w jakim niniejsza Karta zawiera prawa, które odpowiadają prawom zagwarantowanym w europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności, ich znaczenie i zakres są takie same jak praw przyznanych przez tę konwencję”⁶¹. Regulacja ta pozwala TSUE

⁵⁹ Karta praw podstawowych Unii Europejskiej (Dz.U. UE. C z 2007 r. Nr 303, s. 1 z późn. zm.).

⁶⁰ Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską, sporządzony w Lizbonie dnia 13 grudnia 2007 r. (Dz.U. z 2009 r. Nr 203, poz. 1569).

⁶¹ Należy zwrócić jednak uwagę – za A. Wróblem – że w dotychczasowym orzecnictwie TS przyjmował niekiedy koncepcję relatywną, gdy twierdził – w odniesieniu jednakże do praw i wolności gwarantowanych EKPC – że: „Tak więc odmiennie od innych praw podstawowych zapisanych w tej konwencji, takich jak prawo każdego człowieka do życia lub zakaz poddawania torturom i niehumanitarnemu lub poniżającemu traktowaniu albo karaniu, które nie podlegają żadnym ograniczeniom, prawo do swobody wypowiedzi i pokojowego zgromadzania się zagwarantowane w EKPC nie stanowią prerogatyw o charakterze absolutnym i powinny być oceniane w świetle ich funkcji społecznej. Wykonanie tych praw może być więc przedmiotem ograniczeń w zakresie, w jakim ograniczenia te są rzeczywiście podyktowane względami interesu ogólnego i nie stanowią dysproporcjonalnej i niedopuszczalnej ingerencji naruszającej istotę chronionych praw, przy uwzględnieniu celu realizowanego przez te ograniczenia” (wyrok TS z dnia 12 czerwca 2003 r. w sprawie Eugen Schmidberger, Internationale Transporte und Planzüge przeciwko Austrii, C-112/00, pkt 80). Koncepcja relatywna tym różni się od koncepcji absolutnej, że „koncepcji absolutnej istota prawa i wolności jest wyznaczona sztywną, abstrakcyjną granicą, poza którą nigdy i w żadnych okolicznościach wykroczyć nie wolno, gdy tymczasem teoria relatywna wyznacza granice zmienne w zależności od kontekstu, w jakim regulacja ograniczająca jest badana” (zob. A. Wróbel, *Komentarz do art. 52*, s. 528). Zarazem spostrzega się, że w procesie orzekania TSUE „preferowanie jakiegoś typu

na uznanie dorobku orzeczniczego ETPC i jego samodzielne rozwinięcie. Po wejściu w życie KPP i w zgodzie z jej postanowieniami TSUE uwzględniła orzecznictwo ETPC, zwiększając tym samym katalog argumentów, które są wykorzystywane w procesie interpretacji Karty⁶².

Pojęcie nielegalnych treści na gruncie pakietu cyfrowego oznacza:

informacje, które same w sobie lub przez odniesienie do działania, w tym sprzedaży produktów lub świadczenia usług, nie są zgodne z prawem Unii lub z prawem jakiegokolwiek państwa członkowskiego, które jest zgodne z prawem Unii, niezależnie od konkretnego przedmiotu lub charakteru tego prawa.

Adresatem norm zawartych w AUC, co należy mieć na uwadze, są pośrednicy internetowi. Jednakże termin „nielegalne treści” jest używany także poza obszarem działalności pośredników internetowych i obejmuje, co wynika wprost z motywu 12 AUC:

informacje niezależnie od ich formy, które zgodnie z obowiązującym prawem są albo same w sobie nielegalne, takich jak nielegalne nawoływanie do nienawiści lub treści o charakterze terrorystycznym i niezgodne z prawem treści dyskryminujące, albo które stają się nielegalne na mocy obowiązujących przepisów ze względu na fakt, iż odnoszą się one do nielegalnych działań. [...] W tym zakresie nie ma znaczenia, czy nielegalny charakter informacji lub działania wynika z prawa Unii, czy z prawa krajowego, które jest zgodne z prawem Unii, oraz jaki jest dokładny charakter lub przedmiot danego prawa.

Obowiązek wykrywania nielegalnych treści, a także obowiązek podejmowania skutecznych środków przeciw nielegalnym treściom został przeniesiony na państwa członkowskie UE. Odpowiednie organy krajowe, jak wskazano w motywie 34 AUC, powinny mieć możliwość wydawania nakazów

argumentacji nie jest stałe i zmienia się wraz z ewolucją UE, jej prawa i organów, a także w zależności od rozpatrywanego przypadku” – zob. L. Leszczyński (red.), *Wykładnia prawa Unii Europejskiej*, t. 3, Warszawa 2019, s. 278 (System Prawa Unii Europejskiej).

⁶² L. Leszczyński (red.), *Wykładnia prawa...*, s. 284.

w odniesieniu do treści uznanych za nielegalne lub nakazów udzielenia informacji na podstawie prawa Unii lub prawa krajowego zgodnego z prawem Unii, w szczególności z Kartą, i kierowania tych nakazów do dostawców usług pośrednich. Na organach krajowych spoczywa także obowiązek uzasadnienia wyjaśniającego, dlaczego dana informacja stanowi nielegalne treści (motyw 34 AUC). Wprowadzono także kategorię „oczywiście nielegalnych treści”, wobec których działania państwa powinny być bardziej zdecydowane i podejmowane szybciej. Informacje należy uważać za stanowiące oczywiście nielegalne treści, jeżeli dla osoby nieposiadającej wiedzy fachowej jest oczywiste, bez przeprowadzenia jakiegokolwiek merytorycznej analizy, że treści są nielegalne (motyw 63 AUC).

B. Mechanizm gilotyny

„Mechanizm gilotyny” oznacza odwołanie się przez organ wymiaru sprawiedliwości do instytucji nadużycia prawa wskazanej w art. 17 EKPC, a w konsekwencji odmowę merytorycznego rozpoznania i wydania rozstrzygnięcia w skierowanej do niego sprawie⁶³. Chodzi zatem o taki sposób załatwienia sprawy, który w miejsce udzielenia ochrony i zastosowania w tym celu odpowiednich środków, oczekiwanych przez wnioskodawcę (skarżącego), nie tylko odmawia ich zastosowania, ale w ogóle odmawia rozpoznania istoty sprawy, wskazując na nadużycie prawa po stronie wnioskodawcy. Rozpoznanie sprawy,

⁶³ Odmiernym instrumentem prawnym, który jednak wywołuje podobny skutek, tj. nierozpoznanie merytoryczne skargi, jest jej odrzucenie. Skarga może zostać odrzucona jako naruszająca art. 35 ust. 3 Konwencji m.in. w sytuacji, jeżeli została oparta na nieprawdziwych faktach (patrz Wyroki ETPC: z dnia 5 października 2000 r. w sprawie Varbanov przeciwko Bułgarii, skarga nr 31365/96, § 36; z dnia 17 stycznia 2006 r. w sprawie Popov przeciwko Mołdawii (nr 1), skarga nr 74153/01, § 48, z dnia 18 maja 2004 r. w sprawie Řehák przeciwko Czechom, skarga nr 67208/01; oraz z dnia 2 maja 2006 r. w sprawie Kéréthachvili przeciwko Gruzji, skarga nr 5667/02). Niepełne, a tym samym mylne informacje również mogą stanowić nadużycie prawa do skargi, zwłaszcza jeżeli informacje te dotyczą istoty sprawy, a nie podano wystarczających powodów nieujawnienia takich informacji (zob. Wyroki ETPC: z dnia 9 czerwca 2006 r. w sprawie Hüttner przeciwko Niemcom, skarga nr 23130/04; z dnia 3 lipca 2007 r. w sprawie Poznański i in. przeciwko Niemcom, skarga nr 25101/05; z dnia 2 grudnia 2008 r. w sprawie Predescu przeciwko Rumunii, skarga nr 21447/03, §§ 25–26; oraz z dnia 18 września 2012 r. w sprawie Kowal przeciwko Polsce, skarga nr 2912/11).

w ocenie Trybunału na gruncie dokonywanej przez ETPC wykładni art. 17 EKPC, niweczyłoby prawa i wolności chronione w Konwencji.

Generalnym celem art. 17 Konwencji jest zapobieganie wykorzystywaniu przez grupy totalitarne zasad uznanych w Konwencji do własnych celów. Aby go osiągnąć, niekoniecznie należy pozbawić każdego z gwarantowanych przez Konwencję praw i wolności te osoby, co do których ustalono, że są zaangażowane w działalność skierowaną na zniweczenie któregośkolwiek z tychże praw i wolności. Art. 17 dotyczy zasadniczo tych praw, które – gdy powołać się na nie – będą ułatwiać próbę wyprowadzenia z nich prawa osobistego zaangażowania w działania zmierzające do zniweczenia któregośkolwiek z praw i wolności wskazanych w Konwencji⁶⁴. Jakkolwiek w orzecznictwie ETPC postrzega się wagę wolności wyrażania opinii w społeczeństwie demokratycznym, to jednak Trybunał wyznacza również jej granice, co sprawia, iż niektóre wypowiedzi nie korzystają z dobrodziejstwa ochrony z art. 10 Konwencji⁶⁵. Art. 17 EKPC jest bowiem przepisem, który eliminuje możliwość użycia konwencyjnych praw i wolności do działań zmierzających do zniszczenia demokratycznego sposobu rządzenia i sprawowania władzy. Innymi słowy – nie ma wolności dla wrogów wolności⁶⁶.

Art. 17 EKPC, jak zauważa Trybunał, znajduje zastosowanie jedynie wyjątkowo i w sytuacjach krańcowych. Jego celem jest uniemożliwienie wykonywania prawa konwencyjnego, którego skarżący chce dochodzić w skardze do Trybunału. W sprawach dotyczących art. 10 Konwencji artykuł ten powinien być stosowany jedynie wówczas, gdy jasne jest, że przedmiotowe wypowiedzi miały na celu odejście od jego faktycznego celu poprzez wykorzystanie prawa do wolności wypowiedzi w sposób jednoznacznie sprzeczny z wartościami Konwencji. Kwestią rozstrzygającą w świetle art. 17 jest to, czy celem wypowiedzi skarżącego było podżeganie do nienawiści lub przemocy, lub czy poprzez takie wypowiedzi skarżący dążył do powołania się na Konwencję w sposób pozwalający mu na prowadzenie działalności lub popełnianie czynów w zamiarze zniweczenia praw i wolności w Konwencji chronionych⁶⁷.

⁶⁴ Decyzja ETPC w sprawie W.P. przeciwko Polsce.

⁶⁵ Decyzja ETPC w sprawie Belkacem przeciwko Belgii.

⁶⁶ I.C. Kamiński, *Pojęcie „mowy nienawiści”...*, s. 20.

⁶⁷ W sprawie zakończonej wydaniem przez ETPC decyzji z dnia 27 czerwca 2017 r. skarżący opublikował na platformie [internetowej] YouTube serię filmów, w których

Trybunał zastosował art. 17 Konwencji, wyłączając niektóre wypowiedzi spod ochrony przyznanej przez art. 10 w sprawach dotyczących wypowiedzi negujących Holokaust lub jego organizację przez Hitlera⁶⁸; zarzucanie Żydom prześladowań Polaków⁶⁹, plakat kojarzący wszystkich muzułmanów z poważnym aktem terroryzmu⁷⁰, a także w sprawach dotyczących publikacji lub przedstawień uznanych za antysemickie i negujące Holokaust⁷¹. Wezwanie do dyskryminacji jest wezwaniem do nietolerancji, która wraz z wezwaniem do przemocy i nienawiści stanowi jedną z granic, których w żadnym wypadku nie wolno przekraczać w korzystaniu z wolności słowa⁷². I.C. Kamiński zauważa, że Trybunał powołując się na art. 17 EKPC, uruchamia mechanizm gilotyny, wyłączając spod konwencyjnej ochrony „mowę nienawiści”. Chodzi zatem o te wypowiedzi, które ze względu na treść, intencje mówcy albo wywołany skutek (nawoływanie do nienawiści, podżeganie do przemocy, usprawiedliwianie przemocy) zostały ocenione jako sprzeczne z celami Konwencji, a wobec powyższego nie zasługują na ochronę na podstawie zawartych w niej przepisów⁷³.

W strasburskim orzecznictwie dała się zarazem zauważyć gotowość, by rezygnować z traktowania art. 17 jako „normatywnej gilotyny”, a korzystać

wzywał widzów do dominacji na osobami niebędącymi muzułmanami, aby dać nie-muzułmanom nauczkę i z nimi walczyć. Trybunał nie miał żadnych wątpliwości co do silnie nienawistnego wydźwięku wypowiedzi skarżącego i zgodził się z wnioskiem sądów krajowych, zgodnie z którym skarżący dążył, za pomocą przedmiotowych filmów, do rozpowszechniania nienawiści, dyskryminacji i stosowania przemocy w stosunku do wszystkich osób, które nie są muzułmanami (Decyzja ETPC w sprawie Belkacem przeciwko Belgii).

⁶⁸ Wyrok ETPC w sprawie Garaudy przeciwko Francji i w sprawie Witzsch przeciwko Niemcom.

⁶⁹ W sprawie skarżącymi były osoby, które podjęły próbę zarejestrowania „Stowarzyszenia Polskich Ofiar Bolszewizmu i Syjonizmu”. Trybunał zgodził się z rządem, że niektóre stwierdzenia zawarte w akcie założycielskim stowarzyszenia dotyczące prześladowania Polaków przez mniejszość żydowską i nierówności między nimi mogą być postrzegane jako odradzający się antysemityzm. Ponadto rasistowskie postawy skarżących zostały uwidocznione w antysemickim wydźwięku niektórych ich wystąpień przed Trybunałem (zob. Decyzja ETPC w sprawie W.P. przeciwko Polsce).

⁷⁰ Wyrok ETPC w sprawie Norwood przeciwko Wielkiej Brytanii.

⁷¹ Decyzja ETPC z dnia 20 lutego 2007 r. w sprawie Paweł Iwanow przeciwko Rosji, skarga nr 35222/04, oraz Wyrok ETPC w sprawie M'Bala M'Bala przeciwko Francji.

⁷² Wyrok ETPC z dnia 11 czerwca 2020 r. w sprawie Baldassi i in. przeciwko Francji, skarga nr 15271/16 i 6 innych, § 64.

⁷³ I.C. Kamiński, *Mowa nienawiści...*, s. 12.

z niego jako przepisu identyfikującego „wzmocnione” uprawnienie państwa do dokonania ingerencji, czy też konieczność ingerencji, którą państwo musi wykazać ze względu na treść art. 10 ust. 2 (trójelementowy test zgodności ingerencji z Konwencją)⁷⁴. Trybunał zauważa zatem, że nie jest powołany do badania, czy w odniesieniu do konkretnych zarzutów kierowanych pod adresem oskarżonych o przestępstwa znieważenia lub zniesławienia, w tym także w postaci publicznego znieważania osoby lub grupy osób ze względu na ich pochodzenie, przynależność lub brak przynależności do danej wspólnoty, narodu, rasy lub religii, wypełnione zostały znamiona opisanego w prawie krajowym występkę. To przede wszystkim do organów władzy krajowej, zwłaszcza sądów, należy wykładnia i stosowanie prawa krajowego. Zadaniem Trybunału jest jedynie kontrola w świetle art. 10 rozstrzygnięć wydanych przez właściwe sądy krajowe zgodnie z przysługującą im swobodą decyzyjną⁷⁵.

W świetle orzecznictwa Trybunału na gruncie art. 10 i art. 17 EKPC zadania państwa w zakresie kształtowania standardu wolności wypowiedzi polegają nie tylko na kontroli następczej, w szczególności ustalaniu okoliczności faktycznych i oceny, czy wobec zebranych dowodów doszło do wypełnienia znamion czynu zabronionego, ale także przeciwdziałania popełnianiu występków z użyciem słowa. Trybunał wyraził na tle powyższych przepisów pogląd, że „co do zasady w społeczeństwach demokratycznych można uznać za konieczne sankcjonowanie, a nawet zapobieganie wszelkim formom wypowiedzi, które propagują, podżegają, promują lub usprawiedliwiają nienawiść opartą na nietolerancji (w tym nietolerancję religijną), jeżeli zadba się o to, by nałożone »formalności«, »warunki«, »ograniczenia« lub »sankcje« były proporcjonalne do zamierzonego zgodnego z prawem celu”. Właściwe organy, działające w charakterze gwarantów instytucjonalnego porządku publicznego, mogą przyjąć środki, w tym środki karne, mające na celu odpowiednią

⁷⁴ I.C. Kamiński, *Pojęcie „mowy nienawiści”...*, s. 20.

⁷⁵ Stanowisko to Trybunał zajął w sprawie, której przedmiotem był skecz (satyra) o wymowie antysemitkiej. Skarżący oddał hołd osobie, która jest znana we Francji ze swych negacjonistycznych poglądów, i która była z tego powodu skazana przez sąd karny, a następnie zachęcała publiczność do „gorącego” aplauzu i odgrywała wręczenie mu „nagrody za niepokorność i odwagę”. Trzeba wskazać, że krajowym sądem karnym, iż skarżący bezspornie postrzegał te czynności i wypowiedzi w pozytywnym świetle. Trybunał zauważył, że w czasie tego znieważającego skeczu program przerodził się w wiec i przestał być formą rozrywki (zob. Decyzja ETPC w sprawie M'Bala M'Bala przeciwko Francji).

i nienadmierną reakcją na takie uwagi⁷⁶. Podżeganie do nienawiści niekoniecznie wiąże się z użyciem konkretnego aktu przemocy lub innego czynu przestępczego. Ataki na osoby polegające na znieważaniu, wyśmiewaniu lub zniesławianiu pewnych grup społecznych mogą wystarczyć, aby władze nadały priorytet walce z rasistowskimi wypowiedziami nad nieodpowiedzialnie wykorzystywaną wolnością słowa⁷⁷.

Zastosowanie przez ETPC mechanizmu gilotyny poprzez nieprzyjęcie do rozpoznania skargi z powołaniem się na art. 17 EKPC ze względu nadużycie prawa po stronie skarżącego wywołuje skutki formalne i kończące drogę sądową, ale także materialnoprawne polegające na potwierdzeniu statusu wypowiedzi jako nielegalnej, a zatem obligującej organy państwowe do przeciwdziałania jej dalszemu rozpowszechnieniu i wyeliminowaniu jej z obiegu publicznego, a nadto na napiętnowaniu autora wypowiedzi lub innej osoby, która przyczyniła się do jej rozgłoszenia. Powołanie się przez ETPC na treść art. 17 Konwencji i motywy uzasadnienia tego stanowiska stanowią, w efekcie, materialnoprawną przesłankę uzasadniającą ściganie sprawców dopuszczających się rozgłaszania albo pochwalania zakwestionowanych przez ETPC wypowiedzi.

W konsekwencji „mechanizm gilotyny” może uzasadniać i usprawiedliwiać podejmowanie przez organy państwowe działań o charakterze prewencyjnym. Materialnoprawnym skutkiem zastosowania mechanizmu gilotyny jest więc także potwierdzenie kompetencji państwa do zastosowania środków ochrony prewencyjnej, a zatem do stworzenia i stosowania instrumentów monitorowania treści i ich weryfikowania pod kątem zgodności z europejskim standardem wolności wypowiedzi i dopuszczalności objęcia takich wypowiedzi w przyszłości, w razie zaistnienia sporu, kontrolą konwencyjną. O ile zatem w odniesieniu do wypowiedzi mieszczących się w europejskim standardzie państwo jest uprawnione do stosowania wyłącznie środków ochrony następczej (*ex post*), o tyle w odniesieniu do „wypowiedzi nielegalnych” (treści nielegalnych) dopuszczalna wydaje się, w świetle wypowiedzi ETPC, kontrola prewencyjna (*ex ante*).

⁷⁶ Wyrok ETPC z dnia 5 grudnia 2019 r. w sprawie Tagijew i Huseynov przeciwko Azerbejdżanowi, skarga nr 13274/08, § 38 i przytoczone tam odesłania.

⁷⁷ Wyrok ETPC z dnia 11 lutego 2020 r. w sprawie Atamanczuk przeciwko Rosji, skarga nr 4493/11, § 52, § 114.

Zastosowanie powyższej reguły na gruncie polskiego prawa, ze względu na treść art. 54 ust. 2 Konstytucji RP⁷⁸, wymagałoby – jak należałoby postulować – uprzedniej kontroli dokonanej przez Trybunał Konstytucyjny. Zgodnie bowiem z art. 54 ust. 2 Konstytucji zakazana jest cenzura przewencyjna środków społecznego przekazu oraz koncesjonowanie prasy. Cenzura, zgodnie z zasadami doktryny, jest realizowana przez organy administracyjne dla potrzeb władz państwowych⁷⁹. Cenzura *sensu stricto* to znajdujące się w rękach władzy państwowej narzędzie kształtowania i utrzymywania pewnej ideologii; dotyczy wszelkich środków komunikacji społecznej, w szczególności zaś prasy⁸⁰.

Środkiem zaradczym, a zarazem służącym oddaleniu ewentualnych zarzutów dotyczących wprowadzania przez organy europejskie mechanizmu cenzury, jest scedowanie na podmioty prywatne kompetencji w zakresie działań wykrywczych polegających na monitorowaniu nielegalnych treści, ich przewencyjnemu usuwaniu albo blokowaniu poprzez uniemożliwienie autorom takich wypowiedzi ich rozgłaszania, jeszcze zanim trafiły do obiegu publicznego. W konsekwencji to nie organy państwowe, ale podmioty prywatne w porozumieniu z państwem stosować mają wskazane powyżej środki w celu osiągnięcia pożądanego przez organy państwowe (organy unijne) skutku. O ile zrealizowanie zarysowanego powyżej konceptu jest trudne w odniesieniu do wypowiedzi rozgłaszanych w warunkach wymagających osobistej styczności nadawcy i odbiorcy komunikatu, o tyle jego zrealizowanie jest możliwe w środowisku cyfrowym (w internecie). Komunikowanie w internecie ze względu na niezbedność korzystania przez komunikujące się strony z usług pośredników internetowych, w szczególności usługi dostępu do internetu, usługi transmisji danych (*mere conduit*), cachingu oraz hostingu stwarza zarówno techniczne, jak i organizacyjne możliwości śledzenia przepływu informacji i opinii oraz analizy, tak pod kątem jakościowym, jak i ilościowym, zasobów informacyjnych i baz danych.

Zmiana europejskiego standardu wolności wypowiedzi polega zatem nie tylko na generowaniu nowych kategorii wypowiedzi, jak w szczególności

⁷⁸ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. Nr 78, poz. 483 z późn. zm.).

⁷⁹ E. Nowińska, *Wolność wyrażania poglądów a cenzura przewencyjna. Próba interpretacji Konstytucji*, [w:] *Wolność wypowiedzi prasowej*, Warszawa 2007, s. 50.

⁸⁰ Tamże, s. 50.

„treści nielegalne”, w tym mowa nienawiści, i odmowie udzielenia ochrony takim wypowiedziom, ale także na poszerzeniu katalogu uprawnień państwa w zakresie kształtowania wolności wypowiedzi oraz ciążących na państwie pozytywnych obowiązków związanych z reagowaniem na nielegalne treści oraz ich eliminowaniem i przeciwdziałaniem ich rozpowszechnieniu. Zmiana standardu wolności wypowiedzi ujawnia się także w sposobie autodefiniowania swojej roli przez organy europejskie, zarówno ustawodawcze, jak i wykonawcze, które ze strażnika praw i wolności stają się arbitrem i nadzorcą. Znany dotychczas standard wolności wypowiedzi będący rezultatem konsensualnych ustaleń trybunałów europejskich próbujących godzić pozostające niekiedy w kolizji interesy wspólnoty europejskiej i poszczególnych państw (standard negocjowany) jest obecnie zastępowany państwową, jednowymiarową koncepcją wolności wypowiedzi, w której kluczowe miejsce zajmuje definicja terminu „nielegalne treści”, przy czym wdrożenie tej koncepcji w obrębie jednolitego rynku cyfrowego zlecono podmiotom prywatnym, tj. pośrednikom internetowym (standard kontraktowy).

3. Standard kontraktowy

Akt o usługach cyfrowych i akt o rynkach cyfrowych, pomimo że oba posiadają formę aktu ustawodawczego, co powinno przesądzać o zakresie terytorialnym, temporalnym oraz przedmiotowym i podmiotowym zawartych w nich norm postępowania, to jednak, ze względu na założoną w tych aktach prawnych elastyczność regulacji oraz nowe mechanizmy i reguły postępowania przewidziane zarówno dla Komisji Europejskiej (uprawnienie do wydawania aktów delegowanych, wytycznych oraz aktów wykonawczych), jak też dla pośredników internetowych, a także ze względu na skutek, jaki powstaje w związku z ich zastosowaniem, zbliżają te akty prawne do formuły kontraktu, który zakłada, że strony ułożonego w nim stosunku prawnego realizują cele interesu publicznego, jednakże przy pomocy i z korzyścią dla partnerów prywatnych.

Użycie formuły „kontraktowy standard wolności wypowiedzi” oznacza, co może budzić wątpliwości natury prawnej, że wolność wypowiedzi stała się przedmiotem umowy (kontraktu) zawartej pomiędzy równoprawnymi podmiotami. W konsekwencji zakres swobody wypowiedzi stałby się rezultatem „umówionego standardu”, na który składają się zobowiązania wzajemne stron do takiego zachowania, które modyfikuje ogólny, wypracowany na gruncie wykładni prawa konwencyjnego (EKPC), traktatowego (TFUE) i prawa krajowego państw członkowskich UE, standard wolności wypowiedzi. O ile poza sporem pozostaje, że jednostronne oświadczenie woli złożone przez jednostkę w przedmiocie samoograniczenia się w wykonywaniu swobody wypowiedzi mieści się w granicach prawa⁸¹, o tyle wątpliwości może budzić taki sposób normowania praw wolnościowych, w tym wolności wypowiedzi, który przyznaje innym podmiotom, w szczególności organom publicznym, kompetencje do kształtowania zakresu cudzej wolności wypowiedzi i nadto upoważnia je do ustalania standardu wolności wypowiedzi oraz egzekwowania go przy pomocy podmiotów prywatnych. Spostrzeżenia te nie dowodzą jednak ani tego, że wolność wypowiedzi została poddana prawnej reglamentacji, ani także tego, że standard wolności wypowiedzi w internecie jest odmienny od standardu wypracowanego na gruncie EKPC i ustawodawstwa państw członkowskich UE (klasyczny standard wolności wypowiedzi).

W niniejszej części rozprawy poddano weryfikacji powyższe hipotezy, zmierzając do ustalenia, czy konstruowanie standardu wolności wypowiedzi na gruncie rozporządzeń cyfrowych odzwierciedla klasyczny jego model oraz mając na celu zidentyfikowanie mechanizmów i narzędzi oddziałujących na jego utrzymanie lub zmianę.

⁸¹ Przykładem kontraktu, którego treścią jest samozwiązanie się (samoograniczenie) strony odnośnie do zakresu wykonywanych przez nią praw wolnościowych, jest umowa o poufność (zob. J. Taczowska-Olszewska, *Dostęp do informacji publicznej w polskim systemie prawnym*, Warszawa 2014, s. 208).

A. Kształtowanie treści stosunku prawnego – dialog regulacyjny

KE negocjowała z pośrednikami internetowymi zakresy ich przyszłych obowiązków, zanim doszło do przekazania Parlamentowi Europejskiemu wniosku o uchwalenie rozporządzeń cyfrowych⁸². Ustalanie ostatecznego kształtu rozwiązań zawartych w rozporządzeniach cyfrowych było poprzedzone także konsultacjami społecznymi⁸³, a dostawcy usług cyfrowych wypowiadali również swoje stanowisko, w szczególności poprzez przyjęcie dobrowolnych kodeksów etycznych⁸⁴. Zarazem w dokumentach KE przyznano, że wniosek Komisji dotyczący aktu o usługach cyfrowych ustanawia współregulacyjny mechanizm ochronny⁸⁵. Podobnie w samym wniosku ustawodawczym Komisja potwierdziła potrzebę utrzymania mechanizmu współregulacji na rynku usług pośrednictwa internetowego. Komisja wskazała, że w akcie o usługach

⁸² ARC, s. 8–9.

⁸³ Od dnia 2 czerwca do dnia 8 września 2020 r. Komisja przeprowadziła dwie osobne edycje otwartych konsultacji publicznych, które dotyczyły dwóch osobnych wstępnych ocen skutków: po pierwsze pakietu w ramach aktu o usługach cyfrowych – oceny instrumentu regulacyjnego *ex ante* dla dużych platform internetowych o znaczących efektach sieciowych pełniących funkcję strażników dostępu na rynku wewnętrznym Unii Europejskiej. Po drugie Komisja przeprowadziła konsultacje z zainteresowanymi stronami dotyczące sprawozdań pośrednich opracowanych przez Obserwatorium Gospodarki Platform Internetowych i wspierające bieżącą inicjatywę (zob. Wyniki konsultacji z zainteresowanymi stronami i ocen skutków, <https://digital-strategy.ec.europa.eu/en/policies/eu-observatory-online-platform-economy> (dostęp: 10.06.2024)).

⁸⁴ Kodeks postępowania w zakresie dezinformacji ustanowiono w październiku 2018 r. Proces jego rewizji został rozpoczęty w czerwcu 2021 r., a jego zwieńczeniem było podpisanie i przedstawienie go 16 czerwca 2022 r. przez 34 sygnatariuszy. Spełnia on założenia Wytycznych Komisji przedstawionych w maju 2021 r., <https://disinfocode.eu/pl/wprowadzenie-do-kodeksu/> (dostęp 10.10.2023). Jak zapowiedziano w europejskim planie działania na rzecz demokracji (EDAP) (*Protecting democracy*, Komisja Europejska, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan_en dostęp 10.10.2023), w wytycznych odniesiono się do niedociągnięć stwierdzonych w ocenie kodeksu przeprowadzonej przez Komisję w 2020 r. (*Assessment of the Code of Practice on Disinformation – Achievements and areas for further improvement*, 10.09.2020, Komisja Europejska, <https://digital-strategy.ec.europa.eu/en/library/assessment-code-practice-disinformation-achievements-and-areas-further-improvement> dostęp 10.10.2023) i wykorzystano wnioski wyciągnięte z programu monitorowania dezinformacji związanej z COVID-19.

⁸⁵ *Komisja przedstawia wytyczne dotyczące ulepszenia kodeksu postępowania w zakresie zwalczania dezinformacji*, 26.05.2021, https://ec.europa.eu/commission/presscorner/detail/pl/ip_21_2585 (dostęp: 10.09.2020).

cyfrowych został określony „współregulacyjny mechanizm ochronny bazujący na istniejących inicjatywach dobrowolnych”⁸⁶. Inicjatywami dobrowolnymi są, w ujęciu AUC, porozumienia samoregulacyjne wsparte porozumieniami współregulacyjnymi⁸⁷. Inicjatywom zmierzającym do ustanowienia dobrowolnych kodeksów i wspierania tych inicjatyw przez KE poświęcono w AUC przepisy zawarte w sekcji VI rozdziału IV⁸⁸.

Niezależnie od przewidzianych w AUC i ARC mechanizmów współregulacyjnych oraz udzielanego przez KE wsparcia dla tworzenia dobrowolnych kodeksów postępowania, w rozporządzeniach cyfrowych (AUC i ARC) stworzony został system upoważnień ustanowionych na rzecz Komisji Europejskiej, dzięki którym Komisja uzyskała legitymację do prowadzenia „dialogu regulacyjnego” z największymi podmiotami świadczącymi usługi pośrednictwa internetowego kwalifikowanymi jako „strażnicy dostępu”. W konsekwencji zarówno zakres wolności wypowiedzi, jak i zakres usług świadczonych przez strażników dostępu stały się wypadkową uzgodnień poczynionych w ramach „dialogu regulacyjnego”.

Poza sporem pozostaje, że przesłanką *sine qua non* otrzymywania i rozpowszechniania treści w internecie jest, co wynika z uwarunkowań technicznych

⁸⁶ Wniosek AUC, s. 3.

⁸⁷ W motywie 104 AUC wskazano, że należy zbadać środki zmniejszające ryzyko związane z określonymi rodzajami nielegalnych treści za pomocą porozumień samoregulacyjnych i współregulacyjnych.

⁸⁸ W Parlamencie Europejskim dominował pogląd, zgodnie z którym dobrowolne działania platform w tym zakresie były niewystarczające. Posłowie chcieli jasnych, ogólnounijnych zasad moderowania treści, poprzez stosowanie mechanizmu zgłaszania i usuwania nielegalnych treści. Przyjęte przepisy mają zapewniać, że mechanizm: 1) jest skuteczny – użytkownicy będą mieli możliwość łatwego powiadamiania pośredników internetowych o potencjalnie nielegalnych treściach online, aby mogły zostać szybko usunięte; 2) nie jest nadużywany – w przypadku, gdy treść zostanie oznaczona lub usunięta, poszkodowani użytkownicy zostaną powiadomieni i będą mieli możliwość odwołania się od decyzji do krajowego organu rozstrzygającego spory; 3) szanuje prawa i wolności użytkowników, takie jak wolność wypowiedzi i wolny dostęp do informacji, aby pośrednicy internetowi usuwali nielegalne treści w sposób rzetelny, proporcjonalny i niedyskryminujący oraz nie usuwali treści, które nie są nielegalne. Jeśli użytkownicy zakwestionują decyzję platformy w sprawie niezgodności z prawem treści przez nich wygenerowanej, będą mieli możliwość dochodzenia swoich praw na drodze sądowej; zob. *Zwalczanie szkodliwych lub nielegalnych treści w internecie*, 30.10.2020, Parlament Europejski, <https://www.europarl.europa.eu/news/pl/headlines/economy/20201022STO89919/zwalczanie-szkodliwych-lub-nielegalnych-tresci-w-internecie> (dostęp: 10.10.2023).

i technologicznych, nawiązanie przez użytkownika internetu stosunku umownego łączącego go z pośrednikiem internetowym. Przedmiotem umowy są warunki świadczenia usługi dostępu do internetu, a także usługi hostingu i transmisji danych. Użytkownik, zawierając umowę z pośrednikiem, uzyskuje status usługobiorcy, co w konsekwencji oznacza, że zakres, tryb, warunki i forma korzystania przez niego z prawa do otrzymywania, przechowywania, udostępniania i rozpowszechniania treści stają się wypadkową – z jednej strony – aktywności użytkownika oraz – z drugiej strony – jakości (rzetelności) świadczonych na jego rzecz usług pośrednictwa internetowego. Niesporne jest zarazem, że wszystkie wyżej wskazane czynności podejmowane przez użytkownika wchodzi w zakres swobody wypowiedzi i stanowią konkretyzację realizowania tej wolności.

W ujęciu teoretycznym uwarunkowania techniczne lub technologiczne powinny pozostawać bez wpływu na kształt standardu wolności wypowiedzi. Zapewnieniu niezmiennego w warunkach cyfrowych standardu służyć miały przede wszystkim zawarte w art. 12–15 dyrektywy 2000/31 o handlu elektronicznym⁸⁹ kontratypy, których zastosowanie było uzależnione od udowodnienia neutralnego i czysto technicznego (biernego, pasywnego)⁹⁰ działania podmiotu świadczącego usługi polegające na udzieleniu użytkownikom dostępu do internetu oraz przechowywaniu i transmitowaniu danych.

Na kształt standardu wolności wypowiedzi – jak się wydaje – nie powinna zatem rzutować okoliczność, że otrzymywanie i rozpowszechnianie treści w internecie zostało poprzedzone i jest warunkowane nawiązaniem stosunku

⁸⁹ Zgodnie z art. 89 AUC przepisy art. 12–15 dyrektywy 2000/31/WE zostały uchylone. W ich miejsce przyjęto, że odesłania do art. 12–15 dyrektywy 2000/31/WE odczytywać należy jako odesłania odpowiednio do art. 4, 5, 6 i 8 AUC.

⁹⁰ Zawarte w art. 12–15 dyrektywy 2000/31 kontratypy były – jak zauważono w doktrynie – kluczowe dla zabezpieczenia interesów pośredników internetowych. Przesłanką wyłączenia odpowiedzialności w odniesieniu do każdej z usług pośrednictwa internetowego, tj. usługi dostępowej, usługi hostingu oraz cachingu stanowiło wykazanie, że aktywność pośrednika internetowego świadczącego jedną z powyżej wskazanych usług miała czysto techniczny, bierny charakter, a pośrednik nie ingerował w treść przekazu. Zgodnie z motywem 43 dyrektywy 2000/31 usługodawca może korzystać z wyłączenia dla „zwykłego przekazu” oraz dla „cachingu”, jeżeli nie jest on związany z przekazywaną informacją; wymaga to m.in., aby nie modyfikował on informacji, które przekazuje; wymaganie to nie obejmuje czynności o charakterze technicznym, które mają miejsce podczas przekazu, jeśli nie wpływają one na integralność informacji zawartej w przekazie.

prawnego z przedsiębiorcą świadczącym usługi pośrednictwa⁹¹, tj. usługi dostępu do internetu, usługi hostingu oraz usługi transmisji danych (*mere conduit*). Jednakże, jak wynika z treści wniosków ustawodawczych, KE doszła do przekonania, że podmioty świadczące usługi pośrednictwa internetowego, w tym bardzo duże platformy internetowe, „są wykorzystywane w sposób, który ma istotny wpływ na bezpieczeństwo w internecie, kształtowanie opinii publicznej i dyskursu” (motyw 56 ARC). Odbywa się to np. poprzez algorytmiczne sugerowanie, plasowanie i szeregowanie informacji, wyróżnianie za pomocą tekstu lub innych przedstawień graficznych lub w inny sposób selekcjonowanie informacji przekazywanych przez użytkowników internetu (odbiorców usług). Stosowane przez pośredników systemy rekomendacji, jak wskazano w motywie w 62 ARC, mogą mieć znaczący wpływ na zdolność odbiorców do pozyskiwania informacji w internecie i interakcji z nimi. Odgrywają one również ważną rolę w akcentowaniu pewnych wiadomości, wirusowym rozpowszechnianiu informacji i stymulowaniu zachowań w internecie. Dostrzeżony przez Komisję Europejską potencjał wpływu, jakim dysponują pośrednicy internetowi i związana z nim skala zagrożenia⁹² przesądziły o podjęciu przez KE inicjatyw ustawodawczych skutkujących uchwaleniem rozporządzeń cyfrowych.

KE zauważyła, że „obywatele Unii i inne osoby są narażeni na coraz większe ryzyko i szkody w internecie – od rozpowszechniania nielegalnych treści i działań po ograniczenia w wyrażaniu opinii i inne szkody społeczne”⁹³. Zauważono, że sposób szeregowania i prezentowania informacji na ich

⁹¹ M. Piech wskazuje, że terminy „pośrednik internetowy” i „usługi pośrednictwa internetowego” nie zostały zdefiniowane, a ich doktrynalne definicje znacząco różnią się między sobą. Jak zauważa, „W Polskiej doktrynie na określenie pośredników internetowych używa się także pojęć „podmiotów pośredniczących w dostępie do treści rozpowszechnianych w sieci internet”, „dostawców usług sieciowych”, „dostawców sieci i usług internetowych”. Mają one na celu m.in. przeciwstawienie tych usługodawców innym podmiotom świadczącym usługi społeczeństwa informacyjnego, określanym jako dostawcy treści (ang. *content providers*). Zob. M. Piech, *Zagadnienia wprowadzające – definicje*, [w:] *Pośrednicy internetowi w prawie Unii Europejskiej. Rola i obowiązki wobec treści użytkowników*, Warszawa 2019, s. 33).

⁹² Omówienie spostrzeżeń KE nastąpiło w komunikacie: *Kształtowanie cyfrowej przyszłości Europy*, Komisja Europejska, pkt 44 i n., https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/shaping-europes-digital-future_pl (dostęp: 30.10.2023).

⁹³ Wniosek AUC.

interfejsach internetowych generuje powstanie ryzyka systemowego⁹⁴ zakłócającego korzystanie z bezpiecznego, przewidywalnego i godnego zaufania środowiska internetowego.

Jak wynika z motywów zawartych w AUC i ARC, jak również z treści innych dokumentów „prawa miękkiego” UE⁹⁵, w tym także wskazywanych w preambułach tych aktów, prawodawca europejski obrał za cel realizowany w AUC i ARC – po pierwsze – ustanowienie środków prawnych służących zwalczaniu dezinformacji i innych nielegalnych treści w internecie, przy czym przyjęto, że założony skutek jest możliwy do osiągnięcia tylko przy współpracy z dostawcami usług pośrednictwa internetowego oraz – po drugie – założono, że zarówno interesie gospodarczym i politycznym UE, jak i w interesie pośredników internetowych jest rozwijanie rynku wewnętrznego usług cyfrowych, co wymaga współpracy pomiędzy organami UE i pośrednikami internetowymi. Wskazano w szczególności, że „dostawcy podstawowych usług platformowych i usług pomocniczych, użytkownicy biznesowi i użytkownicy końcowi odniosą korzyść z wyraźnie zdefiniowanych i ograniczonych obowiązków określonych we wniosku”. Celem ARC

⁹⁴ W AUC zidentyfikowano trzy kategorie ryzyka systemowego. Pierwsza z nich dotyczy ryzyka związanego z niewłaściwym korzystaniem z usług poprzez rozpowszechnianie nielegalnych treści. Druga kategoria dotyczy faktycznego lub przewidywalnego wpływu usługi na wykonywanie chronionych Kartą praw podstawowych, w tym godności ludzkiej, wolności wypowiedzi i informacji, wolności i pluralizmu mediów, prawa do życia prywatnego, ochrony danych, prawa do niedyskryminacji, praw dziecka i ochrony konsumentów. Trzecia kategoria ryzyka dotyczy faktycznego lub przewidywalnego negatywnego wpływu na procesy demokratyczne, dyskurs obywatelski i procesy wyborcze, a także na bezpieczeństwo publiczne. Czwarta kategoria ryzyka wynika z podobnych obaw związanych z projektowaniem i funkcjonowaniem bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych lub korzystaniem z nich, w tym poprzez manipulację [...] (motywy 80–83 AUC).

⁹⁵ W szczególności chodzi o Rezolucję Parlamentu Europejskiego z dnia 20 października 2020 r. w sprawie aktu prawnego o usługach cyfrowych i związanych z nim kwestii z zakresu praw podstawowych (https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=OJ:JOC_2021_404_R_0004, dostęp: 10.06.2024), a także w dokumencie roboczym służb Komisji: Ocena Kodeksu postępowania w zakresie dezinformacji – osiągnięcia i obszary wymagające dalszej poprawy, (<https://digital-strategy.ec.europa.eu/en/library/assessment-code-practice-disinformation-achievements-and-areas-further-improvement>), a także: Wytoczne Komisji w sprawie ulepszenia kodeksu postępowania w zakresie zwalczania dezinformacji (<https://digital-strategy.ec.europa.eu/en/library/guidance-strengthening-code-practice-disinformation>, dostęp: 10.06.2024).

stało się także ułatwienie zrównoważonego wzrostu podstawowych usług platformowych i szeroko pojętej gospodarki platform⁹⁶.

AUC i ARC mają formę rozporządzeń uchwalonych przez Parlament Europejski i Radę na wniosek Komisji Europejskiej. Zgodnie z art. 288 TFUE rozporządzenia są aktami ustawodawczymi, które wiążą w całości i są bezpośrednio stosowane we wszystkich państwach członkowskich. W praktyce zawierają one normy o charakterze generalnym i abstrakcyjnym i mogą znaleźć zastosowanie w nieokreślonej liczbie przypadków⁹⁷. Zauważa się, że „Rozporządzenia UE stanowią przykład najgłębszej ingerencji prawodawcy unijnego w wewnętrzne porządki prawne, zmierzając do unifikacji prawa państw członkowskich. W konsekwencji państwa te nie mogą podejmować jakichkolwiek środków krajowych, które mogłyby zmienić stosowanie rozporządzenia, ani też przyjmować żadnych środków ustawodawczych, które byłyby sprzeczne z rozporządzeniem”⁹⁸. W odniesieniu do rozporządzeń PE i Rady istnieje domniemanie skutku bezpośredniego, co oznacza, że „z samej swej natury i funkcji w systemie źródeł prawa wspólnotowego, wywierają skutki natychmiastowe i jako takie rozporządzenie zdolne jest przyznać jednostkom prawa, które sądy krajowe mają obowiązek chronić”⁹⁹.

Specyfika AUC i ARC przyjmujących postać rozporządzeń PE i Rady¹⁰⁰ polega na tym, że zawierają one spłot postanowień normatywnych o niejednolitych zakresach i mocy obowiązywania i to zarówno w ujęciu podmiotowym,

⁹⁶ ARC, s. 13.

⁹⁷ K. Scheuring, *System źródeł prawa pochodnego UE oraz sposoby jego tworzenia po wejściu w życie Traktatu z Lizbony*, „Studia Lubuskie” 2015, nr 11, s. 79.

⁹⁸ Tamże, s. 80.

⁹⁹ Tamże, s. 80.

¹⁰⁰ W treści wniosku ustawodawczego w sprawie AUC Komisja wskazała, że podjęła decyzję o przedstawieniu wniosku dotyczącego rozporządzenia w celu zapewnienia spójnego poziomu ochrony w całej Unii i uniknięcia rozbieżności utrudniających swobodne świadczenie odnośnych usług na rynku wewnętrznym, a także w celu zagwarantowania jednakowej ochrony praw oraz jednakowych obowiązków przedsiębiorstw i konsumentów na całym rynku wewnętrznym. Jest to konieczne do zapewnienia pewności prawa i przejrzystości zarówno podmiotom gospodarczym, jak i konsumentom. Rozporządzenie, którego dotyczy niniejszy wniosek, zapewnia ponadto spójne monitorowanie praw i obowiązków oraz równoważne sankcje we wszystkich państwach członkowskich, a także skuteczną współpracę między organami nadzorczymi poszczególnych państw członkowskich i na szczeblu unijnym (Wniosek AUC, s. 8). Natomiast w sprawie przyjęcia ARC Komisja uznała, że zidentyfikowane problemy można rozwiązać wyłącznie za pomocą aktu ustawodawczego. Rozporządzenie jest ponadto niezbędne ze względu na

jak i przedmiotowym, a w konsekwencji nie określają one w sposób trwały praw i obowiązków wskazanych w tych aktach. AUC i ARC są zbudowane z regulacji upoważniająco-odsyłających (blankietowych), przy czym przepisy blankietowe odsyłają do regulacji hipotetycznych, prawdopodobnych, lecz na dzień wejścia w życie AUC¹⁰¹ i ARC¹⁰² nieistniejących. AUC i ARC wyposażają zatem zarówno Komisję Europejską, jak i podmioty prywatne (tzw. strażników dostępu) w upoważnienia do aktualizowania, tj. przekształcania i zmiany, łączących ich zobowiązań wzajemnych w ramach „dialogu regulacyjnego”.

Zaproponowane w rozporządzeniach cyfrowych rozwiązania, które – jak wskazano we wnioskach ustawodawczych – służą zapewnieniu nowoczesnych ram zarządzania skutecznie chroniących prawa i prawnie uzasadnione interesy wszystkich zaangażowanych stron, przede wszystkim obywateli Unii¹⁰³, Komisja Europejska zakwalifikowała jako „środki polityczne”¹⁰⁴. Środki polityczne – na gruncie AUC i ARC – należy rozumieć jako znajdujące podstawę w aktach ustawodawczych działania faktyczne podejmowane, w szczególności przez Komisję Europejską i inne organy lub podmioty, zmierzające do realizacji celów politycznych UE. Celem politycznym, w ujęciu ogólnym, jest – jak wynika *explicite* z art. 1 AUC – „zapewnienie bezpiecznego, przewidywalnego i budzącego zaufanie środowiska internetowego, które ułatwia innowacje, i w którym skutecznie chronione są prawa podstawowe zapisane

fakt, że ma ono zastosowanie bezpośrednio w państwach członkowskich, ustanawia ten sam poziom praw i obowiązków dla podmiotów prywatnych, a także umożliwia spójne i skuteczne stosowanie przepisów w transgranicznym z zasady pośrednictwie handlowym online, które generowane jest w gospodarce platform internetowych. Rozporządzenie jest najbardziej odpowiednim sposobem rozwiązania zidentyfikowanych problemów dotyczących uczciwości i kontestowalności oraz przeciwdziałania fragmentacji jednolitego rynku podstawowych usług platformowych świadczonych lub oferowanych przez strażników dostępu (Wniosek ARC, s. 8).

¹⁰¹ AUC stosuje się od dnia 17 lutego 2024 r. (art. 93 ust. 2 AUC), jednakże rozporządzenie do dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych wskazanych zgodnie z art. 33 ust. 4 ma zastosowanie po upływie czterech miesięcy od powiadomienia danego dostawcy, o którym mowa w art. 33 ust. 6, w przypadku gdy data ta jest wcześniejsza niż dzień 17 lutego 2024 r. (art. 92 AUC).

¹⁰² ARC stosuje się od dnia 2 maja 2023 r. Jednakże art. 3 ust. 6 i 7 oraz art. 40, 46, 47, 48, 49 i 50 stosuje się od dnia 1 listopada 2022 r., a art. 42 i 43 stosuje się od dnia 25 czerwca 2023 r. (art. 54 ARC).

¹⁰³ Tamże, s. 14.

¹⁰⁴ Tamże, s. 14.

w Karcie, w tym zasada ochrony konsumentów” (art. 1 ust. 1 AUC). W ujęciu szczegółowym cel ten miałby zostać zrealizowany m.in. poprzez – z jednej strony – wdrożenie takich instrumentów, które zagwarantują realizację wolności wypowiedzi – a z drugiej strony – pozwolą na zwalczanie nielegalnych treści.

Rozporządzenie AUC ma zatem, w zamyśle prawodawcy, „ograniczyć ryzyko błędnego lub nieuzasadnionego blokowania wypowiedzi, złagodzić efekt mrozący w odniesieniu do wypowiedzi oraz stymulować swobodę otrzymywania informacji i wyrażania opinii, a także zwiększyć możliwości dochodzenia roszczeń przez użytkowników”¹⁰⁵. Zgodnie z wnioskiem wymagane miałyby być „jedynie usuwanie nielegalnych treści”¹⁰⁶. Zarazem jednak, jak wskazano we wniosku ustawodawczym, „rozporządzenie nie zawiera definicji nielegalnego charakteru takich treści, produktów lub usług”¹⁰⁷. Wyjaśniono jednak, że używane na gruncie rozporządzeń cyfrowych pojęcie nielegalnych treści obejmuje treści, produkty lub usługi wskazane jako niedozwolone w przepisach sektorowych, a ponadto inne treści, które nie zostały nimi objęte. Przepisy sektorowe są ograniczone z dwóch względów. Po pierwsze, interwencje sektorowe dotyczą niewielkiego podzbioru kwestii (np. naruszeń prawa autorskiego, treści o charakterze terrorystycznym, materiałów przedstawiających niegodziwe traktowanie dzieci w celach seksualnych lub nielegalnego nawoływania do nienawiści, niektórych nielegalnych produktów). Po drugie, obejmują one wyłącznie rozpowszechnianie takich treści w ramach określonych rodzajów usług (np. podzbiór platform internetowych w zakresie naruszeń prawa autorskiego, wyłącznie platformy udostępniania plików wideo i wyłącznie w zakresie audiowizualnych treści o charakterze terrorystycznym lub nawoływania do nienawiści). Rozporządzenia cyfrowe uzupełniają zatem regulacje sektorowe¹⁰⁸.

Osiąganie celów politycznych UE znajduje oparcie w akcie ustawodawczym realizującym założoną przez prawodawcę politykę prawa¹⁰⁹. Środkiem

¹⁰⁵ Wniosek KE w sprawie AUC, s. 14.

¹⁰⁶ Tamże, s. 14.

¹⁰⁷ Tamże, s. 4.

¹⁰⁸ Tamże, s. 5.

¹⁰⁹ W literaturze wskazuje się, że termin „polityka prawa” może być rozumiany dwojako, tj. jako dyscyplina naukowa, a także jako faktyczna działalność polegająca na wykorzystaniu prawa jako środka do realizacji założonych celów. Polityka prawa jako działalność faktyczna obejmuje: 1) politykę tworzenia prawa; 2) politykę stosowania prawa

służącym osiągnięciu celów politycznych UE jest ustanowiony na gruncie ARC „dialog regulacyjny”.

Terminem „dialog regulacyjny” Komisja posłużyła się w treści wniosku ustawodawczego w sprawie aktu o rynkach cyfrowych, dokonując wyboru jednego z trzech analizowanych „wariantów strategicznych”¹¹⁰. Warianty te zawierały modele regulowania stosunków ze strażnikami dostępu, przy czym różniły się od siebie przede wszystkim stopniem stanowczości odnośnie do sposobu regulowania obowiązków strażników dostępu. Wariant pierwszy zakładał, że zarówno wykaz strażników dostępu, jak i zakres ich obowiązków zostaną wyznaczone wprost w akcie normatywnym bez możliwości negocjowania tego statusu przez strażników dostępu. W wariantcie drugim przewidziano częściowo elastyczne ramy wyznaczania dostawców podstawowych usług platformowych jako strażników dostępu i aktualizowania obowiązków, w tym dialog regulacyjny na potrzeby wdrożenia niektórych z nich. Wariant trzeci – elastyczny wariant opierał się wyłącznie na progach jakościowych służących ustalaniu zakresu¹¹¹.

Mechanizmy zawarte w AUC i ARC stanowią realizację koncepcji zawartej w wariantcie drugim, który obejmuje: a) zamknięty wykaz podstawowych usług platformowych; b) połączenie ilościowych i jakościowych kryteriów w celu wyznaczenia dostawców podstawowych usług platformowych jako strażników dostępu; c) mające bezpośrednie zastosowanie obowiązki, w tym niektóre obowiązki, w przypadku których dialog regulacyjny może ułatwić ich skuteczne wdrażanie; oraz d) możliwość aktualizowania przez Komisję instrumentu po przeprowadzeniu badania rynku, jeżeli chodzi o obowiązki strażników dostępu, za pośrednictwem aktów delegowanych w zakresie, w jakim zostaną zidentyfikowane nowe praktyki, które są równie nieuczciwe

oraz 3) politykę wykonywania decyzji stosowania prawa (zob. W. Lang, J. Wróblewski, S. Zawadzki, *Teoria państwa i prawa*, Warszawa 1979, s. 128; podobnie J. Niesiołowski, *Polityka prawa*, [w:] *Leksykon współczesnej teorii i filozofii prawa*, J. Zajadło (red.), Warszawa 2007, s. 234).

¹¹⁰ W treści wniosku wskazano, że rozważane warianty strategiczne miały „służyć osiągnięciu ogólnego celu polegającego na zapewnieniu prawidłowego funkcjonowania rynku wewnętrznego przez promowanie skutecznej konkurencji na rynkach cyfrowych oraz w szczególności kontestowalnego i uczciwego środowiska platform internetowych” (zob. Wniosek w sprawie ARC, s. 12).

¹¹¹ ARC, s. 11 (elementy fakultatywne).

i które mogą z dużym prawdopodobieństwem zakłócać kontestowalność, a także za pośrednictwem wniosków w sprawie zmiany przepisów w pozostałych przypadkach. Badania rynku mogą również wskazać na potrzebę zmiany wykazu podstawowych usług platformowych. Uznano, iż wariant ten będzie w stanie w najbardziej skuteczny sposób przyczynić się do osiągnięcia celów niniejszej inicjatywy. Zapewnia on szybką interwencję w odniesieniu do wszystkich zidentyfikowanych problematycznych praktyk, umożliwiając jednocześnie w przypadku niektórych z nich dialog regulacyjny.

Wybrany wariant zakłada „dialog regulacyjny”, który ma zapewnić efektywną realizację celów ARC. W treści wniosku w sprawie aktu o rynkach cyfrowych „przewidziano możliwość dostosowanego do potrzeb stosowania niektórych obowiązków w drodze dialogu między Komisją a zainteresowanymi strażnikami dostępu”¹¹². Taki mechanizm uznano za „zapewniający uniknięcie nadmiernej regulacji, a jednocześnie umożliwiający uniknięcie braku interwencji”¹¹³. Parlament Europejski poparł działania KE polegające na – jak to określono – „pogłębionym dialogu” z „zainteresowanymi podmiotami”¹¹⁴ mającym na celu rozwijanie, ocenę i udoskonalenie podejść opartych na prawie miękkim, takich jak unijny kodeks postępowania w zakresie zwalczania dezinformacji. PE wskazał, że oczekuje od Komisji wydania, w ramach szczegółowego instrumentu towarzyszącego ustawie o usługach cyfrowych, wytycznych obejmujących zasady zwiększonej przejrzystości w zakresie moderacji treści oraz reguł reklamy w celu zapewnienia, by usuwanie i blokowanie zgodnych z prawem treści na podstawie warunków było ograniczone do niezbędnego minimum. Parlament wezwał ponadto Komisję do ustanowienia ram, które będą zakazywać platformom sprawowania drugiej warstwy kontroli nad treściami udostępnianymi w ramach odpowiedzialności dostawcy usług medialnych i podlegającymi szczególnym standardom i nadzorowi.

¹¹² ARC, s. 7.

¹¹³ Tamże, s. 7.

¹¹⁴ Akt prawny o usługach cyfrowych i związane z nim kwestie z zakresu praw podstawowych, Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. w sprawie aktu prawnego o usługach cyfrowych i związanych z nim kwestii z zakresu praw podstawowych, pkt 34, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020IP0274#ntc8-C_2021404PL.01005301-E0008 (dostęp: 10.06.2024).

Dialog regulacyjny, o którym mowa w treści wniosku ustawodawczego, może być ujmowany jako środek politycznego oddziaływania na pośredników internetowych, ale może być także ujmowany jako instrument prawny. Komisja została bowiem na gruncie AUC i ARC wyposażona nie tylko w uprawnienia do uruchamiania mechanizmów współregulacji i zachęcania pośredników do przyjmowania dobrowolnych kodeksów postępowania (art. 45–47 AUC), ale także do wydawania wytycznych (art. 47 ARC, motyw 95 ARC¹¹⁵) oraz aktów wykonawczych¹¹⁶, tj. zarówno podejmowania środków (motyw 29, 99), jak i wydawania decyzji wykonawczych (art. 46 ARC, motyw 100 ARC) oraz wydawania aktów delegowanych (art. 12 w zw. z art. 49 ARC).

Ustawodawca europejski założył, że aby osiągnąć cele określone w ARC, należy przekazać Komisji uprawnienia do wydawania aktów zgodnie z art. 290 Traktatu w celu uzupełnienia rozporządzenia. J. Barcz zauważa, że „Pojęcie »uzupełnienie« użyte w art. 290 ust. 1 TFUE dotyczy zasadniczo sytuacji, gdy akt delegowany wprowadza nowe uregulowania (zasady) do aktu podstawowego, rozszerzające zakres jego stosowania, niemające jednak charakteru »istotnych elementów« aktu podstawowego; punktem wyjścia do przekazania uprawnień Komisji w tej dziedzinie jest zamierzony brak spójności w określeniu przez prawodawcę treści aktu podstawowego; prawodawca określa w nim zasadnicze zobowiązania (»istotne elementy«), pozostawiając KE w ramach uprawnień delegowanych możliwość ich uzupełnienia (znaczącą swobodę uznaniowości)»¹¹⁷. Pojęcie istotnego elementu Trybunał Sprawiedliwości odnosi do przepisów aktu ustawodawczego: „których przedmiotem

¹¹⁵ Uprawnienie Komisji dotyczące wydawania wytycznych dotyczących zasad planowania zostały potwierdzone także w art. 5 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1150 z dnia 20 czerwca 2019 r. w sprawie propagowania sprawiedliwości i przejrzystości dla użytkowników biznesowych korzystających z usług pośrednictwa internetowego (Dz.U. UE L Nr 186, s. 57).

¹¹⁶ Zakres wydawanych przez Komisję aktów wykonawczych został wskazany w art. 46 ARC. Na podstawie zawartego w tym przepisie upoważnienia KE wydała rozporządzenie wykonawcze Komisji (UE) 2023/814 z dnia 14 kwietnia 2023 r. w sprawie szczegółowych zasad dotyczących prowadzenia przez Komisję niektórych postępowań na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/1925 (Dz.U. UE L Nr 102, s. 6).

¹¹⁷ J. Barcz, *Akty delegowane i akty wykonawcze – pojęcie i kryteria rozróżnienia*, „Europejski Przegląd Sądowy” 2012, nr 3, s. 6–16, <https://sip.lex.pl/#/publication/151139724> (dostęp: 17.10.2023).

jest skonkretyzowanie podstawowych wytycznych polityki wspólnotowej”¹¹⁸. Zauważa się, że „granice uprawnień wykonawczych są określone przede wszystkim w odniesieniu do cech danej polityki i mniej lub bardziej szerokiej swobody działania przyznanej Komisji w wykonaniu tej polityki. Ponadto wspomniane granice określone są na podstawie brzmienia przepisu delegującego, treści i celów aktu podstawowego oraz jego całego systemu”¹¹⁹. Elementy, które uważa się za istotne, a zatem niepodlegające kształtowaniu za pomocą aktów delegowanych, to np. zmiana materialnego, geograficznego lub czasowego zakresu zastosowania aktu podstawowego, wyjątki mogą więc dotyczyć sytuacji, gdy uprawnienia przekazywane w tych dziedzinach Komisji zostaną poprzez prawodawcę na tyle ściśle ograniczone, że nie dysponuje ona żadnym marginesem uznaniowości¹²⁰. Z kolei „zmiana” aktu ustawodawczego przez akt delegowany może polegać na usunięciu, zastąpieniu lub dodaniu innego elementu niż „istotny”¹²¹.

Zgodnie z art. 12 ARC Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 49¹²² w celu uzupełnienia rozporządzenia w odniesieniu do obowiązków ustanowionych wobec strażników dostępu w art. 5 i 6 oraz art. 7 ARC. Akty delegowane stanowią grupę aktów o charakterze nieustawodawczym o zasięgu ogólnym, wydawanych przez Komisję, uzupełniających lub zmieniających inne niż istotne elementy w akcie ustawodawczym. „Zasięg ogólny” oznacza, że na mocy art. 290 TFUE, musi znajdować zastosowanie do obiektywnie określonych sytuacji i wywoływać skutki prawne wobec adresatów określonych w sposób

¹¹⁸ Wyrok TS z dnia 27 października 1992 r. w sprawie Niemcy przeciwko Komisja (tzw. mięso baranie), C-240/90, s. I-5383.

¹¹⁹ K. Scheuring, *System źródeł...*, s. 93.

¹²⁰ J. Barcz, *Akty delegowane...*, s. 10.

¹²¹ Tamże, s. 8.

¹²² W myśl zawartych w tym przepisie postanowień uprawnienia do przyjmowania aktów delegowanych, o których mowa w art. 3 ust. 6 i 7 i art. 12 ust. 1, 3 i 4, powierza się Komisji na pięć lat od dnia 1 listopada 2022 r. (art. 49 ust. 2). Przed przyjęciem aktu delegowanego Komisja konsultuje się z ekspertami wyznaczonymi przez każde państwo członkowskie zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa (art. 49 ust. 4). Akt delegowany przyjęty na podstawie art. 3 ust. 6 i 7 i art. 12 ust. 1, 3 i 4 wchodzi w życie tylko wówczas, gdy ani Parlament Europejski, ani Rada nie wyraziły sprzeciwu w terminie dwóch miesięcy od dnia przekazania tego aktu Parlamentowi Europejskiemu i Radzie (art. 49 ust. 6).

ogólny i abstrakcyjny, w konsekwencji nie można przekazać Komisji uprawnień do wydawania aktów indywidualnych (odnoszących się do pojedynczych państw lub jedynie grupy państw, albo też grupy podmiotów dających się zindywidualizować za pomocą indywidualnych cech bądź właściwości)¹²³.

W celu zapewnienia jednolitych warunków wykonywania rozporządzenia AUC, Parlament powierzył Komisji także uprawnienia wykonawcze. W motywie 99 ARC określono zakres tych uprawnień, wskazując, że Komisja ma uprawnienia wykonawcze do określania środków, które mają być wdrożone przez strażników dostępu w celu skutecznego wypełniania obowiązków wynikających z niniejszego rozporządzenia, tj. do zawieszenia w całości lub w części określonego obowiązku nałożonego na strażnika dostępu; do zwolnienia strażnika dostępu w całości lub w części z określonego obowiązku; do określania środków, które mają być wdrożone przez strażnika dostępu, w przypadku gdy obchodzi on obowiązki wynikające z niniejszego rozporządzenia; do zakończenia badania rynku służącego wskazaniu strażników dostępu; do nakładania środków zaradczych w przypadku systematycznego niewypełniania obowiązków; do zarządzenia środków tymczasowych wobec strażnika dostępu; do uczynienia zobowiązań podjętych przez strażnika dostępu wiążącymi; do przedstawienia ustaleń dotyczących niewypełniania obowiązków; do ustalenia ostatecznej wysokości okresowej kary pieniężnej; do określania formy, treści i innych szczegółów powiadomień, przekazywanych informacji, uzasadnionych wniosków i obowiązkowych sprawozdań, przedkładanych przez strażników dostępu; do ustanawiania ustaleń operacyjnych i technicznych służących wdrożeniu interoperacyjności oraz metodyki i procedury odnośnie do poddanego audytowi opisu technik wykorzystywanych do profilowania konsumentów; do określania praktycznych ustaleń w odniesieniu do postępowań, przedłużania terminów, wykonywania praw w toku postępowania, warunków ujawnienia, a także współpracy i koordynacji między Komisją a organami krajowymi¹²⁴.

¹²³ K. Scheuring, *System źródeł...*, s. 92.

¹²⁴ Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiającym przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję (Dz.U. UE L Nr 55, s. 13).

Komisja Europejska, która została wyposażona w upoważnienia do przyjmowania aktów delegowanych i wykonawczych oraz wydawania wytycznych, uzyskała legitymację do permanentnego „dialogowania” ze strażnikami dostępu w przedmiocie – po pierwsze – zakresu, trybu i okresu realizacji ciążyących na nich obowiązków, albowiem KE może je modelować w trybie aktów wykonawczych, a także – po drugie – ustalania statusu podmiotu jako strażnika dostępu oraz treści i charakteru ciążyących na nim obowiązków, co KE może ustalać, wydając akty delegowane¹²⁵ oraz – po trzecie – w przedmiocie sposobu interpretowania zarówno treści ARC, jak i przyjmowanych aktów delegowanych i wykonawczych. Komisja jest bowiem uprawniona, w świetle literalnego brzmienia art. 47 ARC, do wydawania wytycznych „dotyczących wszelkich aspektów niniejszego rozporządzenia w celu ułatwienia jego skutecznego wykonania i egzekwowania”. Wytyczne – jak wskazano w motywie 95 ARC – są udzielane „w celu zapewnienia dalszych wskazówek dotyczących różnych aspektów niniejszego rozporządzenia lub w celu udzielenia przedsiębiorstwom świadczącym podstawowe usługi platformowe pomocy w wypełnianiu obowiązków wynikających z niniejszego rozporządzenia”.

Rodzaj upoważnień udzielonych Komisji Europejskiej rzutuje na ocenę charakteru norm zawartych w ARC, a także zakresu ich obowiązywania. Jeśli przyjąć, że akt ustawodawczy – co do zasady – zawiera normy o charakterze abstrakcyjnym i generalnym, a nadto, że zawarte w akcie ustawodawczym

¹²⁵ W szczególności KE może wydawać akty delegowane, zmieniając lub uzupełniając obowiązki strażników dostępu wskazane w art. 5 i 6 ARC, a zatem np. dotyczące: przetwarzania danych osobowych, w tym ich łączenia, wykorzystania w celach reklamowych, a także logowania do produktów lub usług, nadto w odniesieniu do użytkowników biznesowych – przedstawiania ofert, korzystania z metod uwierzytelniania, rozwiązań dotyczących płatności, subskrybowania innych usług oferowanych przez pośrednika internetowego, a także obowiązków dotyczących rozliczalności przekazów reklamowych realizowanych przez pośredników (art. 5). W art. 6 ARC określono natomiast obowiązki dotyczące, w szczególności, wykorzystywania do celów konkurencyjnych z innymi przedsiębiorcami dostępnych pośrednikowi danych użytkowników; zasad instalowania i odinstalowywania aplikacji w systemie operacyjnym strażnika dostępu, udzielania dostępu do aplikacji tworzonych przez użytkowników; oferowania, w tym plasowania i indeksowania usług i produktów oferowanych przez samego strażnika dostępu; zapewnienie interoperacyjności jego produktów i usług; dostępu do wyników pomiarów reklamowych; dostępu do danych dotyczących plasowania, zapytań, kliknięć i wyświetleń związanych z nieodpłatnym i płatnym wyszukiwaniem, wygenerowanych przez użytkowników końcowych (art. 6 ARC). W art. 7 określone zostały natomiast obowiązki dotyczące interoperacyjności usług łączności interpersonalnej niewykorzystujących numerów.

normy mają charakter wiążący ich adresatów (*ius cogens*), to na gruncie ARC reguły te znajdują zastosowanie jedynie częściowo. Z uwagi na uprawnienie KE do przyjmowania aktów delegowanych i wykonawczych, normy zawarte w ARC, w szczególności nakładające na strażników dostępu obowiązki (art. 5–7 ARC), należy kwalifikować jako względnie wiążące (*ius dispositivum*). Ustawodawca europejski cedując na KE upoważnienia do wydawania aktów na gruncie art. 290 TFUE, udzielił *de facto* Komisji Europejskiej upoważnienia do prowadzenia „dialogu regulacyjnego”, którego rezultatem jest porozumienie się dialogujących stron odnośnie do zakresu wzajemnych obowiązków oraz zasad ich spełniania oraz oceny.

Komisja może bowiem podejmować z własnej inicjatywy czynności w zakresie ustalania lub zmiany zakresu adresowanych do strażników obowiązków oraz badać naruszenie tych obowiązków (motyw 138), a także – jak wynika z art. 36 ust. 6 – „z własnej inicjatywy lub na wniosek dostawcy – może nawiązać dialog z dostawcą, aby ustalić, czy w świetle szczególnych okoliczności, w jakich znajduje się dostawca, zamierzone lub wdrożone środki są skuteczne i proporcjonalne do osiągnięcia zamierzonych celów” oraz „może skorzystać z uprawnień w zakresie czynności sprawdzających nawet przed wszczęciem postępowania, wykonując te uprawnienia z własnej inicjatywy lub na wniosek strażnika dostępu, a także z własnej inicjatywy lub na wniosek może wznawiać postępowanie” (art. 71 ust. 2).

Szeroka interpretacja terminu „dialog regulacyjny” obejmuje wszelkie instrumenty prawnego i pozaprawnego oddziaływania, w jakie została wyposażona Komisja Europejska do konsultowania, negocjowania i dialogowania ze strażnikami dostępu.

Dialog regulacyjny jako instrument oddziaływania na treść praw i obowiązków strażników dostępu w efekcie wyposaża Komisję w upoważnienie do kształtowania zakresu wpływów pośredników internetowych. Rozmiar wpływu, jaki wywierają na opinię publiczną pośrednicy internetowi, został zauważony przez Parlament Europejski w Rezolucji z dnia 20 października 2020 r.¹²⁶, w której wezwano Komisję Europejską do wystąpienia z inicjatywą ustawodawczą

¹²⁶ Akt prawny o usługach cyfrowych i związane z nim kwestie z zakresu praw podstawowych, Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. w sprawie aktu prawnego o usługach cyfrowych i związanych z nim kwestii z zakresu praw podstawowych, lit. J.

i podkreślono, że „niewielka liczba w większości pozaeuropejskich dostawców usług posiada dużą władzę rynkową i wywiera wpływ na prawa i wolności jednostek, nasze społeczeństwa i demokracje, kontrolując sposób prezentacji informacji, usług i produktów, co ma ogromne skutki dla funkcjonowania państw członkowskich oraz ich obywateli”¹²⁷. Zauważono także, że „decyzje tych platform mogą mieć daleko idące konsekwencje dla korzystania z wolności wypowiedzi i informacji oraz dla wolności i pluralizmu mediów”¹²⁸.

Poczynione przez KE i inne organy UE spostrzeżenie odnoszące się do zagrożeń dla realizacji praw podstawowych, w tym wolności wypowiedzi, mających źródło w działalności pośredników internetowych, wskazuje *per se* na potrzebę zaktualizowanego podejścia do oceny standardu wolności wypowiedzi polegającego przede wszystkim na uwzględnieniu istniejącego i potencjalnego zakresu wpływu pośredników internetowych, spośród których 6 zostało zakwalifikowanych przez KE¹²⁹ jako tzw. strażnicy dostępu.

¹²⁷ Akt prawny o usługach cyfrowych i związane z nim kwestie z zakresu praw podstawowych, Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. w sprawie aktu prawnego o usługach cyfrowych i związanych z nim kwestii z zakresu praw podstawowych, lit. J.

¹²⁸ Akt prawny o usługach cyfrowych i związane z nim kwestie z zakresu praw podstawowych, Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. w sprawie aktu prawnego o usługach cyfrowych i związanych z nim kwestii z zakresu praw podstawowych, lit. J.

¹²⁹ 6 września 2023 r. Komisja Europejska wskazała po raz pierwszy sześciu strażników dostępu – firmy Alphabet, Amazon, Apple, ByteDance, Meta i Microsoft oraz oznaczyła 22 podstawowe usługi platformowe, tj.: 1) sieci społecznościowe: TikTok, Facebook, Instagram, LinkedIn; 2) NI-ICS (czyli usługi przesyłania wiadomości): WhatsApp, Messenger; 3) pośrednictwo: Mapy Google, Google Play; 4) zakupy: Google, Amazon Marketplace, Apple App Store, Meta Marketplace; 5) udostępnianie wideo: YouTube; 6) usługi reklamowe: Google, Amazon, Meta; 7) przeglądarki internetowe: Chrome, Safari; 8) wyszukiwanie: Wyszukiwarka Google; 9) systemy operacyjne: Android, iOS, Windows. Jednocześnie Komisja rozpoczęła cztery badania rynku w celu dogłębszej oceny stanowisk przedstawionych przez firmy Microsoft i Apple, które argumentują, że pomimo osiągnięcia progów niektóre z ich podstawowych usług platformowych nie powinny kwalifikować się jako punkty dostępu: Microsoft: Bing, Edge i Microsoft Advertising oraz Apple: iMessage. Ponadto Komisja stwierdziła, że chociaż Gmail, Outlook.com i Samsung Internet Browser (przeglądarka internetowa firmy Samsung) osiągnęły progi określone w akcie o rynkach cyfrowych, co pozwala zakwalifikować je jako strażników dostępu, firmy Alphabet, Microsoft i Samsung przedstawiły wystarczająco uzasadnione argumenty wskazujące, że usługi te nie kwalifikują się jako punkty dostępu w odniesieniu do odpowiednich podstawowych usług platformowych. W związku z tym Komisja postanowiła nie wskazywać Gmail, Outlook.com i Samsung Internet Browser jako

Niektóre doktryny polityczne i kierunki badawcze, jak zauważa P. Winczorek, wyraźnie rozróżniają dwie sytuacje, tj. sprawowania władztwa oraz wywierania wpływu. Jak zauważa P. Winczorek, „gdy sprawuje się władzę, można uzyskać takie zachowanie podmiotu podporządkowanego, jakich nie uzyskałoby się, gdyby nie oddziaływanie władcze [...] Wpływ może być oddziaływaniem skierowanym zarówno w stronę sprawujących władzę, jak i tych, którzy w stosunkach władczych zajmują pozycje podporządkowane”¹³⁰, przy czym „środki wpływu są zbliżone do tych, z których korzystają podmioty sprawujące władzę”¹³¹. Istnieją zwolennicy tezy, wedle której „nie ma w społeczeństwach współczesnych żadnych ośrodków władzy w znaczeniu podmiotowym ani żadnej władzy w znaczeniu relacjonalnym. Istnieją jedynie wpływy, większe lub mniejsze, trwa gra wpływów”¹³².

Wskazane przez P. Winczorka rozróżnienie pomiędzy „sprawowaniem władzy” polegającym w szczególności na zastosowaniu przymusu państwowego a „posiadaniem wpływów” ma istotne znaczenie w relacjach między prawodawcą europejskim a strażnikami dostępu. Zasadność zaproponowanego rozróżnienia znajduje potwierdzenie na gruncie AUC i ARC. Wydaje się, że dostrzeżenie przez prawodawcę istnienia ośrodka wpływu poza strukturami organów UE stanowiło przyczynę podjęcia inicjatyw ustawodawczych skutkujących przyjęciem przez Parlament Europejski rozporządzeń cyfrowych oraz wyboru wariantu strategicznego przewidującego „dialog regulacyjny”. Zaakceptowanie faktu przeniesienia ośrodka wpływu poza zinstytucjonalizowane struktury państwowe wymusiło bowiem na prawodawcy europejskim zaaprobowanie i wdrożenie nowych rozwiązań regulacyjnych zbliżonych do partnerstwa publiczno-prywatnego.

Relacje pomiędzy pośrednikami internetowymi a Komisją Europejską mają źródło w akcie ustawodawczym. Niemniej zawarty w nim katalog upoważnień dla Komisji, a także świadomość potencjału wpływu, jakim

podstawowych usług platformowych. Oznacza to, że firmy Samsung nie wskazano jako strażnika dostępu w odniesieniu do jakiegokolwiek podstawowej usługi platformowej (*Akt o rynkach cyfrowych: Komisja wskazała sześciu strażników dostępu* 6.09.2023, Komisja Europejska, https://ec.europa.eu/commission/presscorner/detail/pl/ip_23_4328 (dostęp: 30.10.2023)).

¹³⁰ P. Winczorek, *Nauka o państwie*, Warszawa 2011, s. 43.

¹³¹ Tamże, s. 43.

¹³² Tamże, s. 44 i 45.

dysponują strażnicą dostępu, stawia organy publiczne w sytuacji przymusowej, kiedy zastosowanie wyłącznie władczych instrumentów oddziaływania może okazać się mniej skuteczne niż relacja oparta na stosunkach partnerskich. W konsekwencji poszukiwano takich rozwiązań prawnych, które przynależność do sfery imperium wiązać będą nie tyle z podejmowaniem jednostronnie wiążących decyzji, lecz ze skutkiem, jaki powstaje w sferze stosunków społecznych (w sferze publicznej), polegającym na realizacji celu publicznego z udziałem podmiotów prywatnych. O ile zatem do wyłącznej kompetencji podmiotu publicznego należeć będzie określenie celu i treści stosunku prawnego, to pożądany skutek stanie się możliwy do osiągnięcia dopiero przy współdziałaniu z podmiotem prywatnym. Uwarunkowania te powodują, że charakter relacji pomiędzy KE a strażnikami dostępu ma cechy partnerstwa publiczno-prywatnego.

Istotę PPP stanowi współpraca (współdziałanie) sektora publicznego z partnerem prywatnym w celu realizacji zadania tradycyjnie przypisanego sektorowi publicznemu¹³³. Słowo „współpraca” oznacza wykonywaną wspólnie bądź w porozumieniu z kimś pracę, a także pomoc lub udział we wspólnej pracy¹³⁴. W literaturze zauważa się, że współpraca w ramach partnerstwa publiczno-prywatnego oparta jest na umowie i powinna cechować się względną równorzędnością stron, w ramach której podmiot publiczny będzie dysponował szczególnymi uprawnieniami jedynie w takim zakresie, w jakim wynika to wprost z przepisów ustawy o partnerstwie publiczno-prywatnym. Umowa o partnerstwie publiczno-prywatnym podlegać będzie zasadzie swobody umów (art. 353¹ k.c.) w zakresie ograniczonym przepisami ustawy o partnerstwie publiczno-prywatnym. Regulacje zawarte w ustawie o partnerstwie publiczno-prywatnym nie tylko zatem ograniczają zakres

¹³³ D. Hajdys, *Formalnoprawne możliwości współpracy sektora publicznego i prywatnego w ramach modelu partnerstwa publiczno-prywatnego*, „Finanse Komunalne” 2009, nr 9, s. 22.

¹³⁴ D. Hajdys zauważa, że instytucji PPP nie da się sprecyzować jedną definicją. Nie da się też ustalić konkretnego schematu postępowania w ramach tej formuły. Zawierane umowy muszą zawsze odnosić się do specyficznych cech konkretnego przedsięwzięcia i wynikać z warunków, w jakich będą realizowane. Cel podjęcia współpracy ma dwojaki charakter. Z jednej strony chodzi o pozyskanie środków finansowych na konkretny projekt inwestycyjny, z drugiej – o jak najlepszy poziom zaspokojenia potrzeb społecznych, który dokonuje się poprzez wzrost inwestycji w sferze użyteczności publicznej (tamże, s. 23).

swobody stron w zakresie kształtowania wzajemnych świadczeń, ale zastępują te postanowienia umowne, które nie mogą być przez strony samodzielnie kształtowane¹³⁵. W rozumieniu krajowych przepisów „przez umowę o partnerstwie publiczno-prywatnym¹³⁶ partner prywatny zobowiązuje się do realizacji przedsięwzięcia za wynagrodzeniem oraz poniesienia w całości albo w części wydatków na jego realizację lub poniesienia ich przez osobę trzecią, a podmiot publiczny zobowiązuje się do współdziałania w osiągnięciu celu przedsięwzięcia, w szczególności poprzez wniesienie wkładu własnego” (art. 7 ust. 1 ustawy o PPP¹³⁷). Jednakże wynagrodzeniem partnera – jak zauważa się w orzecznictwie – może być nie tylko wartość wyrażona w pieniądzu, lecz także wynikające z umowy prawo do pobierania w przyszłości wynagrodzenia np. z tytułu wybudowanego ze środków własnych podmiotu prywatnego budynku, przeznaczonego do realizacji celów publicznych. Wojewódzki Sąd Administracyjny w Krakowie stwierdził, że w przypadku budowy parkingów wynagrodzeniem dla partnera prywatnego jest wyłączne prawo do eksploatacji parkingów¹³⁸. Umowa o PPP ma charakter dwustronnie zobowiązujący

¹³⁵ W literaturze wyróżniono trzy modele partnerstwa publiczno-prywatnego: model niemiecki, model francuski i model brytyjski oraz tzw. model przemysłowy. Model niemiecki charakteryzuje się wysokim stopniem uzależnienia partnera prywatnego od podejmowanych w trakcie realizacji kontraktu aktów i czynności organu publicznego. D. Hajdys wskazuje, że w modelu tym zwraca się uwagę na duże uzależnienie podmiotu świadczącego usługi od polityki władz lokalnych, które w sposób bezpośredni mogą wpływać na zasady jego funkcjonowania. Model brytyjski polega na skupieniu w jednym ręku funkcji właściciela infrastruktury i jej operatora. Różnica w stosunku do modelu niemieckiego polega na tym, że właścicielem infrastruktury jest podmiot prywatny, który nie ma zapewnionej stałej kontroli nad daną usługą, chyba że zagwarantuje sobie to w umowie. Zaletą modelu brytyjskiego jest swoboda działania podmiotu dostarczającego usługi. Model francuski polega na oddzieleniu funkcji właściciela infrastruktury od jej operatora. Regułą jest dążenie, aby właścicielem był organ publiczny. Rola operatora skupiona jest na zarządzaniu majątkiem i dostarczaniu usług przez okres oznaczony w umowie (tamże, s. 57).

¹³⁶ Umowa o PPP jest także umową wzajemną, odpłatną. W zamian za realizację przedsięwzięcia partner prywatny ma prawo oczekiwać wynagrodzenia, które może przyjąć wymiar pieniężny lub niepieniężny.

¹³⁷ Ustawa z dnia 19 grudnia 2008 r. o partnerstwie publiczno-prywatnym (t.j. Dz.U. z 2023 r., poz. 1637).

¹³⁸ W ocenie Sądu wybudowanie parkingów – w ramach zawartej umowy PPP – nie stanowi czynności odrębnej od pozostałych czynności Partnera Prywatnego wynikających z ww. umowy, lecz jest to element czynności złożonej, kompleksowej odpowiadającej zakresowo pojęciu „przedsięwzięcia” definiowanego w art. 2 pkt 4 ustawy o partnerstwie publiczno-prywatnym. W konsekwencji podmiot prywatny jest uprawniony do wynagrodzenia

(realizacja przedsięwzięcia będzie możliwa wyłącznie w przypadku realizacji świadczeń zarówno przez partnera prywatnego, jak i przez podmiot publiczny) i konsensualny (do jej zawarcia dochodzi poprzez złożenie zgodnych oświadczeń woli przez obie strony umowy)¹³⁹.

W art. 7 ARC ustanawia się ramy możliwego dialogu między dostawcą podstawowych usług platformowych wyznaczonym jako strażnik dostępu a Komisją w odniesieniu do środków, które strażnik dostępu wdraża lub zamierza wdrożyć w celu spełnienia obowiązków określonych w art. 6¹⁴⁰. Komisja może – z własnej inicjatywy lub na wniosek dostawcy – nawiązać dialog z dostawcą (art. 36 ust. 6 AUC). AUC i ARC przyznają Komisji Europejskiej uprawnienia w zakresie precyzowania praw i obowiązków pośredników internetowych, w tym także weryfikowania statusu pośredników jako tzw. strażników dostępu (art. 3 ARC), co więcej Komisja została wyposażona w upoważnienie do modyfikowania kryteriów, jakie winny być stosowane przy dokonywaniu kwalifikowania podmiotu do grupy strażników dostępu. W motywie 22 ARC wskazano, że Komisja powinna być uprawniona do określania metodyki ustalania, czy osiągnięte zostały progi ilościowe, oraz – w razie potrzeby – w celu regularnego dostosowywania tej metodyki do zmian na rynku i rozwoju technologicznego. Komisja Europejska uzyskała kompetencje do wydawania aktów delegowanych i wykonawczych natomiast strażnicy dostępu uzyskali uprawnienia do zwracania się do Komisji o wszczęcie postępowań, których skutkiem może być zmiana zakresu, zasad lub trybu ciężających na nich z mocy rozporządzeń obowiązków. Ustawodawca dopuścił

z tytułu – zagwarantowanego w umowie – wyłącznego prawa do eksploatacji parkingu przez okres 28 lat, a zatem nie przysługuje mu wynagrodzenie za jego budowę (Wyrok WSA w Krakowie z dnia 24 listopada 2022 r., I SA/Kr 611/22, LEX nr 3445740).

¹³⁹ Przepisy ustawy o partnerstwie publiczno-prywatnym nie określają wprost formy prawnej zawarcia umowy o partnerstwie publiczno-prywatnym. M. Grabiec zwraca uwagę, że do zawarcia umowy o partnerstwie publiczno-prywatnym wystarczy wymiana dokumentów obejmujących treść oświadczeń woli, z których każdy jest podpisany przez jedną ze stron, lub dokumentów, z których każdy obejmuje treść oświadczenia woli jednej ze stron i jest przez nią podpisany (art. 78 § 1 zdanie drugie k.c.). Krąg podmiotowy umowy o partnerstwie publiczno-prywatnym ograniczony został do podmiotu publicznego i partnera prywatnego, co nie wyklucza wielości podmiotowej po każdej ze stron umowy (zob. T. Chentosz, M. Wawrzyniak, *Art. 7, [w:] Ustawa o partnerstwie publiczno-prywatnym. Komentarz*, M. Grabiec (red. nauk.), Warszawa 2019).

¹⁴⁰ ARC, pkt 5 (elementy fakultatywne).

zatem, by modyfikowanie treści stosunku prawnego łączącego strażników dostępu z KE następowało w ramach tzw. dialogu regulacyjnego.

Ustalenie standardu wolności wypowiedzi może następować na dwóch płaszczyznach, tj. na płaszczyźnie materialnoprawnej, kiedy zasadniczym celem badań jest oznaczenie granic wolności wypowiedzi i uchwycenie styku pomiędzy zakresami legalnych i nielegalnych treści oraz na płaszczyźnie prawa formalnego, kiedy przedmiotem badań staje się proces konstruowania standardu wolności wypowiedzi, w szczególności ustalenie typu organów oraz oznaczenie roli i zakresu upoważnień, jakie organy te uzyskały do dokonywania wiążącej oceny w zakresie dopuszczalności ingerowania w wolność wypowiedzi.

Na gruncie rozporządzeń cyfrowych organem wyposażonym w kompetencje zarówno do ustalania znaczenia terminu „nielegalne treści”, jak i do dokonywania oceny potrzeby ich zwalczania z wykorzystaniem odpowiednich środków (moderowanie treści, monitorowanie, depozycjonowanie, demonetyzacja, ograniczanie świadczenia usług i inne) jest Komisja Europejska. Komisja Europejska, realizując cele polityczne UE, jest zarazem zainteresowana osiąganiem skutku polegającego na usuwaniu lub blokowaniu nielegalnych treści. Skutek ten jest możliwy jednak do osiągnięcia jedynie przy współpracy ze strażnikami dostępu. W konsekwencji zasadne staje się porównanie stosunku prawnego powstałego pomiędzy Komisją a strażnikami dostępu do stosunku dwustronnie zobowiązującego przybierającego postać umowy (kontraktu). W efekcie w drodze realizacji istniejącego między tymi stronami porozumienia może zostać uzyskany nowy standard wolności wypowiedzi – standard kontraktowy. Realizuje on model oczekiwanego zachowania się przez strony stosunku zobowiązaniowego, prowadzący do zapewnienia ochrony jednych wypowiedzi (treści legalne) i usunięcia innych (treści nielegalne) w sposób odpowiadający prawu i wypracowanym w „dialogu regulacyjnym” (kontrakcie) postanowieniom.

B. Rola Komisji Europejskiej

W AUC wskazano, że rozporządzenie w pełni harmonizuje przepisy mające zastosowanie do usług pośrednich na rynku wewnętrznym w celu zapewnienia bezpiecznego, przewidywalnego i budzącego zaufanie środowiska

internetowego, przeciwdziałania rozpowszechnianiu nielegalnych treści w internecie oraz zagrożeniom społecznym, jakie może stwarzać rozpowszechnianie dezinformacji lub innych treści, w którym to środowisku prawa podstawowe zapisane w Karcie są skutecznie chronione, a innowacje są wspierane. W rezultacie – o ile nie jest to wyraźnie przewidziane w rozporządzeniu – państwa członkowskie nie powinny przyjmować lub utrzymywać w mocy dodatkowych wymogów krajowych w odniesieniu do spraw objętych zakresem rozporządzenia, ponieważ miałyby to wpływ na bezpośrednie i jednolite stosowanie w pełni zharmonizowanych przepisów mających zastosowanie do dostawców usług pośrednich zgodnie z celami rozporządzenia (motyw 9 AUC).

Szczególny status uzyskała w tym systemie Komisja Europejska, która pełni zarówno rolę regulatora, korzystając z szerokich uprawnień do wydawania aktów delegowanych, co miałyby stanowić reakcję na zmieniające się uwarunkowania funkcjonowania rynków cyfrowych i pojawiające się nowe zagrożenia, jak też korzysta z szerokich uprawnień kontrolnych, a także nadzorczych. W celu wykonywania tych uprawnień KE może, a niekiedy ma obowiązek, korzystać z wyników ustaleń dokonanych przez specjalnie do tego utworzony organ, tj. Radę ds. Usług Cyfrowych. Rada została określona w AUC jako „niezależna grupa doradcza na poziomie unijnym” (art. 61 ust. 1 AUC). Zadaniem Rady jest udzielanie wsparcia i pomocy Komisji. Rada Usług Cyfrowych powinna składać się z koordynatorów ds. usług cyfrowych, jeżeli zostali oni wyznaczeni, bez uszczerbku dla możliwości zapraszania przez koordynatorów ds. usług cyfrowych na jej posiedzenia lub wyznaczania przez nich delegatów ad hoc z innych właściwych organów (motyw 131 AUC). Organy te mają zatem pełnić funkcje pomocnicze wobec Komisji, przy czym krajowi koordynatorzy ds. usług cyfrowych wykonywać mają zarazem zadania punktów kontaktowych, a państwa członkowskie są zobowiązane do zapewnienia im swobody i autonomii działania. Rada ds. Usług Cyfrowych formalnie zachowuje autonomię, jednakże Komisja, poprzez funkcję przewodniczącego, bez prawa do głosowania, uczestniczy w jej pracach (motyw 134 AUC). Wyposażenie w wiedzę ekspercką powinno zapewniać Komisji i Radzie Obserwatorium Gospodarki Platform Internetowych utworzone na mocy decyzji Komisji z dnia 26 kwietnia 2018 r. (motyw 137). Komisji Europejskiej zostały powierzone zadania w zakresie wdrażania i zapewniania skuteczności i elastyczności rozwiązań przyjętych

w rozporządzeniach cyfrowych, w tym poprzez wydawanie aktów delegowanych (motyw 152 AUC), a także kontroli, nadzoru oraz egzekwowania i monitorowania wykonania przepisów na szczeblu UE. Komitet Regionów poparł wnioszek, by monitorowanie egzekwowania przepisów rozporządzeń cyfrowych (AUC i ARC) powierzyć KE¹⁴¹. Przykładem powierzenia KE poważnych instrumentów kontrolnych jest nadanie Komisji uprawnienia dostępu do baz danych i algorytmów dowolnego organu¹⁴² publicznego, podmiotu, agencji, osoby fizycznej lub osoby prawnej (art. 54 AUC i motyw 99).

Komisja jest zatem – na gruncie rozwiązań przyjętych w AUC i ARC – organem centralnym wyposażonym zarówno w funkcje normodawcze, kontrolne, jak i wykonawcze, a także egzekucyjne. Co prawda w art. 56 ust. 1 AUC postanowiono, że „Państwo członkowskie, w którym znajduje się główne miejsce prowadzenia działalności dostawcy usług pośrednich, ma wyłączne uprawnienia w zakresie nadzorowania i egzekwowania niniejszego rozporządzenia”, to jednak kompetencja ta została obwarowana zastrzeżeniami, co może powodować, że wykonywanie jej przez państwo członkowskie będzie nieefektywne. Przede wszystkim zastrzeżono, że wyłączne kompetencje w zakresie regulowania działalności bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych należą wyłącznie do Komisji Europejskiej (art. 56 ust. 1 w zw. z art. 33 i n. AUC). Co więcej, wskazano, że aby skutecznie wykonywać swoje zadania, Komisja powinna zachować pewien margines uznaniowości, jeżeli chodzi o decyzje o wszczęciu postępowania przeciwko dostawcom bardzo dużych platform internetowych lub bardzo dużych wyszukiwarek internetowych. Po wszczęciu przez Komisję postępowania należy pozbawić zainteresowanych koordynatorów ds. usług cyfrowych właściwych dla miejsca siedziby możliwości wykonywania ich uprawnień w zakresie czynności sprawdzających i uprawnień w zakresie egzekwowania w odniesieniu do danych praktyk dostawcy bardzo dużej platformy internetowej lub bardzo dużej wyszukiwarki internetowej (motyw 139 AUC). Zarazem w przypadku wykonywania przez państwo wobec dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych

¹⁴¹ Opinia Europejskiego Komitetu Regionów – Akt o usługach cyfrowych i akt o rynkach cyfrowych (Dz.U. UE C z 2021 r. Nr 440, s. 67), pkt 16.

¹⁴² G. Bar, R. Skibicki, *Wyzwania prawne związane z wykorzystaniem sztucznej inteligencji w usługach cyfrowych*, „Prawo Nowych Technologii” 2021, Nr 1, s. 40.

kompetencji niezastrzeżonych dla KE (kompetencje dzielone), „Komisja powinna oceniać, czy w danym przypadku uważa za stosowne wykonywanie tych kompetencji dzielonych, a po wszczęciu postępowania państwa członkowskie nie powinny mieć już takiej możliwości” (motyw 125 AUC).

Ograniczeniem dla wykonywania kompetencji przez państwo członkowskie jest także zasada *ne bis in idem*, której skuteczność została rozciągnięta na wszystkie państwa członkowskie UE, co oznacza, że dostawca usług może odpowiadać za naruszenie tylko raz, pomimo że do tego naruszenia doszło na terytorium wielu państw członkowskich. W motywie 123 AUC wskazano, że:

aby zapewnić przestrzeganie zasady *ne bis in idem*, a w szczególności uniknąć sytuacji, w której to samo naruszenie obowiązków ustanowionych w niniejszym rozporządzeniu jest karane więcej niż jeden raz, każde państwo członkowskie, które zamierza wykonywać swoje kompetencje w odniesieniu do takich dostawców, powinno bez zbędnej zwłoki poinformować o tym wszystkie inne organy, w tym Komisję, za pośrednictwem systemu wymiany informacji ustanowionego do celów niniejszego rozporządzenia.

Nadto w art. 56 ust. 5 zobowiązano państwa członkowskie do „ściślej współpracy” z Komisją Europejską w zakresie wykonywania kompetencji dotyczących nadzoru i egzekwowania przepisów rozporządzenia. Wobec organów wymiaru sprawiedliwości państw członkowskich zawarto zalecenie, by wydając rozstrzygnięcia, uwzględniały stanowisko KE. W celu zagwarantowania zharmonizowanego stosowania i egzekwowania rozporządzenia ważne jest – jak wskazano w motywie 147 AUC – zapewnienie, aby organy krajowe, w tym sądy krajowe, miały wszystkie informacje niezbędne do zapewnienia, by ich decyzje nie były sprzeczne z decyzją przyjętą przez Komisję na podstawie AUC. Podkreślono, że „Trybunał Sprawiedliwości Unii Europejskiej powinien mieć nieograniczone prawo orzekania w odniesieniu do grzywien i kar pieniężnych zgodnie z art. 261 TFUE” (motyw 144 AUC).

Jakkolwiek zatem, w art. 56 AUC zawarowano istnienie kompetencji państw członkowskich, to jednak ich wykonywanie także zostało poddane kontroli organów europejskich, w tym Komisji Europejskiej. Nie jest bez znaczenia, że ograniczenia te wynikać mogą także z zastosowanej przez KE i PE

metody regulacyjnej, tj. harmonizacji pełnej. Zatem nawet jeśli państwa będą podejmowały samodzielnie wobec pośredników czynności nadzorcze lub kontrolne, to ich zakres, cel i metody, a także rezultat wymagają dostosowania do wspólnego, unijnego wzorca. Rola państwa członkowskiego przypomina zatem rolę egzekutora i poborcy, nie zaś suwerena, który samodzielnie określa cele i metody działania.

Na etapie ustawodawczym Komisja, wnioskując do Parlamentu Europejskiego, opowiedziała się, za przyjęciem scentralizowanych rozwiązań¹⁴³ zapewniających Komisji skupienie wszystkich uprawnień zarówno kontrolnych, koordynacyjnych, nadzorczych, jak i wykonawczych. Centralizacja kompetencji w odniesieniu do środowiska internetowego oznacza nie tylko skupienie w jednym organie kompetencji danego rodzaju, np. nadzorczych, ale też powierzenie jednemu organowi upoważnień do podejmowania wielopłaszczyznowych działań, a zatem także w zakresie wykonywania kontroli, wydawania aktów normotwórczych, monitorowania wykonywania obowiązków przez dostawców usług oraz przez państwa członkowskie, a także kompetencje władcze do wydawania rozstrzygnięć (decyzji) kształtujących prawa i obowiązki podmiotów rynku cyfrowego. W treści wniosku do PE o przyjęcie rozporządzenia o rynkach cyfrowych (ARC) odrzucono zdecentralizowany model regulowania środowiska internetowego, wskazując, że stoi temu na przeszkodzie ani zasada proporcjonalności, ani pomocniczości. Komisja wskazała, że „zdecentralizowany model egzekwowania nie wydaje się możliwym alternatywnym rozwiązaniem, w tym w kontekście ryzyka fragmentacji regulacyjnej, której ma zaradzić niniejsza inicjatywa; model ten nie wydaje się także proporcjonalny, biorąc pod uwagę ograniczoną liczbę strażników dostępu, których obejmowałby zakres proponowanych ram”¹⁴⁴. Centralizacji funkcji kontrolnych, zarządczych i nadzorczych podporządkowany został także instrument, jakim KE i Parlament posłużyły się do regulacji. Komisja podjęła decyzję o zastosowaniu rozporządzenia jako właściwego instrumentu, uzasadniając tę decyzję potrzebą zapewnienia spójnego poziomu ochrony w całej Unii i uniknięcia rozbieżności utrudniających swobodne świadczenie odnośnych usług na rynku wewnętrznym, a także

¹⁴³ Wniosek ARC, s. 11.

¹⁴⁴ Tamże, s. 11.

w celu zagwarantowania jednakowej ochrony praw oraz jednakowych obowiązków przedsiębiorstw i konsumentów na całym rynku wewnętrznym. Jest to konieczne do zapewnienia pewności prawa i przejrzystości tak podmiotom gospodarczym, jak i konsumentom¹⁴⁵.

Zarówno zatem w ujęciu materialnoprawnym (zakres przedmiotowy i podmiotowy AUC i ARC), jak i formalnym, tj. ze względu na zastosowany instrument (rozporządzenie) i metodę (harmonizacja pełna), jaką się posłużono, należy stwierdzić, że Komisja Europejska uzyskała kompetencje do tworzenia architektury internetu i budowania struktury organów europejskiego państwa cyfrowego¹⁴⁶.

Konieczne wydaje się zwrócenie uwagi na niektóre kompetencje KE (kompetencje wyłączne) potwierdzone w rozporządzeniach cyfrowych, a także rezultat, jaki powstaje w wyniku ich wykonywania, tj. powstanie hierarchicznej struktury organów i podmiotów realizujących wspólny cel określony jako

¹⁴⁵ Wniosek AUC, s. 8.

¹⁴⁶ Propozycja KE dotycząca rozwiązań zawartych w rozporządzeniach cyfrowych stanowi realizację wcześniejszych zobowiązań KE. W komunikacie *Kształtowanie cyfrowej przyszłości...* Komisja zobowiązała się do aktualizacji przepisów horyzontalnych, w których określono zadania i obowiązki dostawców usług cyfrowych, w szczególności platform internetowych. W ten sposób Komisja uwzględniła kwestie zidentyfikowane w sprawozdaniach z własnej inicjatywy Parlamentu Europejskiego i przeanalizowała zawarte w nich wnioski. Parlament Europejski przyjął dwie rezolucje na podstawie art. 225 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE): pt. *Akt prawny o usługach cyfrowych: poprawa funkcjonowania jednolitego rynku i Akt prawny o usługach cyfrowych: dostosowanie przepisów prawa handlowego i cywilnego do podmiotów gospodarczych prowadzących działalność internetową*. Parlament Europejski przyjął również rezolucję w ramach procedury nieustawodawczej pt. *Akt prawny o usługach cyfrowych i związane z nim kwestie z zakresu praw podstawowych* (Parlament Europejski, Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. w sprawie aktu prawnego o usługach cyfrowych i związanych z nim kwestii z zakresu praw podstawowych, <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020IP0274>, dostęp: 10.06.2024). Zasadniczo rezolucje te pod wieloma względami wzajemnie się uzupełniają. Zdecydowanie wzywa się w nich do zachowania podstawowych zasad określonych w dyrektywie o handlu elektronicznym oraz do ochrony praw podstawowych w środowisku internetowym, a także ochrony anonimowości w internecie w każdym przypadku, gdy jest to technicznie możliwe.

W rezolucjach tych Parlament wzywa do zapewnienia przejrzystości, obowiązków informacyjnych i rozliczalności w odniesieniu do dostawców usług cyfrowych oraz opowiada się za skutecznymi zobowiązaniami do zwalczania nielegalnych treści w internecie. Opowiedziano się w nich również za nadzorem publicznym na szczeblach unijnym i krajowym oraz współpracą między właściwymi organami różnych jurysdykcji w zakresie egzekwowania prawa, szczególnie w sprawach transgranicznych (Wniosek AUC).

budowanie „bezpiecznego, przewidywalnego i budzącego zaufanie środowiska internetowego” (art. 1 ust. 1 AUC). Zważywszy zarazem na kompetencje KE, zasadne jest usystematyzowanie struktury organów i podmiotów, których wzajemne powiązania przesądzą o powstaniu bezpośredniego skutku wertykalnego albo horyzontalnego, jaki wywołuje stosowanie postanowień AUC i ARC. Zagadnienie to dotyczy w szczególności ustalenia, kiedy i wobec jakich podmiotów (organów) jednostka może skutecznie żądać zapewnienia realizacji jej praw, w tym wolności wypowiedzi. Istotne jest ustalenie, czy rozporządzenia cyfrowe (AUC i ARC) wywołują pełny bezpośredni skutek wertykalny lub horyzontalny, czy też częściowy bezpośredni skutek (tj. wyłącznie wertykalny)¹⁴⁷. Zgodnie z orzecznictwem TSUE w odniesieniu do rozporządzeń dopuszczalny jest zarówno wertykalny, jak i horyzontalny skutek bezpośredni¹⁴⁸.

Zasada skutku bezpośredniego oznacza możliwość powoływania się przez jednostki na przepisy prawa wspólnotowego bezpośrednio przed organami krajowymi (przede wszystkim sądami), natomiast organy te mają obowiązek

¹⁴⁷ Wykształcenie zasady skutku bezpośredniego miało fundamentalne znaczenie dla funkcjonowania i efektywności prawa UE (zob. M. Koenig-Witkowska, A. Łazowski, R. Ostrihansky, *Prawo instytucjonalne Unii Europejskiej*, Warszawa 2007, s. 278). Jego istotą miała być ochrona praw jednostek jako sposób na zapewnienie efektywności prawa europejskiego (zob. C. Mik, *Europejskie prawo...*, s. 559). Bezpośredni skutek wertykalny ma znaczenie dla stosunków między jednostkami a państwem. Oznacza to, że jednostki mogą powoływać się na zapisy prawa UE w stosunku do państwa. Bezpośredni skutek horyzontalny ma znaczenie dla stosunków między jednostkami. Oznacza to, że jednostka może przywołać zapisy prawa UE w sporze z inną jednostką. W zależności od rodzaju aktu Trybunał przyjął bądź pełny bezpośredni skutek (tzn. bezpośredni skutek horyzontalny i wertykalny), bądź częściowy bezpośredni skutek (tylko skutek wertykalny); zob. *Zasada bezpośredniego skutku prawa Unii Europejskiej*, <https://eur-lex.europa.eu/PL/legal-content/summary/the-direct-effect-of-european-union-law.html> (dostęp: 10.06.2024). Zasadę skutku bezpośredniego należy odróżnić od zasady bezpośredniej stosowalności prawa europejskiego. Dotyczą one dwóch różnych kwestii stosowania prawa w państwach członkowskich UE. Prawo bezpośredniego skutku pozwala na powołanie się przed krajowymi organami na konkretny przepis prawa europejskiego. Zasada bezpośredniości stosowania odnosi się do „formalnego aspektu włączenia przepisów prawa wspólnotowego do prawa wewnętrznego i w prawie wspólnotowym ma szczególne zastosowanie w odniesieniu do rozporządzeń (zob. M. Koenig-Witkowska, A. Łazowski, R. Ostrihansky, *Prawo instytucjonalne...*, s. 279).

¹⁴⁸ Wyrok Trybunału z dnia 5 lutego 1963 r. w sprawie NV Algemene Transport-en Expeditie Onderneming van Gend & Loos przeciwko niderlandzkiej administracji celnej, nr 26-62, <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:61962CJ0026> (dostęp: 10.06.2024).

udzielić ochrony uprawnieniom, jakie jednostki wywodzą bezpośrednio z prawa wspólnotowego¹⁴⁹. TSUE wskazał jednocześnie, że aby przepis mógł być uznany za bezpośrednio skuteczny, musi być jasny i precyzyjny, bezwarunkowy – „nie jest obwarowany żadnym zastrzeżeniem ze strony państw członkowskich” i kompletny – „nie wymaga podjęcia przez państwa członkowskie żadnej interwencji ustawodawczej”¹⁵⁰. „Wertykalny bezpośredni skutek” oznacza sytuację, kiedy na przepis prawa jednostka może się powołać przeciwko organom państwa. „Horyzontalny bezpośredniego skutku” oznacza sytuację, kiedy na przepis prawa wspólnotowego jednostka może się powołać w sporze z innymi jednostkami¹⁵¹.

Nie podejmując szczegółowej analizy treści AUC i ARC pod kątem charakteru skutków, jakie wywołują zawarowane w nich konkretne postanowienia, wskazać należy, że przedmiotem ich regulacji jest ułożenie stosunków pomiędzy pośrednikami internetowymi, odbiorcami usług i państwami członkowskimi, przy czym legitymację do działania w imieniu państw członkowskich i ich obywateli wobec bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych otrzymała Komisja Europejska. Sposób ukształtowania relacji między tymi podmiotami przybiera postać złożonych, niekiedy trójstronnych, wzajemnych zobowiązań, w których państwa członkowskie i Komisja występują, co do osiągnięcia właściwego celu, w charakterze gwaranta lub poręczyciela wyposażonego w instrumenty władcze, które mogą znaleźć zastosowanie wobec pośredników internetowych na wypadek niewykonania przez nich obowiązków wskazanych w rozporządzeniach. Państwa członkowskie gwarantują zatem przestrzeganie postanowień zawartych w rozporządzeniu – akt o usługach cyfrowych, których adresatami są, w myśl art. 56 AUC, dostawcy usług pośrednich posiadający w tych państwach główne miejsce prowadzenia działalności. Komisja Europejska wykonuje

¹⁴⁹ M. Szwarc-Kuczer, *Bezpośrednia skuteczność przepisów prawa wspólnotowego – wprowadzenie i wyrok ETS z 5.02.1963 r. w sprawie 26/62 NV Algemene Transport – en Expeditie Onderneming van Gend an Loos przeciwko holenderskiej administracji celnej*, „Europejski Przegląd Sądowy” 2006, nr 12, s. 60.

¹⁵⁰ Wyrok Trybunału z dnia 5 lutego 1963 r. NV Algemene Transport- en Expeditie Onderneming van Gend & Loos przeciwko niderlandzkiej administracji celnej, nr 26-62, <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:61962CJ0026> (dostęp: 10.06.2024).

¹⁵¹ Tamże, s. 60.

obowiązki gwaranta wobec bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych (art. 56 ust. 1 w zw. z art. 33 i n. AUC, a także art. 3 i n. ARC).

Rola państw członkowskich w wykonywaniu nadzoru nad pośrednikami internetowymi sprowadzona została *de facto* do wyznaczenia organu, który będzie pełnił funkcję koordynatora ds. usług cyfrowych, który odpowiada za wszystkie kwestie związane z nadzorowaniem i egzekwowaniem rozporządzenia w danym państwie członkowskim (art. 56 ust. 1 AUC). W art. 56 ust. 1 akapit drugi potwierdzono upoważnienie dla państw członkowskich do „wprowadzenia mechanizmów współpracy i regularnej wymiany poglądów między koordynatorem ds. usług cyfrowych a innymi organami krajowymi”. Wyraźnie wskazano zarazem na obowiązki, jakie spoczywają na koordynatorze wobec Komisji Europejskiej oraz koordynatorów ustanowionych w innych państwach członkowskich. Państwa członkowskie zostały zobowiązane do zapewnienia koordynatorom warunków zachowania niezależności, bezstronności i autonomii działania. W art. 50 ust. 2 AUC wskazano, że „podczas wykonywania swoich zadań i uprawnień koordynatorzy ds. usług cyfrowych działają w sposób w pełni niezależny. Pozostają oni wolni od jakichkolwiek bezpośrednich i pośrednich wpływów zewnętrznych, nie zwracają się do żadnego innego organu publicznego ani podmiotu prywatnego o instrukcje, ani nie przyjmują takich instrukcji”.

Koordynatorzy uzyskali uprawnienia do podejmowania czynności sprawdzających (art. 51 ust. 1 AUC) w odniesieniu do praktyk dostawców usług pośrednich podlegających kompetencji ich państwa członkowskiego (udzielanie informacji, prowadzenie kontroli, żądanie złożenia wyjaśnień), a także w zakresie egzekwowania wykonywania zobowiązań, nakazywania zaprzestania naruszeń, podejmowania czynności niezbędnych do skutecznego zakończenia naruszeń oraz stosowania zwracania się do sądów o zastosowanie środków tymczasowych i nakładanie okresowych kar pieniężnych. Koordynator jest także uprawniony do wszczynania postępowań sądowych, przy czym udział w tym postępowaniu może zgłosić, poza dostawcą usług, „jakakolwiek inna osoba trzecia wykazująca prawnie uzasadniony interes” (art. 51 ust. 3 lit. b akapit drugi).

Koordynatorzy krajowi współpracują ze sobą w szczególności w ramach Europejskiej Rady ds. usług cyfrowych, której *ex lege* stają się członkami. Rada

ma status organu opiniującego-doradczego, a jej głównym zadaniem jest przyczynienie się do spójnego stosowania niniejszego rozporządzenia i skutecznej współpracy koordynatorów, a także koordynowanie sporządzania wytycznych i prowadzenia analiz przez Komisję oraz wspieranie koordynatorów ds. usług cyfrowych i Komisji w nadzorowaniu bardzo dużych platform internetowych (art. 61 ust. 2 AUC).

Komisja Europejska pełni funkcję centralną ze względu zarówno na zakres uprawnień, jak i na hierarchiczne *de facto* zwierzchnictwo nad działalnością pozostałych podmiotów (organów). Aby zapewnić przestrzeganie zasady *ne bis in idem*, a w szczególności uniknąć sytuacji, w której to samo naruszenie obowiązków ustanowionych w niniejszym rozporządzeniu jest karane więcej niż jeden raz, każde państwo członkowskie, które zamierza wykonywać swoje kompetencje w odniesieniu do takich dostawców, powinno bez zbędnej zwłoki poinformować o tym wszystkie inne organy, w tym Komisję, za pośrednictwem systemu wymiany informacji ustanowionego do celów niniejszego rozporządzenia (motyw 123 AUC). Komisja powinna oceniać, czy w danym przypadku uważa za stosowne wykonywanie tych kompetencji dzielonych, a po wszczęciu postępowania państwa członkowskie nie powinny mieć już takiej możliwości (motyw 125). Komisja może zatem przejąć postępowanie prowadzone przez koordynatorów krajowych, przy czym uzasadnieniem wyłączenia koordynatorów krajowych będzie ryzyko naruszenia zasady *ne bis in idem*.

Nadto, w zakresie niezbędnym do prowadzenia postępowań, zagwarantowano Komisji uprawnienia porównywalne do tych, jakie posiadają państwa członkowskie. Komisja ma być zatem uprawniona do podejmowania działań koniecznych do monitorowania skutecznego wdrażania i wypełniania obowiązków ustanowionych w rozporządzeniu (motyw 143). Wobec powyższego zapewniono Komisji „dostęp do istotnych dokumentów, danych i informacji niezbędnych do podjęcia i prowadzenia czynności sprawdzających oraz monitorowania wypełniania odpowiednich obowiązków ustanowionych w rozporządzeniu, niezależnie od tego, w czym posiadaniu znajdują się przedmiotowe dokumenty, dane lub informacje, oraz niezależnie od tego, w jakiej są formie lub w jakim formacie, na jakim nośniku są przechowywane lub w jakim dokładnie miejscu. Komisja powinna mieć możliwość zażądania bezpośrednio – w drodze należycie uzasadnionego wniosku o udzielenie informacji – od odpowiedniego dostawcy bardzo dużej platformy internetowej

lub bardzo dużej wyszukiwarki internetowej, a także od wszelkich innych osób fizycznych lub prawnych działających w celach związanych z ich działalnością handlową, gospodarczą, rzemieślniczą lub zawodową, w których przypadku można zasadnie oczekiwać, że dysponują informacjami związanymi z podejrzeniem naruszenia lub naruszeniem, stosownie do przypadku, przekazania wszelkich istotnych dowodów, danych i informacji. Ponadto na potrzeby rozporządzenia Komisji udzielono upoważnienia do zwracania się o wszelkie istotne informacje do dowolnego organu publicznego, podmiotu lub agencji w państwie członkowskim. Komisja powinna mieć możliwość zażądania dostępu – w ramach wykonywania uprawnień w zakresie czynności sprawdzających, takich jak wnioski o udzielenie informacji lub odbieranie wyjaśnień – do dokumentów, danych, informacji, baz danych i algorytmów odpowiednich osób oraz wyjaśnień z nimi związanych, a także do odbierania – za ich zgodą – wyjaśnień od osób fizycznych lub prawnych, które mogą posiadać użytecznych informacji, oraz do rejestrowania ich oświadczeń za pomocą wszelkich środków technicznych. Komisja powinna być także uprawniona do przeprowadzania kontroli niezbędnych do egzekwowania odpowiednich przepisów niniejszego rozporządzenia. Celem tych uprawnień w zakresie czynności sprawdzających jest uzupełnienie możliwości zwrócenia się przez Komisję o wsparcie do koordynatorów ds. usług cyfrowych i organów innych państw członkowskich, np. poprzez przekazanie informacji lub wsparcie w wykonywaniu tych uprawnień (motyw 141 AUC).

C. Delegowanie uprawnień na podmioty prywatne – aspekt formalny

Komisja Europejska nie może wkraczać w dziedzinę prywatnej działalności jakiegokolwiek osoby, czy to fizycznej, czy prawnej, ingerencja taka musi mieć podstawę prawną i być uzasadniona względami określonymi w prawie¹⁵². Ten wymóg ochrony, uznany za zasadę ogólną prawa unijnego, jest

¹⁵² Wyroki TS: z dnia 24 listopada 2011 r. w sprawie Scarlet Extended SA przeciwko Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), C-70/10, poz. I-11959, pkt 67 (dalej: Wyrok TS w sprawie Scarlet Extended przeciwko SABAM); z dnia 5 października 2010 r. w sprawie J. McB. przeciwko L.E., C-400/10 PPU, s. I-8965, pkt 53; z dnia

korelatem zasad legalności i pewności prawa, które wynikają z idei państwa prawa. Trybunał wielokrotnie orzekał, że zasada pewności prawa wymaga, by uregulowania nakładające obciążenia na jednostki, wywierające dla nich negatywne skutki, a także nakładające środki ograniczające mające znaczący wpływ na prawa i wolności określonych osób, były na tyle jasne i precyzyjne, by zainteresowane osoby miały możliwość jednoznacznego poznania swoich praw i obowiązków i podjęcia w związku z tym odpowiednich działań.

Partnerem dla Komisji Europejskiej jako organu centralnego¹⁵³ w wykonywaniu, kontroli i egzekwowaniu zasad opisanych w rozporządzeniach regulujących świadczenie usług cyfrowych, stali się – ze względu na transgraniczność usług oraz ryzyko „fragmentacji regulacyjnej”¹⁵⁴ – pośrednicy internetowi, w tym bardzo duże platformy internetowe i bardzo duże wyszukiwarki internetowe (strażnicy dostępu)¹⁵⁵. Podmioty te zostały zobowiązane do współpracy z Komisją Europejską oraz wskazanymi w rozporządzeniach (AUC i ARC) organami poprzez wzięcie na siebie obowiązków pod rygorem nałożenia na te podmioty przez Komisję, w razie ich niewykonania albo wadliwego wykonania, kar finansowych.

Analiza zakresów i charakteru wskazanych w rozporządzeniach praw i obowiązków nałożonych na pośredników internetowych wskazuje, że bardzo duże platformy internetowe i bardzo duże wyszukiwarki (strażnicy dostępu),

22 grudnia 2010 r. w sprawie DEB Deutsche Energiehandels- und Beratungsgesellschaft mbH przeciwko Niemcom, pkt 35; z dnia 21 września 1989 r. w sprawie Hoechst AG przeciwko Komisji Wspólnot Europejskich, 46/87, poz. 2859 (dalej: Wyrok TS w sprawie Hoechst AG przeciwko Komisji Wspólnot Europejskich).

¹⁵³ Na odrzucenie „zdecentralizowanego modelu egzekwowania” jako niewystarczającego do realizacji zadań wskazanych w AUC Komisja wskazała w uzasadnieniu Wniosku ARC, s. 11.

¹⁵⁴ Wniosek ARC, s. 11.

¹⁵⁵ Zgodnie z art. 33 ust. 1 status strażników dostępu uzyskują dostawcy platform internetowych i wyszukiwarek internetowych, które mają średnią liczbę miesięcznie aktywnych odbiorców usługi w Unii wynoszącą co najmniej 45 mln, i które zostały wskazane jako bardzo duże platformy internetowe lub bardzo duże wyszukiwarki internetowe. Zgodnie z art. 24 ust. 2 AUC do dnia 17 lutego 2023 r., a następnie co najmniej raz na sześć miesięcy dostawcy, w odniesieniu do każdej platformy internetowej lub wyszukiwarki internetowej, publikują w publicznie dostępnej sekcji swojego interfejsu internetowego informacje na temat średniej liczby aktywnych miesięcznie odbiorców usługi w Unii, obliczonej jako średnia liczba w okresie poprzednich sześciu miesięcy oraz zgodnie z metodyką ustanowioną w aktach delegowanych, o których mowa w art. 33 ust. 2, jeżeli te akty delegowane zostały przyjęte.

wypełniając nałożone na nich obowiązki, realizują nie tylko cele UE, lecz także własne, przede wszystkim gospodarcze. W zamian za zobowiązanie się do realizacji zadań wskazanych w AUC i ARC pośrednicy uzyskali zapewnienie stosowania jednolitych zasad wobec wszystkich dostawców usług cyfrowych oraz potwierdzenie swobody prowadzenia działalności we wszystkich państwach członkowskich UE. Dostawcy bardzo dużych platform i wyszukiwarek internetowych zyskali ponadto pewność prawa gwarantowaną w szczególności w ten sposób, że państwa członkowskie są wobec pośredników reprezentowane przez KE¹⁵⁶. Zgodnie bowiem z art. 56 ust. 2 AUC KE ma wyłączne uprawnienia w zakresie egzekwowania i nadzorowania bardzo dużych platform i bardzo dużych wyszukiwarek.

Charakter stosunku prawnego, który powstał pomiędzy KE a strażnikami dostępu, uwzględnia potencjał gospodarczy, jakim dysponują dostawcy bardzo dużych platform i bardzo dużych wyszukiwarek internetowych. Wyznaczenie i nałożenie na pośredników obowiązków zostało poprzedzone konsultacjami i porozumieniami, które przybrały postać dobrowolnych kodeksów etyki postępowania. Mechanizm niewładczego regulowania obowiązków dostawców usług cyfrowych, przyjmujący formę współregulacji, został także – w dużym stopniu – zastosowany w AUC (art. 45–47 AUC). Jednostronne, władcze wyznaczenie takich obowiązków mogłoby bowiem okazać się nieefektywne ze względu na silną pozycję ekonomiczną tych strażników i skalę upowszechnienia świadczonych przez nich usług¹⁵⁷.

¹⁵⁶ *Europa na miarę ery cyfrowej: nowe przepisy dla platform internetowych*, Komisja Europejska, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment/europe-fit-digital-age-new-online-rules-platforms_pl (dostęp: 12.01.2024).

¹⁵⁷ KE i PE musiały np. uwzględnić, że Google w krajach Unii Europejskiej ma pozycję dominującą i kontroluje ponad 90% rynku wyszukiwarek; zob. M. Chrobot, *Google dogadało się z Unią. Konkurencja będzie miała fory w wyszukiwarce*, 15.04.2013, Komputer Świat, <https://www.komputerswiat.pl/aktualnosci/wydarzenia/google-dogadalo-sie-z-unia-konkurencja-będzie-miała-fory-w-wyszukiwarce/wbtfbsn> (dostęp: 12.01.2024). Koncern Google zagroził w 2021 r. np. wyłączeniem swojej wyszukiwarki w Australii, jeśli władze tego kraju nie zmienią projektu przepisów, które mają nakazać gigantom technologicznym płacić mediom za tworzone przez nie treści. Władze Australii zamierzały wprowadzić przepisy zmuszające Google, Facebooka i potencjalnie również inne wielkie koncerny do negocjacji z lokalnymi mediami opłat za udostępniane w internecie informacje. Według projektu, jeśli koncerny i wydawcy nie dojdą do porozumienia w sprawie wartości tych treści, wówczas wyceniac je będzie rządowy arbitraż;

Obowiązki ogólne nałożone na pośredników internetowych, tj. niezależnie od skali prowadzonej przez nich działalność, w tym liczby aktywnych odbiorców w rozumieniu art. 33 ust. 1 AUC, zostały wskazane w art. 9–32 AUC (nakaz podjęcia działań przeciwko nielegalnym treściom; nakazy udzielenia informacji; obowiązek utworzenia punktu kontaktowego dla KE, państw członkowskich i odbiorców usług; obowiązek wyznaczenia przedstawiciela prawnego, nakaz posiadania regulaminu korzystania z usług; wywiązywanie się z obowiązków sprawozdawczych wobec KE i państw członkowskich; zapewnienie stosowania mechanizmu „zgłaszania i działania”; obowiązek zgłaszania podejrzenia popełnienia przestępstwa; posiadanie wewnętrznego mechanizmu rozstrzygania skarg i przedsądowego rozstrzygania sporów; posiadanie mechanizmu współpracy z sygnalistami; stosowanie środków ochrony na zasadach wskazanych w AUC; posiadanie przejrzystego systemu rekomendacji, reklam i interfejsów; ochrona małoletnich; identyfikowanie przedsiębiorców; obowiązek informowania użytkowników o nielegalnym produkcie lub nielegalnej usłudze) oraz art. 44–48 (stosowanie znormalizowanych wzorców zgłaszania, zapewnianie stosowania innych środków technicznych; współpraca w zakresie dobrowolnie przyjmowanych kodeksów; przyjmowanie dobrowolnych protokołów kryzysowych).

Na strażników dostępu poza wskazanymi powyżej obowiązkami ogólnymi nałożono dodatkowe zadania określone w art. 24 ust. 2 i 3, a także art. 33–42 (obowiązek analizy i szacowania ryzyka systemowego; obowiązek zmniejszania ryzyka; stosowanie mechanizmu reagowania kryzysowego; przeprowadzanie okresowych audytów; posiadanie dodatkowych mechanizmów zapewniających przejrzystość systemu reklam i systemu rekomendacji; udzielanie koordynatorom ds. rynku usług cyfrowych dostępu do danych i informacji; ustanowienie komórki nadzoru przestrzegania AUC; uiszczenie rocznej opłaty nadzorczej na rzecz KE). Obowiązki strażników dostępu zostały wskazane ponadto w rozporządzeniu w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym (ARC), przy czym w art. 5–8 określono obowiązki negatywne adresowane do strażników dostępu, a w kolejnych

zob. *Google grozi Australii blokadą swojej wyszukiwarki. „Nie odpowiadamy na groźby”*, 22.01.2021, Forsal, <https://forsal.pl/biznes/media/artykuly/8074993,google-grozi-australii-blokada-swojej-wyszukiwarki.html> (dostęp: 12.01.2024).

postanowieniach rozporządzenia wskazano uprawnienia KE wobec strażników dostępu w zakresie kontroli i nadzoru prowadzonej przez nich działalności oraz zawarto przepisy normujące tryb i zakres postępowań prowadzonych przez KE oraz wysokość i przesłanki nakładania grzywien.

Rodzaj i zakres obowiązków nałożonych w rozporządzeniach cyfrowych na strażników dostępu jest rezultatem konsultacji i uzgodnień KE z pośrednikami internetowymi. Przyjęcie rozwiązań zawartych w rozporządzeniach zostało poprzedzone okresem wdrażania dobrowolnych zobowiązań, w szczególności w odniesieniu do obowiązku, który w rozporządzeniach ma kluczowe znaczenie, tj. wykrywania, usuwania i przeciwdziałania nielegalnym treściom. W dniu 31 maja 2016 r. przyjęty został Kodeks postępowania dotyczący nielegalnego nawoływania do nienawiści w Internecie (Kodeks). Kodeks powstał wskutek współpracy Komisji Europejskiej z pośrednikami internetowymi, nazywanymi w treści Kodeksu „przedsiębiorstwami z branży IT” (Facebook, Twitter, YouTube, Microsoft)¹⁵⁸. Komisja Europejska oraz cztery giganty informatyczne zobowiązały się stosować zapisy przyjętego Kodeksu postępowania w sprawie przeciwdziałania nielegalnej mowie nienawiści online¹⁵⁹. Z biegiem czasu wskazany Kodeks zobowiązały się stosować także inne firmy komputerowe takie jak Instagram, Snapchat, Dailymotion, Jeuxvideo.com, TikTok, LinkedIn, a wiosną 2022 r. do grupy tej przystąpiły także Rakuten Viber i Twitch¹⁶⁰.

Komisja Europejska, pomimo że jej udział w pracach nad przyjęciem Kodeksu został wyraźnie w nim odnotowany, nie występuje tam jako organ wyposażony w instrumenty władczego oddziaływania, ale – przeciwnie – organ, który wymaga wsparcia. Sygnatariusze Kodeksu wyraźnie zaznaczyli w treści dokumentu, że Komisja jest beneficjentem tego porozumienia, podkreślając, że „Przedsiębiorstwa z branży IT wspierają Komisję Europejską

¹⁵⁸ *Kodeks postępowania w zakresie zwalczania nielegalnego nawoływania do nienawiści w internecie*, Komisja Europejska, https://ec.europa.eu/newsroom/document.cfm?doc_id=42869 (dostęp: 12.01.2024).

¹⁵⁹ G. Tylec, *Ograniczenia mowy nienawiści w świetle regulacji prawnych obejmujących jednolity rynek usług cyfrowych*, [w:] *Kwalifikacja prawna...*, s. 45.

¹⁶⁰ *The EU Code of conduct on countering illegal hate speech online*, Komisja Europejska, https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en (dostęp: 12.01.2024).

i państwa członkowskie UE w ich działaniach, których celem jest sprostanie wyzwaniu, jakim jest dopilnowanie, by platformy internetowe nie ułatwiały rozpowszechniania nielegalnej mowy nienawiści na masową skalę¹⁶¹. Przedsiębiorstwa IT dokonując autodefiniowania swojej roli, statuują się na prowadzonych przez nich platformach jako „strażnicy” przestrzegania prawa europejskiego, w szczególności przestrzegania postanowień KE wynikających z Decyzji ramowej 2008/913/WSiSW z dnia 28 listopada 2008 r. w sprawie zwalczania pewnych form i przejawów rasizmu i ksenofobii¹⁶². W kodeksie wskazano, że: „By zapobiec rozprzestrzenianiu się nielegalnej mowy nienawiści, ogromne znaczenie ma dopilnowanie, by stosowne przepisy prawa krajowego transponujące decyzję 2008/913/WSiSW były w pełni egzekwowane przez państwa członkowskie w środowisku internetowym, jak również poza nim¹⁶³. Na gruncie Kodeksu, przedsiębiorstwa IT (obecnie: strażnicy dostępu) zobowiązały się do realizacji obowiązków, które następnie zostały wyartykułowane w rozporządzeniach cyfrowych.

Podobne inicjatywy Komisja Europejska podejmowała w zakresie zwalczania dezinformacji w internecie, w szczególności wydając Wytyczne dotyczące wzmocnienia kodeksu postępowania w zakresie zwalczania dezinformacji¹⁶⁴. Komisja zastrzega na swojej stronie internetowej, że Kodeksy postępowania, w szczególności Kodeks z 2022 r. jest wynikiem prac przeprowadzonych przez sygnatariuszy. Zapewnia, że to sygnatariusze decydują, jakie zobowiązania podejmą, a ich obowiązkiem jest zapewnienie skuteczności realizacji swoich zobowiązań. Kodeks nie został zatwierdzony przez Komisję, natomiast Komisja określiła swoje oczekiwania w wytycznych i uważa, że kodeks jako całość spełnia te oczekiwania¹⁶⁵. Sygnatariuszami są obecnie główne platformy internetowe działające w UE, a także m.in. duże stowarzyszenia branżowe reprezentujące europejski sektor reklamowy. Jak zapowiedziano

¹⁶¹ *Kodeks postępowania w zakresie zwalczania nielegalnego...*, s. 1.

¹⁶² Decyzja ramowa 2008/913/WSiSW z dnia 28 listopada 2008 r. w sprawie zwalczania pewnych form i przejawów rasizmu i ksenofobii.

¹⁶³ *Kodeks postępowania w zakresie zwalczania nielegalnego...*, s. 1.

¹⁶⁴ Wytyczne dotyczące wzmocnienia kodeksu postępowania w zakresie zwalczania dezinformacji, <https://digital-strategy.ec.europa.eu/pl/library/guidance-strengthening-code-practice-disinformation> (dostęp: 12.01.2024).

¹⁶⁵ *Kodeks postępowania w zakresie zwalczania dezinformacji z 2022 r.*, Komisja Europejska, <https://digital-strategy.ec.europa.eu/pl/policies/code-practice-disinformation> (dostęp: 10.10.2024).

w europejskim planie działania na rzecz demokracji (EDAP)¹⁶⁶, w wytycznych odniesiono się do niedociągnięć stwierdzonych w ocenie kodeksu przeprowadzonej przez Komisję w 2020 r. Najpoważniejszym zastrzeżeniem do wytycznych dotyczących wzmocnienia kodeksu postępowania w zakresie praktyk dezinformacji stanowiło to, że „zbytńio skupiają się one na treści i jej moderowaniu, a niewystarczająco – na podmiotach rozpowszechniających informacje. Treści nieustannie się zmieniają i wykorzystywane platformy się rozwijają, lecz główne podmioty i motywacje pozostają zasadniczo takie same. Podejście musi się raczej opierać na zapobieganiu, a nie na środkach zaradczych, a Komisja powinna dać pierwszeństwo raczej pracom nad przyczynami niż nad konsekwencjami”¹⁶⁷. W wytycznych z dnia 26 maja 2021 r. zwalczających niedociągnięcia postulowano w szczególności: wzmocnienie demontyzacji dezinformacji; zwiększenie zakresu weryfikacji faktów i zapewnienie naukowcom szerszego dostępu do danych; wzmocnienie monitorowania treści¹⁶⁸. Wzmocniony kodeks postępowania w zakresie dezinformacji¹⁶⁹ został podpisany i przedstawiony w dniu 16 czerwca 2022 r. przez 34 sygnatariuszy, którzy przystąpili do procesu przeglądu kodeksu z 2018 r.¹⁷⁰

Z pewną ostrożnością, niemniej – jak się wydaje – zasadnie stawiać można tezę o istnieniu porozumienia zawartego ponad głowami państw członkowskich pomiędzy KE a przedsiębiorstwami IT, w szczególności strażnikami dostępu. Porozumienie obejmuje wymianę polegającą na udzieleniu przez strażników dostępu wsparcia w realizacji celu politycznego przez KE w zamian za wsparcie udzielone przez KE w zakresie realizacji przez pośredników ich celów ekonomicznych, przy czym za takie wsparcie uznać należy legitymizowanie przez KE podziału rynku usług cyfrowych pomiędzy kilka podmiotów. Istnienie scentralizowanego rynku cyfrowego jest przez KE dostrzegane

¹⁶⁶ *Ochrona demokracji*, Komisja Europejska, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan_pl (dostęp: 12.01.2024).

¹⁶⁷ Tamże, pkt 4.4.

¹⁶⁸ *Komisja przedstawia wytyczne dotyczące ulepszenia kodeksu postępowania w zakresie zwalczania dezinformacji*, 26.05.2021, Komisja Europejska, https://ec.europa.eu/commission/presscorner/detail/pl/ip_21_2585 (dostęp: 12.01.2024).

¹⁶⁹ Wzmocniony kodeks postępowania w zakresie zwalczania dezinformacji z 2022 r.

¹⁷⁰ *Kodeks postępowania w zakresie dezinformacji z 2022 r.*, Komisja Europejska, <https://digital-strategy.ec.europa.eu/pl/policies/code-practice-disinformation> (dostęp: 12.01.2024).

oraz identyfikowane jako zagrożenie dla rozwoju gospodarki europejskiej i praw podstawowych ze względu na niski poziom kontestowalności, a zarazem zostaje usankcjonowane, w szczególności w AUC i ARC, jako sytuacja zastana i niepodlegająca wzruszeniu¹⁷¹. KE potwierdza, że celem przyjęcia aktu o rynkach cyfrowych (ARC) jest umożliwienie platformom wykorzystania ich pełnego potencjału dzięki rozwiązaniu na szczeblu UE problemu najpoważniejszych przypadków nieuczciwych praktyk i słabej kontestowalności, aby zarówno użytkownicy końcowi, jak i użytkownicy biznesowi mogli czerpać w pełni korzyści wynikające z gospodarki platform oraz gospodarki cyfrowej w ujęciu ogólnym, w kontestowalnym i uczciwym środowisku¹⁷².

Nie można nie dostrzec, że Komisja i Parlament Europejski nakładając na pośredników internetowych obowiązki określone w AUC i ARC, realizują własne cele polityczne, które nie byłyby do osiągnięcia bez współpracy z pośrednikami internetowymi. Cele te dotyczą realizacji swobody wypowiedzi. Strażnicy dostępu przyjęli do wykonania obowiązki mające znaczenie dla użytkowników internetu z całej UE, realizując zarazem wizję i próbując interpretację naświetloną przez KE, w szczególności w Decyzji ramowej z 2008 r. Pośrednicy internetowi przyjęli do wykonania zobowiązanie, które adresowane było do państw członkowskich. Komisja dzięki wsparciu przedsiębiorstw IT uzyskała skuteczny instrument oddziaływania w środowisku cyfrowym

¹⁷¹ KE stwierdza, że: „Słaba kontestowalność i nieuczciwe praktyki w sektorze cyfrowym to problem, który w przypadku niektórych usług cyfrowych występuje częściej i jest wyraźniejszy niż w przypadku innych usług. Dotyczy to w szczególności szeroko rozpowszechnionych i powszechnie wykorzystywanych usług cyfrowych i infrastruktury cyfrowych, które przeważnie bezpośrednio pośredniczą między użytkownikami biznesowymi a użytkownikami końcowymi. Doświadczenia w zakresie egzekwowania reguł konkurencji UE, jak również wyniki wielu sprawozdań i badań ekspertów oraz otwartych konsultacji publicznych świadczą o tym, że wiele usług cyfrowych ma następujące właściwości: (i) są to wysoce skoncentrowane, wielostronne usługi platformowe, w przypadku których jedna duża platforma cyfrowa lub bardzo ograniczona liczba dużych platform cyfrowych ustala warunki handlowe, mając w tym zakresie znaczną autonomię; (ii) kilka dużych platform cyfrowych pełni funkcję punktów dostępu umożliwiających użytkownikom biznesowym dotarcie do konsumentów i odwrotnie; oraz (iii) uprawnienia strażnika dostępu takich dużych platform cyfrowych są często nadużywane, co przejawia się nieuczciwym postępowaniem wobec ekonomicznie zależnych użytkowników biznesowych i konsumentów” (zob. ARC, s. 2).

¹⁷² Tamże, s. 3.

bezpośrednio na podmioty prawa prywatnego, w tym osoby fizyczne, w celu efektywnego stosowania prawa europejskiego.

Komisja występuje w podwójnej roli, tj. z jednej strony organu zlecającego obowiązki, a w konsekwencji kompetentnego w zakresie ustalania treści tych obowiązków, a z drugiej strony poręczyciela i egzekutora ich wykonania. Komisja Europejska poręcza zatem wykonanie przez strażników powierzonych im w AUC i ARC zadań publicznych, występując w charakterze gwaranta¹⁷³, który dysponuje arsenałem środków, w szczególności kar finansowych, przymuszających strażników dostępu do wykonania wskazanych w AUC i ARC zadań.

Komisja Europejska stała się interpretatorem obowiązków powierzonych przedsiębiorstwom IT; wywodzi stąd także uprawnienie do ingerowania w sferę praw i wolności jednostek. Uprawnienie to stanowi naturalną konsekwencję dokonywanej przez KE oceny wywiązywania się przez strażników dostępu z obowiązków wynikających z AUC i ARC. Ocena ta pozostaje bowiem w związku z realizacją wolności wypowiedzi przez użytkowników internetu i wywołuje, równolegle, skutek ustalający zakres tej wolności. KE uzyskała w ten sposób realny wpływ na sposób realizacji wolności wypowiedzi w internecie.

Komisja i PE określili w AUC i ARC wartości, których ochrony oczekują, powierzając zarazem rolę ich strażnika pośrednikom internetowym. Podmioty prywatne zastąpiły w realizacji tego zadania państwa członkowskie, których rola została zmarginalizowana. W ARC wskazano, że fragmentacji rynku wewnętrznego można skutecznie zapobiec jedynie wówczas, gdy państwa członkowskie nie będą mogły stosować przepisów krajowych, których zakres stosowania pokrywa się z zakresem stosowania rozporządzenia w sprawie usług cyfrowych (AUC) i które służą tym samym celom co niniejsze rozporządzenie. Nie wyklucza to możliwości stosowania do strażników dostępu

¹⁷³ Pojęcia „gwarancji” i „poręczenia” używam w szerokim znaczeniu, stąd występują one zamiennie. Zarówno umowa gwarancyjna, jak i poręczenie należą do „gwarancji” pojmowanych w ich sensie najobszerniejszym, potocznym, jednak wskazuje się na to, że „gwarancja” ma samodzielny i nieakcesoryjny charakter, co różni ją od umowy poręczenia. Cechą charakterystyczną gwarancji nie jest bowiem przejęcie zobowiązań dłużnika, lecz przejęcie ryzyka transakcji, które ponosi wierzyciel. Poręczyciel odpowiada za dłużnika głównego, gwarant zaś za uzyskanie zagwarantowanego rezultatu (zob. Wyrok SA w Warszawie z dnia 27 czerwca 2018 r., VI ACa 1879/16, LEX nr 2617884).

w rozumieniu niniejszego rozporządzenia innych przepisów krajowych, które służą innym uzasadnionym celom interesu publicznego określonym w TFUE lub które służą nadrzędnym względom interesu publicznego uznanym w orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej (zwanego dalej „Trybunałem Sprawiedliwości”)¹⁷⁴.

Komitet Regionów postulował, by zdefiniować pojęcie nadrzędnych względów interesu publicznego, przyjmując, że termin ten oznacza: „te w szczególności względy interesu ogólnego, które zostały uznane za takie w orzecznictwie Trybunału Sprawiedliwości, w tym następujące: polityka publiczna, bezpieczeństwo publiczne, zdrowie publiczne, zachowanie równowagi finansowej systemu zabezpieczenia społecznego, ochrona konsumentów, usługobiorców i pracowników, ochrona młodzieży, uczciwość transakcji handlowych, zwalczanie nadużyć, ochrona środowiska naturalnego i miejskiego, zdrowie zwierząt, własność intelektualna, zachowanie dziedzictwa historycznego, kulturowego i artystycznego, cele polityki społecznej i kulturalnej, mieszkalnictwo, promowanie kultury, badań i nauki, zapewnianie pluralizmu w mediach i równości mężczyzn i kobiet¹⁷⁵.

Ustanowiony w AUC i ARC system organów (podmiotów), na których ciąży wskazany w art. 1 AUC obowiązek zapewnienia „bezpiecznego, przewidywalnego, budzącego zaufanie środowiska internetowego” opiera się – z jednej strony – na systemie wzmocnionych kompetencji Komisji jako organu centralnego, dysponującego upoważnieniami do podejmowania w obszarze normowania, kontroli i nadzoru nad wykonaniem, a z drugiej strony na – lojalnej współpracy z cyfrowymi gigantami, którzy dysponują realnym władztwem w środowisku cyfrowym. Instrumentem oddziaływania na pośredników internetowych umożliwiającym określanie kierunków i programowanie oczekiwań, niezależnie od narzędzi stosowanych *ex post*, jak w szczególności nakładanie grzywien, stanowi negocjowalny z pośrednikami wzorzec należytej staranności.

¹⁷⁴ Motyw (aktu o rynkach cyfrowych).

¹⁷⁵ Opinia Europejskiego Komitetu Regionów – Akt o usługach cyfrowych i akt o rynkach cyfrowych (Dz.U. UE C z 2021 r. Nr 440, s. 67), poprawka nr 12.

D. Obowiązek starannego działania i neutralności jako kontratyp – aspekt materialnoprawny

Zmiana standardu wolności wypowiedzi w kierunku osłabienia jej ochrony następuje na dwóch płaszczyznach, tj. płaszczyźnie publicznoprawnej – co ujawnia się poprzez wyposażenie podmiotów prywatnych w kompetencje właściwe dla organów publicznych, w szczególności kompetencje do ingerowania w sferę wolności, w tym stosowania środków organizacyjnych i technicznych wywołujących skutek prewencyjny, ograniczający korzystanie z wolności wypowiedzi – oraz w sferze prywatnoprawnej poprzez przyjęcie rozwiązań statuujących i legalizujących asymetrię wolności wypowiedzi i informacji pomiędzy podmiotami prawa prywatnego oraz poszerzenie zakresu uprawnień przysługujących pośrednikom internetowym kosztem odbiorców usług i pozostałych użytkowników internetu. Rozwiązaniom tym towarzyszy trend konfrontowania wolności wypowiedzi z innymi wartościami takimi jak prawo do niedyskryminacji, równouprawnienia płci oraz prawo do tożsamości, które uzyskują ochronę porównywalną albo dalej idącą niż ochrona przyznana wolności wypowiedzi.

O ile wolność wypowiedzi – w ujęciu formalnym – nadal zajmuje wysokie miejsce w hierarchii wartości chronionych, to jednak jej ranga jest osłabiana ze względu na zrównanie poziomu jej ochrony z innymi wartościami wywodzonymi z Karty praw podstawowych i europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności, pomimo że wartości te nie były wprost wymienione w tych aktach prawnych. W drodze poprawki zgłoszonej przez Komisję Europejską w dniu 20 stycznia 2022 r. do projektu rozporządzenia w sprawie jednolitego rynku usług cyfrowych (AUC) Parlament Europejski uzupełnił treść motywu 3 rozporządzenia, poszerzając – w stosunku do pierwotnego projektu – katalog praw i wolności, które powinny podlegać ochronie w środowisku cyfrowym¹⁷⁶. Wymieniając prawa i wolności wymagające ochrony, poza wolnością wypowiedzi i informacji oraz wolnością prowadzenia działalności gospodarczej, które były wskazywane w pierwotnym

¹⁷⁶ Poprawki przyjęte przez Parlament Europejski w dniu 20 stycznia 2022 r. w sprawie wniosku dotyczącego AUC.

tekście projektu AUC¹⁷⁷, Komisja Europejska uzupełniła katalog o: prawo do prywatności, ochrony danych osobowych i poszanowania godności ludzkiej, a także równouprawnienie płci i prawo do niedyskryminacji¹⁷⁸. W tym samym miejscu (motyw 3 AUC) wskazano na cele nadrzędne, jakie powinno realizować rozporządzenie AUC, tj. zapewnienie bezpiecznego, dostępnego, przewidywalnego i budzącego zaufanie środowiska internetowego oraz umożliwienie obywatelom Unii i innym osobom korzystanie z przysługujących im praw podstawowych i wolności zagwarantowanych w Karcie praw podstawowych Unii Europejskiej (KPP). Zasygnalizowano zarazem, co zostało następnie szeroko rozwinięte w kolejnych postanowieniach AUC i ARC, jaki mechanizm należy zastosować dla spełnienia powyższych założeń. Wskazano zatem, że zasadnicze znaczenie dla osiągnięcia zakładanego celu ma wypełnienie przez dostawców usług pośrednich obowiązku dochowania należytej staranności. W ten sposób ciężar działania został przeniesiony z podmiotów publicznych na pośredników internetowych, którym ustawodawca europejski pozostawił swobodę wyboru adekwatnych środków organizacyjnych i technicznych oraz wyposażył ich w domniemanie zgodności z prawem także takiego działania, które ingeruje, ze względu na zastosowane przez pośrednika środki, w wolność wypowiedzi usługobiorców.

Wymóg należytej staranności i wynikające z niego obowiązki szczegółowe podlegały – jak zostało to przesądzone w AUC – harmonizacji¹⁷⁹. Dyskusyjne

¹⁷⁷ Tamże, motyw 3.

¹⁷⁸ Tamże, motyw 3 w brzmieniu po przyjęciu przez PE poprawki z dnia 20 stycznia 2022 r.

¹⁷⁹ Pojęcie harmonizacji odnosi się do stopnia spójności rozwiązań prawnych, których adresatem stają się obywatele wszystkich państw członkowskich UE. Harmonizacja minimalna w procesie transpozycji polega na pozostawieniu państwom członkowskim większej swobody w określaniu standardów i wymagań ochrony wyższych niż ustalone w dyrektywie, w tym – w utrzymaniu już obowiązujących w prawie krajowym rozwiązań korzystniejszych dla chronionej grupy podmiotów (np. konsumentów). Mimo implementacji tej samej dyrektywy w całej UE, uregulowania w poszczególnych krajach pozostają zróżnicowane. Z kolei – jak zauważa się w doktrynie – „harmonizacja maksymalna (pełna), nakazująca implementację *in extenso* przepisów dyrektywy, pozostaje ciągle w fazie próbnej, budząc od dawna sceptycyzm doktryny, m.in. ze względu na zbyt szeroki zakres stosowania, nadmierną ingerencję w wykładnię tradycyjnych instytucji prawa prywatnego (narzucanie definicji pojęć) oraz zaburzenie struktury skodyfikowanych systemów prawnych” (zob. W.J. Kocot, *Europeizacja materialnego prawa prywatnego – stan obecny i perspektywy*, „Państwo i Prawo” 2020, nr 2, s. 100).

pozostaje, czy harmonizacja obowiązków dostawców usług ma charakter pełny, minimalny czy mieszany. Pojęcie należytej staranności jest konstrukcją elastyczną, która pozwala na modyfikowanie modelu pożądanego zachowania, którego kształt zależy od okoliczności faktycznych, w jakich dostawca usług działał. Posłużenie się przez ustawodawcę europejskiego konstrukcją należytej staranności pozostawia zatem margines swobody oceny, w pierwszej kolejności dostawcom, którzy dokonują doboru środków i metod działania, a w dalszej kolejności innym właściwym organom, w tym pozasądowym dekodującym treść tego obowiązku *in casu*.

Obowiązki w zakresie należytej staranności są niezależne od kwestii odpowiedzialności dostawców usług pośrednich, należy je zatem oceniać oddzielnie. Dochowanie należytej staranności nie stanowi zatem samoistnej przesłanki uchylenia się przez dostawcę od odpowiedzialności prawnej. Obowiązki w zakresie należytej staranności – jak wskazano w AUC – są potrzebne, aby zaradzić zidentyfikowanym obawom dotyczącym ochrony interesów odbiorców usługi, w szczególności zwalczanie nielegalnych praktyk i ochrona praw podstawowych zapisanych w Karcie (motyw 41).

Niedopełnienie obowiązku należytej staranności może uzasadniać zarzut „przyczynienia się do naruszenia”, a w konsekwencji prowadzić do poniesienia odpowiedzialności. Zakres obowiązku należytej staranności zależy od tego, czy i w jakim zakresie od „osoby przyczyniającej się do naruszenia” można racjonalnie wymagać, aby sprawdzała lub kontrolowała działania osób trzecich w celu przeciwdziałania naruszeniom, w tym rozpowszechnianiu nielegalnych treści lub naruszeniom własności intelektualnej¹⁸⁰.

Nie można jednak pominąć, że ewentualne uchylenie się przez dostawców usług cyfrowych od odpowiedzialności prawnej dotyczy wyłącznie sytuacji, gdy dochodzi do naruszenia prawa przez odbiorcę usługi, nie zaś wówczas, kiedy naruszenia dokonuje pośrednik internetowy. Przesłanki uchylenia odpowiedzialności wymienione w dyrektywie o handlu elektronicznym (art. 12–14) oraz AUC (art. 4–6) nie znajdują zastosowania do naruszeń dokonywanych przez dostawcę usług także wówczas, gdy przedmiotem

¹⁸⁰ Wyrok TS z dnia 22 czerwca 2021 r. w sprawie Frank Peterson przeciwko Google LLC i in., C-682/18, pkt 121, LEX nr 3189118 (dalej: Wyrok TS w sprawie Frank Peterson przeciwko Google).

naruszenia jest wolność wypowiedzi. Przeciwnie, ustawodawca europejski dopuszcza i legalizuje działalność polegającą na monitorowaniu treści (motyw 66), usuwaniu treści (motyw 54), ograniczaniu widoczności w internecie (motyw 54), depozycjonowaniu (motyw 55), demonetyzacji (art. 3 pkt t AUC), moderowaniu treści (motywy: 45, 49, 66, 84, 86, 97), usuwaniu treści (motywy: 22, 26, 87, 145), a także zawieszeniu, zakończeniu lub innym ograniczeniu płatności pieniężnych na rzecz odbiorcy usługi (art. 17 ust. 1 pkt b AUC), zawieszeniu lub zakończeniu świadczenia usługi w całości lub w części (art. 17 ust. 1 pkt c AUC), zawieszeniu lub zamknięciu konta odbiorcy usługi (art. 17 ust. 1 pkt d AUC).

Ustawodawca europejski nie przewidział żadnego ustawowego mechanizmu ustalania odpowiedzialności prawnej pośredników internetowych za usuwanie legalnych treści ani za nadużycia dostawcy usług, który w sposób nieproporcjonalny ogranicza wolność wypowiedzi albo czyni to bez wystarczającej podstawy bądź powołuje się na wadliwie ustalone przyczyny. Ustawodawca europejski przenosi na podmioty prywatne, tj. pośredników internetowych, kompetencje zarówno w zakresie wykrywania treści szkodliwych i nielegalnych, jak i ustalania ich bezprawnego statusu, a nadto w zakresie prowadzenia postępowania sprawdzającego i procedury odwoławczej z wykorzystaniem swobodnie wypracowanych i przyjmowanych przez pośredników internetowych polityk i procedur.

Obowiązek starannego działania nie oznacza ogólnego obowiązku monitorowania, jednakże takie działanie, tj. polegające na filtrowaniu treści, legalizuje. Zastosowanie także innych środków ingerujących w wolność wypowiedzi takich jak moderowanie, blokowanie treści, ograniczanie dostępu lub usuwanie treści jest – co do zasady – legalne, jeśli stanowi realizację obowiązku starannego działania dostawcy. W art. 8 AUC zastrzeżono co prawda, że „na dostawców usług pośrednich nie nakłada się ogólnego obowiązku monitorowania informacji, które dostawcy ci przekazują lub przechowują, ani aktywnego ustalania faktów lub okoliczności wskazujących na nielegalną działalność”, jednakże brak ogólnego obowiązku monitorowania nie powoduje, że stosowanie przez pośredników rozwiązań technicznych lub podejmowanie innych środków jest niezgodne z prawem. Dostawcy mogą – co do zasady – stosować ograniczenia świadczenia usług, w tym moderować treści, usuwać je, ograniczać do nich dostęp, a nawet uzyskiwać informacje

dotyczące usługobiorców za pomocą własnych metod, o ile podejmowane działania nie są arbitralne albo dyskryminacyjne (motyw 56).

Dochowanie należytej staranności nie stanowi samoistnej przesłanki uchylającej odpowiedzialność prawną dostawcy usług. Jak bowiem przesądził ustawodawca europejski, obowiązki w zakresie należytej staranności są niezależne od kwestii odpowiedzialności dostawców usług pośrednich, należy je zatem oceniać oddzielnie (motyw 41 AUC).

Powołanie się przez pośrednika na obowiązek starannego działania – paradoksalnie – usprawiedliwia stosowanie środków ingerujących w wolność wypowiedzi. Dopiero bowiem nadmierne (zbyt częste, zbyt intensywne) albo nieadekwatne (nieproporcjonalne w stosunku do zagrożenia) wykorzystanie przez dostawcę tych środków może zostać ocenione jako naruszenie przez dostawcę zasady neutralności i stanowić skuteczny zarzut pozbawiający dostawcę możliwości uchylenia się od odpowiedzialności.

Należy zatem wskazać, że na gruncie AUC ustawodawca europejski ustanowił dwa równoległe mechanizmy wyłączania odpowiedzialności. Pierwszy jest uruchamiany wówczas, gdy do naruszenia prawa doszło przez odbiorcę usługi, jednakże pośrednik pod warunkami wskazanymi w art. 4–6 AUC (a dla dostawców pozostałych usług społeczeństwa informacyjnego na warunkach wskazanych w art. 12–15 dyrektywy o handlu elektronicznym) może uchylić się od odpowiedzialności prawnej. Odpowiedzialność ponosić będzie wówczas wyłącznie odbiorca usługi. Drugi mechanizm wyłączania odpowiedzialności, tym razem w odniesieniu do naruszeń spowodowanych wkroczeniem przez dostawców usług w sferę praw i wolności chronionych na podstawie Karty praw podstawowych, w szczególności w związku z naruszeniem wolności wypowiedzi, zostaje uruchomiony poprzez powołanie się pośrednika internetowego na obowiązek działania z należytą starannością.

Wymóg staranności pozwala bowiem na usprawiedliwienie bardziej intensywnej ingerencji pośrednika w sferę wolności odbiorcy usługi wówczas, gdy pośrednik uzna to za konieczne ze względu na potrzebę ochrony interesu publicznego. Interes publiczny oznacza działanie w celu ochrony porządku publicznego, prawnie uzasadnionych interesów odbiorców usługi, zwalczanie nielegalnych praktyk i ochrony praw podstawowych zapisanych w Karcie (motyw 41). Definiowanie interesu publicznego zostało *de facto* pozo-

powinien dokonywać *ad hoc*, a zatem stało się zadaniem należącym – przynajmniej w pierwszej fazie – do pośrednika internetowego.

Wyłączenia odpowiedzialności pośredników ustanowione w AUC nie powinny mieć zastosowania w przypadku, gdy dostawca usług pośrednich, zamiast ograniczać się do świadczenia usług w sposób neutralny poprzez czysto techniczne i automatyczne przetwarzanie informacji przekazanych przez odbiorcę usług, odgrywa aktywną rolę, która może pozwolić mu na powzięcie wiedzy o tych informacjach lub sprawowanie nad nimi kontroli (motyw 18 AUC). Obowiązek neutralności był przewidziany w dyrektywie o handlu elektronicznym i został utrzymany w rozporządzeniu o usługach cyfrowych (AUC). O ile jednak na gruncie dyrektywy 2000/31 TSUE dopuszczalność uchylenia się dostawców usług jest warunkowana obowiązkiem wykazania, że ich działanie nie naruszyło zasady neutralności, o tyle na gruncie AUC o uchyleniu odpowiedzialności pośrednika decyduje wynik ważenia pomiędzy obowiązkiem neutralności a obowiązkiem starannego działania pośrednika. Obowiązki te nie zawsze się uzupełniają. Może zdarzyć się bowiem, że realizacja modelu starannego działania, jakiego ustawodawca europejski oczekuje od pośrednika, pociąga za sobą naruszenie zasady neutralności. Wobec powyższego podzielić należy spostrzeżenie K. Gliścińskiego, że „istnieje konieczność wprowadzenia jakichś gwarancji *ex ante* o randze ustawowej. Obecny stan wiedzy [...] uzasadnia bowiem twierdzenie, że zagrożenie naruszenia praw podstawowych takich jak wolność wypowiedzi w ramach nowego reżimu odpowiedzialności – w braku takich gwarancji – będzie występowało i miało charakter masowy”¹⁸¹.

Zastosowanie wyłączeń odpowiedzialności, o których mowa w art. 4–5 AUC, jest zatem – co prawda – nadal uzależnione od respektowania zasady neutralności przez dostawcę, a więc poprzez wykazanie, że jego aktywność wobec użytkowników internetu stanowiła czysto techniczne i automatyczne przetwarzanie informacji przekazanych przez odbiorcę usługi¹⁸², ale zarazem ustalenie

¹⁸¹ K. Gliściński, *Gwarancje ex ante praw użytkowników na tle wyroku Trybunału Sprawiedliwości z 26.04.2022 r., C-401/19, Rzeczpospolita Polska przeciwko Parlamentowi Europejskiemu i Radzie Unii Europejskiej*, „Europejski Przegląd Sądowy” 2023, nr 3, s. 28–36.

¹⁸² W. Chomiczewski, *Zasady wyłączeń odpowiedzialności dostawców usług pośrednich w projekcie rozporządzenia Akt o usługach cyfrowych (cz. I)*, „Prawo Nowych Technologii” 2021, nr 2, s. 19.

zakresu neutralności jest wypadkową ustaleń podjętych przez dostawcę w wyniku starannego działania. Na gruncie AUC obowiązki te zakresowo nie tylko się nie uzupełniają, ale mogą pozostawać ze sobą w sprzeczności. Oznacza to, że w pewnych sytuacjach, uzasadnionych interesem publicznym, na pośredniku spoczywać będzie obowiązek filtrowania, moderowania, usuwania lub ograniczania treści, a nawet tzw. shadow banning, czyli blokowanie widoczności wpisów danego użytkownika dla całej społeczności internetowej poza autorem bez jego wiadomości (motyw 55).

Nie można zgodzić się z wyrażanym w doktrynie stanowiskiem, że aktualne pozostaje – jak zauważa W. Chomiczewski – stanowisko orzecznictwa tak TSUE, jak i sądów polskich, które odmawiały możliwości powołania się przez pośrednika na wyłączenia odpowiedzialności w przypadkach, gdy przestawał on zachowywać się neutralnie względem treści¹⁸³, lecz zaczynał wpływać chociażby na ich widoczność w swoim serwisie¹⁸⁴. Obowiązek neutralności w mniejszym bowiem stopniu niż miało to miejsce na gruncie dyrektywy o handlu elektronicznym (art. 14 ust. 1) stanowić będzie mechanizm ograniczający (blokujący) ingerencję *ex ante* pośrednika w sferę wolności wypowiedzi odbiorców usług i użytkowników internetu.

Spełnienie wymogu neutralności na gruncie dyrektywy 2000/31 wskazywało, że działalność usługodawcy ma charakter czysto techniczny, automatyczny i bierny, co oznacza, że nie posiada on wiedzy na temat informacji przekazywanych lub przechowywanych przez jego klientów ani kontroli nad nimi oraz że nie odgrywa on aktywnej roli poprzez umożliwienie klientom optymalizacji ich działalności polegającej na sprzedaży online, czego ustalenie

¹⁸³ W wyroku z dnia 18 września 2017 r. Sąd Apelacyjny w Krakowie stwierdził, że „podmiot współuczestnicząc w realizowaniu transferów naruszających majątkowe prawa autorskie, jest współsprawcą, współnaruszycielem praw innych osób do utworów. Tym samym w pełni uzasadnione jest stanowisko, iż sposób działania podmiotu sprawia, że nie może być on traktowany jako podmiot podlegający art. 14 ustawy o świadczeniu usług drogą elektroniczną, lecz jest po prostu podmiotem, który także sam bezprawnie rozpowszechnia chronione prawem autorskim utwory. Skoro tak – to podmiot nie może powoływać się na art. 14 i 15 ustawy o świadczeniu usług drogą elektroniczną, a do przyjęcia jego odpowiedzialności należy zastosować art. 79 ustawy o prawie autorskim i prawach pokrewnych” (Wyrok SA w Krakowie z dnia 18 września 2017 r., I ACa 1494/15, LEX nr 2354397).

¹⁸⁴ Tamże, s. 22.

należy do sądu odsyłającego¹⁸⁵. Zachowanie neutralne TSUE definiował jako „(brak) aktywnej roli, dzięki której pośrednik ma informacje o treściach zamieszczonych na jego platformie i może je kontrolować”¹⁸⁶. Już bowiem na gruncie dyrektywy o handlu elektronicznym TSUE wywiódł zasadniczo dwie przesłanki, które warunkują dopuszczalność uchylecia się przez pośrednika od odpowiedzialności za rozpowszechniane treści lub świadczone usługi. Jest to – po pierwsze – przesłanka neutralności i – po drugie – dochowanie przez dostawcę usługi należytej staranności¹⁸⁷.

W wyroku z dnia 22 czerwca 2021 r. w sprawie Frank Peterson przeciwko Google TSUE dostrzegł w art. 14 ust. 1 dyrektywy 2000/31 TSUE wskazanie, że tenże artykuł należy interpretować następująco: działalność dostawcy usługi jest objęta zakresem stosowania tego przepisu pod warunkiem – po pierwsze – że operator ten nie odgrywa aktywnej roli, dzięki której ma informacje o treściach zamieszczonych na jego platformie i może je kontrolować oraz – po drugie – że brak jest wiarygodnej informacji, która potwierdzałaby, że rozpowszechniane treści są bezprawne (nielegalne). Dostawca nie poniesie zatem odpowiedzialności wówczas, gdy nie wie o konkretnych bezprawnych działaniach użytkowników internetu. TSUE zauważył, że powiadomienie o treściach chronionych, które zostały bezprawnie udostępnione publicznie, musi zawierać wystarczające informacje umożliwiające operatorowi tej platformy stwierdzenie, bez konieczności przeprowadzania szczegółowego badania stanu prawnego, czy udostępnienie to jest bezprawne i czy ewentualne usunięcie tych treści nie będzie kolidować z wolnością wypowiedzi¹⁸⁸. TSUE wskazał zarazem, że zaniechanie działania przez dostawcę pomimo wejścia w posiadanie informacji o bezprawnych treściach może być identyfikowane jako „przyczynienie się do naruszenia” i przesądzać o pociągnięciu dostawcy do odpowiedzialności.

„Przyczynienie się do naruszenia” zostało przez TSUE zidentyfikowane jako niedochowanie przez dostawcę należytej staranności¹⁸⁹. TSUE wskazał, że:

¹⁸⁵ Wyrok TS z dnia 7 sierpnia 2018 r. w sprawie Coöperatieve Vereniging SNB-RE-ACT U.A. przeciwko Deepakowi Mehcie, C-521/17, pkt 52 i pkt 2 sentencji, poz. I-639.

¹⁸⁶ Wyrok TS w sprawie Frank Peterson przeciwko Google.

¹⁸⁷ Tamże, pkt 115.

¹⁸⁸ Tamże, pkt 116.

¹⁸⁹ Tamże, pkt 121.

każdy, kto nie będąc sprawcą albo współsprawcą naruszenia, umyślnie przyczynia się do niego w jakikolwiek sposób i w adekwatnym związku przyczynowym, mimo że miał prawną i materialną możliwość przeciwdziałania naruszeniu, może ponosić odpowiedzialność jako „osoba przyczyniająca się do naruszenia”. Powstanie „odpowiedzialności za przyczynienie się do naruszenia” zakłada zatem naruszenie obowiązku starannego działania, którego zakres zależy od tego, czy i w jakim zakresie od „osoby przyczyniającej się do naruszenia” można racjonalnie wymagać, aby sprawdzała lub kontrolowała działania osób trzecich w celu przeciwdziałania naruszeniom [...] ¹⁹⁰.

O ile wskazane w art. 12–14 dyrektywy 2000/31 i art. 4–6 AUC przesłanki wyłączenia odpowiedzialności pośredników internetowych są – co do brzmienia – takie same, o tyle, ze względu na treść wskazówek interpretacyjnych, w szczególności zawartych w motywach 22, 26, 40 i 41 AUC, a także treść przepisów zawartych w rozdziale III AUC, będą one musiały być inaczej stosowane. Ustawodawca europejski rozwinął bowiem wykładnię terminu „należyta staranność”, poświęcając mu rozdział III AUC zatytułowany *Obowiązki w zakresie należytej staranności na potrzeby przejrzystego i bezpiecznego środowiska internetowego*. Wskazano w nim szczegółowo obowiązki składające się na model wymaganego od dostawców usług poziomu staranności. W konsekwencji oznacza to, że powołanie się przez dostawcę usług na brak wiarygodnej wiadomości o bezprawnym charakterze przechowywanej wiadomości, co było wystarczające na gruncie art. 14 ust. 1 dyrektywy, może okazać się niewystarczające dla uchylenia się od odpowiedzialności na gruncie art. 6 AUC. Nieprzekazanie przez osoby trzecie wiarygodnej informacji o nielegalnych treściach nadal nie zwalnia – na gruncie art. 6 AUC – pośrednika od odpowiedzialności prawnej. Konieczne jest bowiem jeszcze wykazanie przez pośrednika, że podjął on czynności polegające na przeciwdziałaniu rozpowszechnieniu nielegalnych treści, w szczególności stosował metody filtrujące i monitorujące, a także moderował udostępniane treści.

Ustawodawca europejski przesądził w AUC o tym, że dostawca usług jest uprawniony do podejmowania działań w celu uzyskania faktycznej wiedzy

¹⁹⁰ Wyrok TS w sprawie Frank Peterson przeciwko Google.

o nielegalnym charakterze treści, między innymi w drodze czynności sprawdzających prowadzonych z własnej inicjatywy lub zgłoszeń przekazanych mu przez osoby lub podmioty zgodnie z niniejszym rozporządzeniem, o ile takie zgłoszenia są wystarczająco precyzyjne i odpowiednio uzasadnione, aby umożliwić działającemu z należytą starannością podmiotowi gospodarczemu rozsądną identyfikację i ocenę potencjalnie nielegalnych treści oraz, w stosownych przypadkach, podjęcie przeciwko nim działań (motyw 22).

Znacząca jest także zmiana sposobu, w jaki ustawodawca europejski definiuje rodzaj wiadomości, która – w ujęciu art. 13–14 ust. 1 dyrektywy 2000/31 oraz art. 5–6 ust. 1 AUC – obliuguje dostawcę usług do podjęcia aktywności w celu usunięcia lub uniemożliwienia dostępu do nielegalnej treści. O ile zatem w dyrektywie 2000/31 ustawodawca europejski posługiwał się pojęciem wiarygodnej wiadomości o tyle w rozporządzeniu o usługach cyfrowych (AUC) pojawia się termin faktycznej wiedzy o nielegalnej działalności lub nielegalnych treściach oraz wiedzy o stanie faktycznym lub okolicznościach, które w sposób oczywisty świadczą o nielegalnej działalności lub nielegalnych treściach (art. 14 ust. 1 AUC).

Zmiana na poziomie językowym prowadząca do zastąpienia terminu „wiarygodna wiadomość” terminem „faktycznej wiedzy” zobowiązuje do zmiany wykładni, a w konsekwencji zmiany sposobu definiowania wymaganego od dostawców modelu staranności.

Obowiązek dostawcy traci charakter wyłącznie reaktywny i wymaga od dostawcy proaktywnego działania. W świetle rozwiązań zawartych w AUC niewystarczające może okazać się zachowanie pośrednika internetowego, który reaguje na nielegalne treści wyłącznie wówczas, gdy zostaje o nich zawiadomiony (poweźmie wiarygodną wiadomość). Konieczne staje się bowiem, by dostawca podejmował samodzielne ustalenia w kierunku wykrywania i przeciwdziałania rozpowszechnianiu takich treści. Jak wskazano bowiem w motywie 22 AUC, dostawca może uzyskać taką faktyczną wiedzę lub wiadomość o nielegalnym charakterze treści między innymi w drodze czynności sprawdzających prowadzonych z własnej inicjatywy lub zgłoszeń przekazanych mu przez osoby¹⁹¹ lub podmioty zgodnie z AUC (art. 16 AUC).

¹⁹¹ Motyw 22 AUC.

Słusznie spostrzega Xawery Konarski, że możliwość skorzystania z warunków wyłączenia odpowiedzialności, określonych w AUC dla dostawców usług pośrednich, zależna jest od łącznego spełnienia dwóch przesłanek: 1) dochowania przez pośredników internetowych wymogu neutralności (pasywności) względem przekazywanych/przechowywanych w internecie treści oraz 2) podjęcia przez nich działań w celu uniemożliwienia dostępu do treści, po uzyskaniu wiedzy/informacji o ich nielegalnym charakterze¹⁹². Nie można jednakże pominąć, że obowiązek dostawców „podjęcia działań w celu uniemożliwienie dostępu do treści” w świetle przyjętych w AUC rozwiązań jest rozumiany szeroko, tj. nie tylko wówczas, gdy pośrednik zostanie zawiadomiony przez podmiot zewnętrzny o przechowywaniu nielegalnych treści (wiarygodna wiadomość), ale także wtedy, gdy samodzielnie ustala i dochodzi własnymi metodami potwierdzenia ich wiarygodności. W tym celu jest on uprawniony do przeszukiwania zasobów w celu wykrycia treści nielegalnych, a nawet ich blokowania *ex ante*, tj. przed ich publicznym udostępnieniem (motyw 55 AUC). Z art. 23 ust. 1 AUC wynika wprost nakaz zawieszania świadczenie usług na rzecz odbiorców usługi często przekazujących oczywiście nielegalne treści.

Wskazane powyżej zmiany mają charakter jakościowy i przesądzają – zarówno w aspekcie podmiotowym, jak i przedmiotowym – o treści standardu wolności wypowiedzi, jego granicach, strukturze i konstrukcji. Ustawodawca europejski włączył podmioty prywatne w proces budowania standardu wolności wypowiedzi i wyposażył je w upoważnienia oraz narzędzia do oddziaływania na zakres i sposób realizacji wolności wypowiedzi przez odbiorców usług i pozostałych użytkowników internetu. Granice wolności wypowiedzi w internecie wyznacza z jednej strony standard starannego działania dostawców, a z drugiej strony obowiązek dochowania przez nich zasady neutralności. Zakres wolności wypowiedzi jest odwrotnie proporcjonalny do rygoryzmu przyjętego przez dostawców usług modelu staranności. Im bardziej zatem rygorystyczny standard staranności przyjmować będzie dostawca, w tym większym stopniu zagrożona staje się realizacja wolności wypowiedzi.

¹⁹² X. Konarski, *Unijny Akt o Usługach Cyfrowych – cele uchwalenia, zakres stosowania oraz najważniejsze obowiązki dostawców usług pośrednich*, „Prawo Nowych Technologii” 2022, nr 3, s. 33.

E. Instytucja dobrego samarytanina – domniemanie prawne wzruszalne

Działanie pośredników internetowych ingerujących w wolność wypowiedzi zostało objęte domniemaniem zgodności z prawem. Domniemanie to, nazwane w doktrynie instytucją dobrego samarytanina¹⁹³, zostało zawarte w art. 7 AUC. Zgodnie z tym przepisem, dostawców usług pośrednich nie uważa się za niekwalifikujących się do wyłączeń odpowiedzialności, o których mowa w art. 4, 5, 6 tylko z tego powodu, że:

w dobrej wierze i z należytą starannością prowadzą z własnej inicjatywy dobrowolne czynności sprawdzające lub podejmują inne środki mające na celu wykrycie, identyfikację i usunięcie nielegalnych treści lub unie możliwienie do nich dostępu lub podejmują niezbędne środki, aby spełnić wymogi prawa Unii i prawa krajowego zgodnego z prawem Unii, w tym wymogi określone w niniejszym rozporządzeniu (art. 7 AUC).

W motywie 56 AUC wskazano ponadto, że dostawca usług hostingu może w niektórych przypadkach uzyskać za pomocą własnych podejmowanych dobrowolnie środków informacje dotyczące określonej działalności odbiorcy usługi, takiej jak przekazywanie niektórych rodzajów nielegalnych treści, które racjonalnie uzasadniają – uwzględniając wszystkie istotne okoliczności, których dostawca usług hostingu ma świadomość – podejrzenie, że ten odbiorca mógł popełnić, może właśnie popełniać lub może popełnić przestępstwo.

Działanie dobrego samarytanina nie stanowi, w świetle art. 7 AUC, naruszenia zasady neutralności¹⁹⁴. O ile więc na gruncie art. 14 ust. 1 dyrektywy

¹⁹³ Tamże, s. 36.

¹⁹⁴ Poparcie dla wprowadzenia klauzuli dobrego samarytanina wyraził polski rząd w ramach konsultacji z państwami członkowskimi projektu AUC. Wskazano, że „Należy zrezygnować z nieprzystającego do obecnych realiów wymogu bierności pośrednika wobec treści, jako przesłanki korzystania przez niego ze zwolnienia z odpowiedzialności za treści użytkowników. W obecnych warunkach rynku cyfrowego pewien stopień aktywności wobec treści jest nieodłącznym elementem świadczenia usług”. Zob. *Postulaty Rządu RP ws. Aktu o Usługach Cyfrowych (DSA)*, <https://www.gov.pl/attachment/49fcf246-83d3-47fe-bf31-497d6b4f554a> (dostęp: 28.08.2023).

2000/31 należało zakładać, że działanie polegające na filtrowaniu treści, uniemożliwianiu do nich dostępu, moderowaniu zostanie ocenione jako naruszenie zasady biernego, czysto automatycznego przetwarzania informacji, a w konsekwencji uniemożliwi powoływania się przez dostawcę na przesłanki uchylające odpowiedzialność¹⁹⁵, o tyle – zgodnie z literalnym brzmieniem art. 7 AUC – działania te zostały zalegalizowane jako nie tylko dopuszczalne oraz zgodne z zasadą neutralności, lecz także oczekiwane i stanowią one konkretyzację modelu należytej staranności.

Zgodnie z orzecznictwem TSUE, aby czynność podmiotu świadczącego usługę w internecie mogła zostać objęta art. 14 dyrektywy 2000/31, podmiot ten koniecznie musiał być „usługodawcą będącym pośrednikiem” w rozumieniu art. 14 ust. 1 dyrektywy¹⁹⁶. Na gruncie dyrektywy nie było tak w przypadku usługodawcy, który, zamiast ograniczyć się do neutralnego świadczenia usługi w drodze czysto technicznego i automatycznego przetwarzania danych dostarczonych przez jego klientów, odgrywał czynną rolę, która mogła pozwolić mu na powzięcie wiedzy o tych danych lub na sprawowanie nad nimi kontroli¹⁹⁷. Na gruncie AUC stanowisko to zostało – jak się wydaje – z jednej strony wzmocnione, z drugiej zaś całkowicie straciło na znaczeniu. Pomiędzy tymi ocenami nie ma – wbrew pozorom – sprzeczności. Trzeba bowiem zauważyć, że wzmocnienie zasady neutralności dotyczy jedynie takich sytuacji, kiedy pośrednik wspiera odbiorcę usługi i identyfikuje się z jego celami. Aktywne działanie w świetle aktualnego stanowiska prawodawcy europejskiego to takie, które w sposób ukryty, pod pozorem neutralności, wspiera odbiorcę usługi. W przypadku zatem gdy dostawca usług pośrednich umyślnie współpracuje z odbiorcą usługi w celu podjęcia nielegalnych działań, nie należy uznawać, że usługę wyświadczono w sposób

¹⁹⁵ W. Chomiczewski, *Zasady wyłączeń odpowiedzialności dostawców usług pośrednich w projekcie rozporządzenia Akt o usługach cyfrowych (cz. II)*, „Prawo Nowych Technologii” 2022, nr 1, s. 24.

¹⁹⁶ Wyrok TS z dnia 23 marca 2010 r. w sprawach połączonych Google France i Google przeciwko Louis Vuitton Malletier SA, od C-236/08 do C-238/08, pkt 112, (dalej: Wyrok TS w sprawach połączonych Google France i Google), <https://curia.europa.eu/juris/document/document.jsf?text=&docid=83961&pageIndex=o&doclang=PL&mode=lst&dir=&occ=first&part=1&cid=2424771> (dostęp: 22.08.2023).

¹⁹⁷ Wyrok TS z dnia 12 lipca 2011 r. w sprawie L'Oréal SA i in. przeciwko eBay International AG i in., C-324/09, poz. I-6011 (dalej: Wyrok TS w sprawie L'Oréal przeciwko eBay).

neutralny i w związku z tym dostawca usług nie powinien mieć możliwości korzystania z wyłączeń odpowiedzialności określonych w niniejszym rozporządzeniu (motyw 20 AUC). Nie będzie natomiast stanowiło naruszenia zasady neutralności takie działanie, którego skutkiem jest osłabienie pozycji odbiorcy usługi (depozycjonowanie) i ograniczenie jego wolności wówczas, jeśli dostawca działał w celu zapobieżenia rozpowszechnieniu treści nielegalnych, będąc w posiadaniu albo chcąc uzyskać „faktyczną wiedzę” o nielegalnej działalności lub nielegalnych treściach (art. 6 ust. 1 lit. a AUC).

Co prawda naruszeniem neutralności będzie – co do zasady – „odgrywanie przez pośrednika aktywnej roli, która może pozwolić na powzięcie wiedzy o tych informacjach lub sprawowanie nad nimi kontroli” (motyw 18 AUC), to jednak instytucja dobrego samarytanina wprost zezwala na wykonywanie tej aktywnej roli. Za działalność fałszywych host providerów¹⁹⁸ uważana będzie więc przede wszystkim działalność dostawcy, której rezultatem jest wsparcie jednej kategorii odbiorców usług kosztem innej. Dużo trudniejsze będzie natomiast wykazanie, że sprzeczna z zasadą neutralności jest ingerencja w wolność wypowiedzi odbiorcy usługi podjęta w celu ustalenia, czy rozpowszechniane przez niego treści nie mają nielegalnego charakteru. W takich bowiem okolicznościach przesłanką uchylającą odpowiedzialność pośrednika będzie odwołanie się do ciężącego na nim obowiązku należytej staranności (motyw 41 oraz rozdział III AUC). Jest zatem prawdopodobne, że pośrednik będzie skutecznie uchylał się od zarzutu naruszenia zasady neutralności, a w konsekwencji będzie miał dużą swobodę działania z powołaniem na instytucję dobrego samarytanina.

W literaturze wyrażony został pogląd, że zmiana, która dopuszcza wprost możliwość korzystania ze środków umożliwiających automatyczne filtrowanie i rozpoznawanie treści, w tym opartych na AI, bez negatywnych konsekwencji dla dostawcy usługi, należy ocenić pozytywnie¹⁹⁹. Z poglądem tym nie można jednak się zgodzić. Zaaprobowanie konstrukcji dobrego samarytanina jest bowiem – jak się wydaje – przejawem determinizmu technologicznego polegającego na poszukiwaniu i aprobowaniu rozwiązań prawnych przede wszystkim dlatego, że odpowiadają one aktualnemu stanowi rozwoju techniki.

¹⁹⁸ X. Konarski, *Unijny Akt...*, s. 33.

¹⁹⁹ G. Bar, R. Skibicki, *Wyzwania prawne...*, s. 41.

Zmiany tej nie można jednak ocenić pozytywnie wówczas, gdy analizie poddane zostaną skutki zastosowania tej instytucji dla sfery praw podstawowych, w szczególności na płaszczyźnie realizacji wolności wypowiedzi.

Narzędzia wykrywcze dostawcy usług mogą uruchamiać nie tylko w celu uzyskania „faktycznej wiedzy” lub „wiarygodnej wiadomości” o treściach nielegalnych, ale także w celu ustalenia, czy odbiorca usługi nie narusza określonych przez pośrednika „warunków korzystania z usług”.

Zaakceptowanie przez odbiorcę „warunków korzystania z usług” w postaci regulaminu lub wzorca umownego oznacza wyrażenie przez odbiorcę usługi zgody na stosowanie przez dostawcę wskazanych w regulaminie środków kontroli, a także metod ich egzekucji oraz ewentualnych sankcji nakładanych na podmiot, który narusza te warunki. Zgodnie z art. 14 ust. 1 AUC w warunkach korzystania z usług dostawcy usług pośrednich uwzględniają informacje na temat wszelkich ograniczeń, które nakładają w związku z korzystaniem z ich usług, w odniesieniu do informacji przekazywanych przez odbiorców usługi. Informacje te muszą zawierać dane na temat wszelkich polityk, procedur, środków i narzędzi wykorzystywanych na potrzeby moderowania treści, w tym na temat algorytmicznego podejmowania decyzji i przeglądu dokonywanego przez człowieka, a także na temat regulaminu wewnętrznego systemu rozpatrywania skarg. Informacje te formułuje się jasno i w sposób prosty, zrozumiały, przyjazny dla użytkownika i jednoznaczny oraz podaje do wiadomości publicznej w łatwo dostępnym i nadającym się do odczytu maszynowego formacie.

Wskazane w art. 14 ust. 1 AUC obowiązki mają na celu zapewnienie „bezpiecznego, przewidywalnego, budzącego zaufanie środowiska internetowego” (motyw 9). Ich zakres dowodzi jednak intensywności i poziomu ryzyka naruszenia praw podstawowych w tym wolności wypowiedzi przez dostawców usług cyfrowych. Wskazane w AUC rodzaje obowiązków – paradoksalnie – legalizują ingerencje w wolność wypowiedzi jednostek. Skoro bowiem na pośredniku ciąży w myśl art. 14 ust. 1 obowiązek dokonywania przez człowieka przeglądu algorytmicznych metod podejmowania decyzji, to stanowi to zarazem zalegalizowanie takich metod, których skutkiem jest zautomatyzowane ingerowanie w wolność wypowiedzi poprzez blokowanie treści, ograniczanie dostępu lub zawieszanie świadczenia usługi.

Ryzyko naruszenia praw podstawowych jest tym większe, im większą liczbę użytkowników internetu obejmują świadczone przez pośredników usługi. Stąd też w sekcji 5 III rozdziału AUC wskazane zostały obowiązki adresowane wyłącznie do bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych, które mają średnią liczbę miesięcznie aktywnych odbiorców usługi w Unii wynoszącą co najmniej 45 mln, i które zostały wskazane jako bardzo duże platformy internetowe lub bardzo duże wyszukiwarki internetowe.

Zakres faktycznie realizowanej wolności wypowiedzi w sferze realnej (poza internetem) może się różnić od zakresu wolności wypowiedzi, z której korzystają użytkownicy internetu. Wbrew oczekiwaniom i przeświadczeniu użytkowników internetu, zakres swobody wypowiedzi online jest bardziej ograniczony niż w sferze realnej, co wynika z wykreowanego w tej przestrzeni standardu wolności wypowiedzi. Ograniczenia wolności wypowiedzi w internecie obejmują zarówno ten jej wymiar, który wiąże się z pozyskiwaniem informacji (profilowanie), jak też odnoszą się do aktywności polegającej na udostępnianiu (rozpowszechnianiu) treści i polegają – w znaczeniu faktycznym – na filtrowaniu treści przed ich publicznym udostępnieniem, a w przypadku podejrzenia niezgodności treści z warunkami świadczenia usług cyfrowych albo niezgodności z prawem (treści nielegalne) – ograniczaniu, blokowaniu lub usuwaniu treści.

W motywie 153 AUC zapewniono, że „rozporządzenie nie narusza praw podstawowych uznanych w Karcie praw podstawowych ani praw podstawowych stanowiących ogólne zasady prawa Unii. W związku z tym niniejsze rozporządzenie powinno być interpretowane i stosowane zgodnie z tymi prawami podstawowymi, w tym dotyczącymi wolności wypowiedzi i informacji oraz wolności i pluralizmu mediów. Wykonując uprawnienia określone w niniejszym rozporządzeniu, wszystkie zaangażowane organy publiczne powinny dążyć – w sytuacjach, w których występuje konflikt odpowiednich praw podstawowych – do osiągnięcia właściwej równowagi między danymi prawami zgodnie z zasadą proporcjonalności”.

Formalne zapewnienie o nienaruszalności praw podstawowych jest – w odniesieniu do wolności wypowiedzi – trudne do realizacji, o ile w ogóle możliwe. Standard wolności w przestrzeni internetowej jest bowiem konstruowany przez podmioty wyposażone w realne władztwo sprawowane nad

widocznością treści i dostępnością usług. Specyfika usług świadczonych przez pośredników internetowych uzasadnia odmienne ich podejście do wolności wypowiedzi i zakresu jej realizacji, a w konsekwencji wymaga zastosowania odmiennych mechanizmów kontroli.

Jeśli zatem w AUC i ARC prawodawca europejski potwierdza nienaruszalność standardu wypracowanego na gruncie art. 11 KPP i art. 10 EKPC, to pojawia się pytanie o to, komu prawodawca europejski powierzył wykonanie trójelementowego testu szkodliwości, o ile w ogóle stosowanie testu szkodliwości znajduje w sferze internetu rację bytu. W motywie 3 AUC wskazano na wymóg należytej staranności jako gwarancję przestrzegania praw podstawowych. W żadnym z postanowień AUC nie nałożono na pośredników obowiązku ustalania, czy ograniczenie wolności wypowiedzi internauty jest ustanowione w ustawie ani czy jest uzasadnione istnieniem pilnej potrzeby, ani tym bardziej pośrednicy nie mają obowiązku ustalać innej wartości, która w większym stopniu w danych okolicznościach faktycznych zasługuje na ochronę. Nie adresuje się także do pośredników obowiązków dotyczących ważenia interesów i stosowania proporcjonalnych środków ingerencji. W miejsce tych kryteriów nałożono na pośredników obowiązek rozsądnego, niedyskryminującego i niearbitralnego działania (motywy 41, 52, 58, 61, art. 20 ust. 4) z zachowaniem wymogów należytej staranności.

Wskazano, że:

odpowiedzialne zachowanie i działanie z należytą starannością dostawców usług pośrednich ma zasadnicze znaczenie dla [...] umożliwienia obywatelom Unii i innym osobom korzystania z przysługujących im praw podstawowych zagwarantowanych w Karcie praw podstawowych Unii Europejskiej, w szczególności z wolności wypowiedzi i informacji (motyw 3).

Ochrona wolności wypowiedzi jest przy tym ujmowana w AUC w aspekcie negatywnym, tj. jako ciążący na pośrednikach internetowych obowiązek blokowania nielegalnych treści i niedopuszczania do dezinformacji. Jak wskazano w motywie 6 AUC, rozporządzenie w pełni harmonizuje przepisy mające zastosowanie do usług pośrednich w celu przeciwdziałania rozpowszechnianiu nielegalnych treści w internecie oraz zagrożeniom społecznym, jakie może

stwarzać rozpowszechnianie dezinformacji lub innych treści, stwarzając w ten sposób zagrożenie dla realizacji praw podstawowych. W motywie 51 potwierdzono dopuszczalność ingerencji w wolność wypowiedzi użytkowników internetowych i zalegalizowano usuwanie treści. Zgodnie z treścią tego przepisu:

wszelkie działania podejmowane przez dostawcę usług hostingu w związku z otrzymaniem zgłoszenia powinny być ściśle ukierunkowane, to znaczy powinny służyć usunięciu określonych informacji uznanych za nielegalne treści lub uniemożliwieniu dostępu do nich, jednak bez nadmiernego naruszania wolności wypowiedzi i informacji odbiorców usługi.

Przy dokonywaniu oceny „oczywiście nielegalnej treści”, która powinna podlegać zablokowaniu lub usunięciu, albo „oczywiście bezzasadnej skargi” proponuje się stosowanie wzorca przeciętnej wiedzy. W motywie 63 wskazano, że „informacje należy uważać za stanowiące oczywiście nielegalne treści, a zgłoszenia lub skargi należy uważać za oczywiście bezzasadne, jeżeli dla osoby nieposiadającej wiedzy fachowej jest oczywiste, bez przeprowadzenia jakiegokolwiek merytorycznej analizy, że treści są nielegalne, a zgłoszenia lub skargi – bezzasadne”. Na pośrednikach internetowych, w tym przede wszystkim dostawcach bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych, ciąży obowiązek „uwzględniania praw podstawowych” (motyw 49); „zapewnienia skutecznej ochrony praw podstawowych” (motyw 109); „uwzględniania potencjalnych negatywnych skutków dla praw podstawowych” (motyw 86); „poszanowania praw podstawowych” (motyw 79, 86); „ochrona praw podstawowych” (motyw 41). Zarazem uzasadnieniem zastosowania metody pełnej harmonizacji przepisów dotyczących pośredników internetowych jest – jak stwierdzono w motywie 155 – ustalenie, że państwa członkowskie nie są w stanie sprostać zadaniu budowania bezpiecznego internetu w sposób, który zapewniłby, że prawa podstawowe są odpowiednio chronione. W konsekwencji ze względu na zakres terytorialny i podmiotowy możliwe jest ich lepsze osiągnięcie na poziomie Unii, może ona podjąć działania zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej, a także zgodnie z zasadą proporcjonalności określoną w tym artykule, uznano, że rozporządzenie nie wykracza poza to, co niezbędne.

W efekcie zastosowanych w AUC rozwiązań powstał system, którego fundamentem uczyniono podmioty prywatne, wyposażając je w instrumenty bezpośredniego oddziaływania, w tym prewencyjnie (*ex ante*) na kształt i zakres wolności wypowiedzi oraz ustalając obszerny katalog przesłanek legitymizujących ingerencje w wolności wypowiedzi albo umożliwiających uchylenie się od odpowiedzialności za taką ingerencję. Wytworzony na gruncie AUC standard wolności wypowiedzi jest rezultatem zawartego między prawodawcą europejskim a przedsiębiorcami IT porozumienia, którego skutkiem jest stworzenie optymalnych dla strażników dostępu warunków rozwoju ich potencjału gospodarczego oraz uzyskanie przez KE kontroli nad przepływem informacji w środowisku internetowym i skuteczne zwalczanie nielegalnych treści.

IV. Mechanizmy i instrumenty ograniczania wolności wypowiedzi na rynku usług cyfrowych

1. Status dostawców usług społeczeństwa informacyjnego – zakresy wpływów

Zakres wpływu dostawców usług społeczeństwa informacyjnego kształtują trzy czynniki:

1. liczba odbiorców świadczonych przez nich usług;
2. rodzaj usług oraz
3. tryb i zasady ponoszenia odpowiedzialności prawnej¹.

Ostatni ze wskazanych czynników może zachęcać albo zniechęcać do prowadzenia działalności na jednolitym rynku cyfrowym. Skoro UE upatruje w rozwoju rynku usług cyfrowych podstawy rozwoju gospodarki europejskiej,

¹ O ile ocena zakresu wpływu miałaby dotyczyć innych sfer działalności, np. sfery gospodarczej, to parametry pomiaru mogą być inne. W sferze gospodarczej siłę, jaką platformy internetowe wywierają na swoich użytkowników, zarówno firmy, jak i konsumentów, można oceniać – po pierwsze – na podstawie wartości netto, jaką dla firm generuje korzystanie z platform, zapewniając im dostęp do rynków zbytu na ich produkty. Firmy zarazem mogą stać się zależne od platform, co może wystąpić w różnym zakresie i zmiennej intensywności. W rezultacie mogą zostać podatne na zmiany w polityce platform (co może np. wpłynąć na udział przychodów firmy, które pojawiają się za pośrednictwem kanałów platformy internetowej). Po drugie – moc platformy można ocenić pod względem jej popularności wśród konsumentów. Im większą popularność ma platforma, tym więcej firm przyciągnie. Po trzecie – strategia konkurencyjna przyjęta przez platformę internetową może określić jej pozycję i dominację na rynku (np. w wyniku fuzji i przejęć). Zob. *EU Observatory on the Online Platform Economy*, Komisja Europejska, <https://platformobservatory.eu/state-of-play/power-over-users/> (dostęp: 16.08.2023).

to w konsekwencji przyjęte w aktach normatywnych rozwiązania muszą sprzyjać rozwojowi tego rynku. Stopień ponoszonego przez przedsiębiorcę (dostawcę usług cyfrowych) ryzyka naruszenia prawa i poniesienia sankcji za to naruszenie w stosunku do nakładów i osiąganego zwrotu nie mogą być nieproporcjonalne i nie mogą zniechęcać do korzystania przez przedsiębiorców z narzędzi informatycznych, w przeciwnym razie rynek usług cyfrowych przestanie się rozwijać, a to – co do zasady – stoi w sprzeczności z celami UE². Zakres wpływu dostawców usług jest zatem wypadkową wskazanych powyżej trzech zmiennych, które zostały przez ustawodawcę europejskiego wykorzystane jako punkty odniesienia i kryteria regulacyjne.

Kryterium rodzaju usług pozwoliło na wyodrębnienie grup podmiotów, które ze względu na specyfikę świadczonych usług operują na wydzielonych, sektorowych rynkach, adresując usługi do wyselekcjonowanej grupy odbiorców. Dostawcy usług mogą zatem osiągać wysoką pozycję na rynku usług danego rodzaju jednakże, globalnie, ich wpływ na otoczenie społeczne jest odpowiednio proporcjonalny do liczby aktywnych użytkowników korzystających z tych usług. Ze względu na charakterystykę świadczonych usług mniejszy wpływ na rynek wewnętrzny wywierają będą dostawcy usług udostępniania treści online niż pośrednicy internetowi. Zarazem wśród pośredników internetowych większy wpływ mieć będą bardzo duże platformy internetowe i bardzo duże wyszukiwarki internetowe, co znajduje także odzwierciedlenie w postanowieniach AUC i ARC charakteryzujących te usługi. Jeśli zatem na katalog usług pośrednictwa internetowego składać się będą usługi: zwykłego przekazu, cachingu i hostingu, o tyle strażnicy dostępu, utrzymując status pośredników internetowych, świadczą tzw. podstawowe usługi platformowe, na które składają się:

² Komisja Europejska wyznaczyła cele i działania dotyczące transformacji cyfrowej planowane na lata 2020–2025 w dokumencie *Kształtowanie cyfrowej przyszłości Europy* (fr. *Façonner l'avenir numérique de l'Europe*). Na lata 2020–2025 KE wskazała trzy kluczowe cele dla przeprowadzenia transformacji cyfrowej z korzyścią dla obywateli i z poszanowaniem unijnych wartości: 1) Technologia, która służy ludziom; 2) Sprawiedliwa i konkurencyjna gospodarka; 3) Otwarte, demokratyczne i zrównoważone społeczeństwo, zob. *Façonner l'avenir numérique de l'Europe*, Komisja Europejska, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/shaping-europes-digital-future_fr (dostęp: 16.08.2023).

- a) usługi pośrednictwa internetowego,
- b) wyszukiwarki internetowe,
- c) internetowe serwisy społecznościowe,
- d) usługi platformy udostępniania wideo,
- e) usługi łączności interpersonalnej niewykorzystującej numerów,
- f) systemy operacyjne,
- g) usługi w chmurze,
- h) usługi reklamowe, w tym wszelkie sieci reklamowe.

Kryterium liczby odbiorców usług pozwoliło na wyodrębnienie w grupie pośredników internetowych tzw. strażników dostępu, tj. tych podmiotów, które co prawda świadczą usługi tego samego rodzaju (usługi pośrednictwa internetowego), jednakże ze względu na znaczący wpływ, jaki wywierają na rynek wewnętrzny, obarczone zostały zwiększonym zakresem obowiązków (art. 33–43 AUC oraz art. 5–6 ARC). Podmioty te podlegają zaostrzonym rygorom odpowiedzialności przede wszystkim o charakterze finansowym, a nadto zastosowano wobec nich pionową, scentralizowaną strukturę kontroli i nadzoru, gdzie w kompetencje kontrolne i nadzorcze wyposażona została Komisja Europejska jako organ wyłącznie uprawniony do przeprowadzania dochodzenia, egzekwowania i monitorowania działalności strażników dostępu w zakresie wykonywanych przez nich obowiązków (art. 18–33 ARC).

Kryterium odnoszące się do przesłanek ponoszenia odpowiedzialności, a przede wszystkim ustanowienie na rzecz dostawców usług pośrednictwa internetowego przesłanek uchylających ich odpowiedzialność, w tym pozwalających na uchylenie się od ewentualnych grzywien i kar okresowych, których nakładanie pozostaje w dyspozycji Komisji Europejskiej, stanowi zachętę dla rozwijania działalności w tych dziedzinach gospodarki cyfrowej, w których istnieją przejrzyste zasady dokonywania oceny prawnej prawidłowości świadczonej usługi. Przejrzystość przesłanek uchylających odpowiedzialność, a także samo ich zawarowanie w akcie ustawodawczym zwiększa atrakcyjność działalności. Okoliczność, że takie przesłanki zostały ustanowione na rzecz podmiotów świadczących usługi pośrednictwa internetowego nie tylko wpłynęło na rozwój tego sektora działalności, lecz także sprawiło, że działalność pośredników na rynku wewnętrznym uzyskała priorytetowe znaczenie dla gospodarki UE.

A. Pośrednicy internetowi – zmiana kontratypu

Działalność pośredników internetowych została wyłączona z zakresu regulacji objętej dyrektywą 2000/31 (dyrektywa o handlu elektronicznym) i stała się przedmiotem normowania w rozporządzeniach składających się na tzw. pakiet cyfrowy, tj. w akcie o usługach cyfrowych (AUC) i akcie o rynkach cyfrowych (ARC), przy czym zakres obowiązków i zasady odpowiedzialności dotyczące wszystkich pośredników internetowych bez względu na ich potencjał gospodarczy i liczbę odbiorców świadczonych przez nich usług zostały określone w pierwszym z nich, AUC. dopełnieniem tych regulacji jest akt o rynkach cyfrowych (ARC) zawierający normy adresowane do szczególnej kategorii dostawców usług pośrednich nazywanych w ARC „strażnikami dostępu”, wyróżnionych ze względu na to, że: a) wywierają znaczący wpływ na rynek wewnętrzny, a także b) świadczą podstawową usługę platformową będącą ważnym punktem dostępu, za pośrednictwem którego użytkownicy biznesowi docierają do użytkowników końcowych (art. 3 ust. 1 pkt a i b ARC).

W motywie 5 AUC wskazano, że akt o usługach cyfrowych „powinien mieć zastosowanie do dostawców tylko niektórych usług społeczeństwa informacyjnego, które wyodrębniono i scharakteryzowano jako usługi pośrednie. Zgodnie z art. 2 ust. 2 AUC rozporządzenie „nie ma zastosowania do usługi, która nie jest usługą pośrednią, ani do wymogów nakładanych w odniesieniu do takiej usługi, niezależnie od tego, czy taka usługa jest świadczona za pośrednictwem korzystania z usługi pośredniej”. W art. 2 ust. 3 AUC potwierdzono, że przepisy aktu o usługach cyfrowych pozostają jednak bez wpływu na stosowanie dyrektywy 2000/31 (dyrektywa o handlu elektronicznym), co oznacza, że pozostają w mocy te rozwiązania, które są adresowane do dostawców usług społeczeństwa informacyjnego³ innych niż pośrednicy. Zamysłem prawodawcy europejskiego było, jak wynika z motywu 4, stworzenie na poziomie UE zestawu jednolitych, skutecznych i proporcjonalnych, obowiązkowych zasad obowiązujących dostawców usług pośrednich w celu „położenia kresu fragmentacji rynku wewnętrznego”.

³ W niniejszej pracy terminy „dostawcy usług cyfrowych” i „dostawcy usług społeczeństwa informacyjnego” stosowane są zamiennie.

Pośrednicy internetowi stanowią grupę dostawców usług społeczeństwa informacyjnego, którzy operują na „rynku wewnętrznym usług pośrednich” (art. 1 ust. 1 AUC). Użyte w art. 1 ust. 1 AUC sformułowanie „rynek wewnętrzny usług pośrednich” sygnalizuje wagę i znaczenie, jakie ustawodawca europejski przypisuje usługom pośrednictwa internetowego. Przyjęto bowiem, że w obrębie rynku wewnętrznego funkcjonuje „rynek usług pośrednich”, a zatem istnieje liczna grupa podmiotów, których aktywność silnie oddziałuje na cały rynek wewnętrzny. Rynek wewnętrzny, zgodnie z art. 26 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE)⁴, obejmuje obszar bez granic wewnętrznych, w którym jest zapewniony swobodny przepływ towarów i usług oraz swoboda przedsiębiorczości, biorąc pod uwagę z natury transgraniczny charakter internetu, który jest powszechnie wykorzystywany w celu świadczenia tych usług. Rynek usług pośrednich per analogiam obejmować będzie obszar bez granic, na którym operują podmioty oferujące świadczenie usług pośrednich. Usługi pośrednie, zgodnie z art. 3 lit. g AUC, oznaczają jeden z następujących rodzajów usług społeczeństwa informacyjnego⁵:

1. usługę zwykłego przekazu („mere conduit”);
2. usługę cachingu lub
3. usługę hostingu.

Usługi pośrednie mogą być świadczone samodzielnie lub równolegle z innymi usługami cyfrowymi. To, czy dana usługa jest usługą „zwykłego przekazu”, „cachingu” czy „hostingu”, zależy wyłącznie od jej funkcji technicznych, które mogą ewoluować w czasie, i powinno być oceniane indywidualnie (motyw 29 AUC).

⁴ Traktat ustanawiający Europejską Wspólnotę Gospodarczą (Dz.U. z 2004 r. Nr 90, poz. 864/2 z późn. zm.).

⁵ Usługi pośrednictwa internetowego należą do szerszej kategorii usług społeczeństwa informacyjnego. Termin ten był przedmiotem analizy we wcześniejszych partiach pracy. Wypada jedynie przypomnieć, że opis tego terminu znalazł się w dyrektywie 2000/31, w szczególności w motywie 18, gdzie wskazano, że „Wykładni tego terminu TSUE dokonywał w szczególności w wyrokach: sprawa C-108/09, Ker-Optika, ECLI:EU:C:2010:725, sprawa C-291/13, Papasavvas, ECLI:EU:C:2014:2209, sprawa C-484/14, Tobias McFadden/Sony Music, ECLI:EU:C:2016:689; sprawa C-434/15, Asociación Profesional Élite Taxi, ECLI:EU:C:2017:981 lub sprawa C-390/18, Airbnb Ireland UC, ECLI:EU:C:2019:1112”.

Zważywszy, że – co do zasady – usługa społeczeństwa informacyjnego jest świadczona, jak wskazano w art. 1 pkt b dyrektywy 2015/1535⁶, „normalnie za wynagrodzeniem”, należy przyjąć, że świadczenie usług pośrednictwa internetowego odbywa się w ramach zorganizowanej działalności zarobkowej, wykonywanej przez pośrednika we własnym imieniu i w sposób ciągły, a zatem jest wykonywana w ramach działalności gospodarczej⁷. Pośrednikiem jest podmiot świadczący takie usługi, jak w szczególności: usługi wyszukiwarki internetowej, systemy operacyjne, internetowe serwisy społecznościowe, usługi platformy udostępniania wideo, usługi łączności interpersonalnej niewykorzystujące numerów, usługi przetwarzania w chmurze, wirtualni asystenci, przeglądarki internetowe i internetowe usługi reklamowe, w tym usługi pośrednictwa reklamowego. Usługi pośrednictwa internetowego mogą również występować w dziedzinie usług finansowych i mogą pośredniczyć w świadczeniu usług lub być wykorzystywane do świadczenia usług, których niewyczerpujący wykaz zawiera załącznik II do dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/1535⁸ (motyw 14 ARC).

M. Piech zauważa, że:

potoczne określenie pośredników jako pewnej kategorii usługodawców pośredniczących w dostępie do treści (podejście podmiotowe) odbiega od przyjętej w dyrektywie 2000/31 konstrukcji, zgodnie z którą nie można mówić o kategoriach usługodawców będących pośrednikami, ale raczej o usługach (podejście przedmiotowe), których charakter pozwala stwierdzić, że usługodawca, wykonując konkretną usługę, działa jako pośrednik⁹.

⁶ Dyrektywa w sprawie usług społeczeństwa informacyjnego.

⁷ Zgodnie z art. 3 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (t.j. Dz.U. z 2023 r., poz. 221 z późn. zm. – dalej: Prawo przedsiębiorców) wskazane powyżej elementy przesądzą o zakwalifikowaniu danej aktywności jako działalności gospodarczej. Przedsiębiorcą jest natomiast osoba fizyczna, osoba prawna lub jednostka organizacyjna niebędąca osobą prawną, której odrębna ustawa przyznaje zdolność prawną, wykonująca działalność gospodarczą (art. 4 ust. 1 Prawa przedsiębiorców).

⁸ W załączniku II wskazano usługi: inwestycyjne, ubezpieczenia i reasekuracji, bankowe, operacje dotyczące funduszy emerytalnych oraz usługi związane z obrotem transakcjami terminowymi i opcjami; (zob. dyrektywa w sprawie usług społeczeństwa informacyjnego).

⁹ M. Piech, *Zagadnienia...*, s. 33.

Blizsze potocznemu rozumieniu terminu „pośrednik internetowy” wydają się rozwiązania przyjęte na gruncie AUC i ARC. W rozporządzeniach cyfrowych przyjęto bowiem, że kategoryzowanie pośrednictwa internetowego powinno następować nie tylko ze względu na rodzaj świadczonej usługi, lecz także ze względu na potencjał podmiotów świadczących usługi pośrednictwa. W sekcji 5 AUC uregulowane zostały bowiem „dodatkowe obowiązki spoczywające na dostawcach bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych w zakresie zarządzania ryzykiem systemowym”.

Zdaniem W. Chomiczewskiego względem stanu prawnego obowiązującego przed przyjęciem i wejściem w życie rozwiązań zawartych w AUC i ARC nie pojawia się żadna modyfikacja odnośnie do zasad ponoszenia odpowiedzialności przez dostawców usług cyfrowych¹⁰. Konstatacja ta jest, jak się wydaje, wynikiem ustalenia, że pośrednicy internetowi, którzy stali się adresatami regulacji zawartych w AUC i ARC, stanowią podgrupę dostawców usług społeczeństwa informacyjnego, których status został uregulowany w dyrektywie o handlu elektronicznym, a zmiana polega *de facto* na zmianie metody regulacyjnej, tj. w miejsce zasady państwa pochodzenia¹¹ zastosowanie znalazła metoda pełnej harmonizacji¹².

Ze stanowiskiem tym nie można się zgodzić. O ile bowiem utrzymany został w AUC sposób definiowania pośredników internetowych, w szczególności poprzez wyodrębnienie trzech rodzajów świadczonych przez nich

¹⁰ W. Chomiczewski, *Zasady wyłączeń...* (cz. I), s. 19.

¹¹ P.P. Polański wskazuje, że zasada państwa pochodzenia zakłada, że „na państwie źródła usługi spoczywa obowiązek kontroli usługodawców mających siedzibę na jego terytorium a pozostałe państwa nie mogą, co do zasady, ingerować w ten proces”; (zob. P.P. Polański, *Europejskie prawo...*, s. 124).

¹² Zgodnie z motywem 9 AUC: „Niniejsze rozporządzenie w pełni harmonizuje przepisy mające zastosowanie do usług pośrednich na rynku wewnętrznym w celu zapewnienia bezpiecznego, przewidywalnego i budzącego zaufanie środowiska internetowego, przeciwdziałania rozpowszechnianiu nielegalnych treści w internecie oraz zagrożeniom społecznym, jakie może stwarzać rozpowszechnianie dezinformacji lub innych treści, w którym to środowisku prawa podstawowe zapisane w Karcie są skutecznie chronione, a innowacje są wspierane. Państwa członkowskie nie powinny przyjmować lub utrzymywać w mocy dodatkowych wymogów krajowych w odniesieniu do spraw objętych zakresem niniejszego rozporządzenia, ponieważ miałyby to wpływ na bezpośrednie i jednolite stosowanie w pełni zharmonizowanych przepisów mających zastosowanie do dostawców usług pośrednich zgodnie z celami niniejszego rozporządzenia”.

usług (zwykły przekaz, caching, hosting), to jednak, po pierwsze, uznano, że systematyzacja dokonywana wg rodzaju świadczonych usług jest niewystarczająca, a efektywność regulacyjną zapewni dopiero wyodrębnienie grupy pośredników (strażnicy dostępu) oddziałujących silniej niż pozostali na kształt rynku wewnętrznego, a po wtóre złagodzone, a nawet – jak się wydaje – zastąpiono wymóg neutralności, którego spełnienia oczekiwano od pośredników na gruncie dyrektywy o handlu elektronicznym, wymogiem należytej staranności, którego dopełnienie przez pośredników warunkuje dopuszczalność uchylenia się przez nich od odpowiedzialności.

W dyrektywie 2000/31 (o handlu elektronicznym) zasady wyłączania odpowiedzialności pośredników internetowych wskazano w art. 12–15. Regulacje te zostały zastąpione postanowieniami zawartymi w art. 4–6 AUC. W dyrektywie o handlu elektronicznym, podobnie jak ma to miejsce w rozporządzeniu – akt o usługach cyfrowych, stwierdzono, że akty te harmonizują przesłanki wyłączenia odpowiedzialności dostawców usług pośrednich niezależnie od dziedziny prawa, z której odpowiedzialność mogłaby wynikać¹³. W podobny sposób został także w AUC zbudowany system odpowiedzialności pośredników internetowych, który przewiduje odpowiedzialność kaskadową dostawcy internetu, dostawcy usług transmisji, dostawcy usługi cachingu oraz host providera. Pośrednicy internetowi mogą, kolejno, począwszy od dostawcy usługi transmisji danych (zwykły przekaz), poprzez dostawcę usługi cachingu, a następnie host providera, uchylać się od odpowiedzialności, przenosząc jej ciężar na kolejny podmiot. System odpowiedzialności kaskadowej prowadzi do ustalenia odpowiedzialności jednego tylko podmiotu, przy czym zazwyczaj nie jest nim żaden z pośredników. W konsekwencji odpowiedzialność za naruszenie prawa spowodowane treścią lub formą materiału rozpowszechnionego w internecie ponosi odbiorca usługi, tj. osoba, która umieściła treść w internecie.

Zgodnie z art. 3 ust. 1 AUC dostawca usługi zwykłego przekazu (usługa mere conduit) nie ponosi odpowiedzialności za przekazywane informacje, jeżeli:

1. nie jest inicjatorem transmisji,
2. nie wybiera odbiorcy transmisji,
3. nie wybiera ani nie modyfikuje informacji zawartych w transmisji.

¹³ Motyw 16 AUC.

Podmiot świadczący usługę cachingu nie poniesie natomiast odpowiedzialności, jeśli łącznie wykaze, że:

1. nie modyfikuje informacji,
2. przestrzega warunków dostępu do informacji,
3. przestrzega zasad dotyczących aktualizowania informacji, określonych w sposób szeroko uznany i stosowany w branży,
4. nie zakłóca zgodnego z prawem posługiwania się technologią szeroko uznaną i stosowaną w branży w celu uzyskania danych o korzystaniu z informacji oraz
5. podejmuje bezzwłocznie odpowiednie działania w celu usunięcia przechowywanych informacji lub uniemożliwienia dostępu do nich, gdy uzyska faktyczną wiedzę, że informacje zostały usunięte z początkowego źródła transmisji lub dostęp do nich został uniemożliwiony, albo gdy organy sądowe lub administracyjne nakazały usunięcie informacji lub uniemożliwienie dostępu do niej.

W przypadku świadczenia usługi społeczeństwa informacyjnego polegającej na przechowywaniu informacji przekazanych przez odbiorcę usługi (hosting) dostawca usług nie ponosi odpowiedzialności za informacje przechowywane na wniosek odbiorcy usługi pod warunkiem, że dostawca: 1) nie ma faktycznej wiedzy o nielegalnej działalności lub nielegalnych treściach, a w odniesieniu do roszczeń odszkodowawczych – nie wie o stanie faktycznym lub okolicznościach, które w sposób oczywisty świadczą o nielegalnej działalności lub nielegalnych treściach – lub 2) podejmuje bezzwłocznie odpowiednie działania w celu usunięcia lub uniemożliwienia dostępu do nielegalnych treści, gdy uzyska taką wiedzę lub wiadomość. Zasady wyłączenia odpowiedzialności dotyczące usług hostingu są stosowane również do operatora wyszukiwarki internetowej¹⁴.

Zasady te – w ujęciu formalnym – nie różnią się od przewidzianych w art. 12–15 dyrektywy o handlu elektronicznym¹⁵. Jednakże, na gruncie

¹⁴ Wyrok TS w sprawach połączonych Google France i Google. Zwraca się uwagę, że pomimo znaczenia, jakie przesądzenie tej kwestii ma dla funkcjonowania internetu, ani w AUC, ani w innym akcie prawnym nie postanowiono wyraźnie o zaliczeniu usługi wyszukiwarki internetowej do usług hostingu; zob. W. Chomiczewski, *Zasady wyłączeń...* (cz. I), s. 19.

¹⁵ Jednakże, jak zauważa W. Chomiczewski, wejście w życie aktu o usługach cyfrowych może mieć znaczenie dla rozwiązań krajowych, przesądzając ostatecznie o rodzaju

dyrektywy 2000/31, cechą relewantną usług pośrednictwa internetowego była neutralność pośrednika wobec treści transmitowanych lub przechowywanych na żądanie odbiorcy usługi. Pośrednik „musi [...] bowiem pozwolić na odróżnienie jego działalności – umożliwiania udostępniania treści innym podmiotom – od usług polegających na udostępnianiu własnych treści”¹⁶.

Dowodząc neutralności świadczenia usług, pośrednik winien był wykazać, że nie ingeruje w treść komunikatów ani nie dokonuje ich oceny, w szczególności nie analizuje zgodności ich treści ze stanem rzeczywistym, ani nie ustala ich zgodności z prawem lub warunkami umowy zawartej pomiędzy komunikującymi się stronami¹⁷. W AUC zasada nieingerowania w treść (zasada neutralności) została formalnie utrzymana, lecz – równolegle – oczekuje się od pośredników internetowych dochowania należytej staranności. Na gruncie AUC, inaczej niż miało to miejsce w dyrektywie 2000/31, neutralność pośrednika nie przesądza o dopuszczalności uchylenia się przez niego od odpowiedzialności prawnej. Będzie on bowiem musiał także dowieść, że dochował

i zakresie stosowania przesłanek wyłączenia odpowiedzialności pośredników internetowych. Autor ten spostrzega, że wadliwa implementacja dyrektywy o handlu elektronicznym do krajowego porządku prawnego spowodowała, że przesłanki wyłączenia odpowiedzialności host providera wymienione w art. 14 usude były interpretowane rozszerzająco, co mogło skutkować uchylaniem się host providera od odpowiedzialności, wbrew treści przepisów zawartych w dyrektywie. W ocenie W. Chomiczewskiego rozwiązanie zaproponowane w rozporządzeniu AUC, które nie wymaga implementacji, ponieważ zawarte w nim rozwiązania będą bezpośrednio stosowane w porządku krajowym, wywoła potrzebę stosowania przez pośredników internetowych w Polsce bardziej rygorystycznych środków, w tym moderowania treści, by móc skorzystać z wyłączenia odpowiedzialności prawnej. Alternatywnie, w pewnych sytuacjach możliwość prowadzenia dyskusji będzie wyłączana lub ograniczana przez samych dostawców usług pośrednich, by minimalizować ryzyko swojej odpowiedzialności; zob. W. Chomiczewski, *Zasady wyłączeń... (cz. I)*, s. 23.

¹⁶ M. Piech, *Usługodawcy przechowujący i udostępniający treści użytkowników jako pośrednicy*, [w:] *Pośrednicy internetowi...*

¹⁷ Jak stwierdził TSUE, usługę pośrednictwa internetowego stanowi np. usługa polegająca na umożliwieniu nawiązania – za pomocą aplikacji na smartfony, za wynagrodzeniem – kontaktów między osobami chcącymi przebyć trasę miejską a kierowcami taksówek posiadającymi zezwolenie, w przypadku której świadczący ową usługę zawarł w tym celu umowy o świadczenie usług z kierowcami w zamian za zapłatę miesięcznego abonamentu, ale nie przekazuje im zamówień, nie określa ceny za kurs ani nie zapewnia jej poboru od zainteresowanych osób, które uiszczają ją bezpośrednio u kierowcy taksówki, a ponadto nie sprawuje kontroli nad jakością pojazdów i ich kierowców ani nad ich zachowaniem. Zob. Wyrok TS z dnia 3 grudnia 2020 r w sprawie Star Taxi App SRL przeciwko Unitatea Administrativ Teritorială Municipiul București prin Primar General i Consiliul General al Municipiului București, C-62/19, LEX nr 3087736.

należytej staranności, wykonując usługi pośrednictwa internetowego. Dopełnienie wymogu należytej staranności upoważnia pośrednika do zastosowania środków organizacyjnych lub technicznych jak w szczególności monitorowania i filtrowania treści przed ich publicznym udostępnieniem motywowanych celem, jakim jest zapobieżenie naruszeniom prawa, w tym rozpowszechnianiu nielegalnych treści. Wobec formalnie utrzymanego w art. 4–6 wymogu neutralności jako przesłanki uchylenia się pośredników od odpowiedzialności prawnej konieczne stało się określenie relacji, w jakiej obowiązek neutralności pozostaje z wymogiem należytej staranności. Dla uchylenia wątpliwości odnośnie do tego, czy stosowanie przez pośredników technik, w tym także zautomatyzowanej analizy treści i danych, nie stoi w sprzeczności z zasadą neutralności, ustawodawca europejski kreuje w art. 7 AUC instytucję dobrego samarytanina. W art. 7 AUC zastrzeżono, że dostawców usług pośrednich nie można uznać za nieuprawnionych do skorzystania z wyłączeń odpowiedzialności tylko z tego powodu, że w dobrej wierze i z należytą starannością prowadzą z własnej inicjatywy dobrowolne czynności sprawdzające lub podejmują inne środki mające na celu wykrycie, identyfikację i usunięcie nielegalnych treści lub uniemożliwienie do nich dostępu lub podejmują niezbędne środki, aby spełnić wymogi prawa Unii i prawa krajowego zgodnego z prawem Unii, w tym wymogi określone w niniejszym rozporządzeniu.

Jeśli zatem ustawodawca europejski stawia pośrednikom wymóg dochowania należytej staranności, to jednak ani nie formułuje obowiązków szczegółowych, które pośrednik musiałby spełnić, by wykazać dopełnienie tego obowiązku, ani nie uzależnia pociągnięcia dostawcy usług do odpowiedzialności od wykazania, że ten rzeczywiście dochował wymaganego poziomu staranności. O dopuszczalności pociągnięcia pośredników internetowych do odpowiedzialności prawnej decyduje zatem nie tyle naruszenie jakiegoś obowiązku pozytywnego, lecz wykazanie przez dostawcę, że w okolicznościach danej sytuacji spornej zaistniały – kumulatywnie – przesłanki przewidziane w art. 4–6 AUC, odmiennie uregulowane dla każdego z pośredników.

Zarazem – jak zauważa M. Piech – nie zostały wskazane zasady ponoszenia odpowiedzialności pośredników internetowych za naruszenia prawa¹⁸.

¹⁸ M. Piech, *Wyłączenie odpowiedzialności dostawców usług pośrednich na gruncie Aktu o Usługach Cyfrowych. Analiza na tle dyrektywy 2000/31*, „Prawo Nowych Technologii” 2002, nr 3.

Ani w dyrektywie o handlu elektronicznym, ani w rozporządzeniach cyfrowych nie wskazano podstawy ponoszenia odpowiedzialności pośredników internetowych¹⁹. Ustawodawca europejski nie nakłada zatem na pośredników obowiązków, których niespełnienie powodowałoby automatyzm co do oceny bezprawności ich działania. W literaturze wskazuje się, że pytanie o odpowiedzialność za szkody spowodowane decyzjami dotyczącymi moderowania treści, usuwania i blokowania treści, a także stosowania systemów rekomendacji, pozostaje otwarte. AUC nie przewiduje żadnych sankcji za naruszenia wolności wypowiedzi przez pośredników, w szczególności stosujących zautomatyzowane systemy przetwarzania danych, w tym wykorzystujące sztuczną inteligencję. Wskazuje się, że w zakresie, w jakim do wadliwych decyzji zastosowanie znajdzie RODO, użytkownik będzie mógł skorzystać z regulacji art. 79 i 82 tego aktu. Natomiast w innych przypadkach zastosowanie będą mogły znaleźć tylko przepisy krajowe prawa cywilnego o odpowiedzialności kontraktowej lub deliktowej, w zależności od stanu faktycznego²⁰.

Mając na uwadze, że w dyrektywie 2000/31 zarówno ze względu na przyjętą metodę regulacji (zasada państwa pochodzenia²¹), jak i z uwagi na charakter

¹⁹ Zakres odpowiedzialności pośredników internetowych TSUE ustalał w szczególności w wyrokach: w sprawach połączonych Google France i Google; w sprawie L'Oréal przeciwko eBay; w sprawie Scarlet Extended przeciwko SABAM; z dnia 16 lutego 2012 r. w sprawie Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) przeciwko Netlog NV, C-360/10 (dalej: Wyrok TS w sprawie SABAM przeciwko Netlog); z dnia 27 marca 2014 r. w sprawie UPC Telekabel Wien GmbH przeciwko Constantin Film Verleih GmbH i Wega Filmproduktionsgesellschaft mbH, C-314/12 (dalej: Wyrok TS w sprawie UPC Telekabel Wien); w sprawie Tobias Mc Fadden przeciwko Sony Music Entertainment Germany GmbH lub z dnia 3 października 2019 r. w sprawie Eva Glawischnig-Piesczek przeciwko Facebook Ireland Limited, C-18/18.

²⁰ G. Bar, R. Skibicki, *Wyzwania prawne...*, s. 43.

²¹ Zgodnie z zasadą państwa pochodzenia, wynikającą z treści art. 3 ust. 2 dyrektywy 2000/31, państwa członkowskie co do zasady nie mogą ograniczać swobodnego przepływu usług społeczeństwa informacyjnego pochodzących z innego państwa członkowskiego. Państwo członkowskie inne niż państwo pochodzenia może bowiem dokonać odstępstwa od tej zasady wyłącznie poprzez podjęcie środków „w odniesieniu do określonej usługi społeczeństwa informacyjnego”, spełniających przesłanki określone w art. 3 ust. 4 lit. a) i b) tej dyrektywy; zob. *Opinia Rzecznika Generalnego z dnia 8 czerwca 2023 r. Sprawa C-376/22 Google Ireland Limited, Meta Platforms Ireland Limited, Tik Tok Technology Limited przeciwko Kommunikationsbehörde Austria (Komm Austria)*, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=274435&pageIndex=o&doclang=PL&mode=req&dir=&occ=first&part=1&cid=370422> (dostęp: 12.01.2024). Zakres obowiązkowej harmonizacji przepisów krajowych normujących świadczenia

instrumentu regulacyjnego (dyrektywa) nie mogła ona zawierać obowiązków (norm), których bezpośrednim adresatem byłiby pośrednicy internetowi, adresatem zawartych w dyrektywie o handlu elektronicznym postulatów były państwa członkowskie. W rozporządzeniach cyfrowych (AUC i ARC) ustawodawca europejski nakłada obowiązki bezpośrednio na podmioty świadczące usługi pośrednictwa internetowego. Obowiązki te zostały wskazane w art. 9–42, przy czym część z nich dotyczy wszystkich pośredników, niezależnie od potencjału, jakim dysponują (art. 9–32), a pozostałe (art. 33–42) przewidują dodatkowe obowiązki spoczywające na dostawcach bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych. AUC nie zawiera jednak przesłanek, które umożliwiałyby dokonywanie oceny zaistnienia albo braku istnienia naruszenia przez dostawców ciążących na nich obowiązków, co utrudnia ewentualne ustalenie związku przyczynowo-skutkowego pomiędzy czynnościami dostawcy usług pośrednich a skutkami jego działania lub zaniechania w sferze praw osobistych i majątkowych odbiorcy usługi.

B. Dostawcy usług udostępniania treści online

„Dostawca usług udostępniania treści online” oznacza dostawcę usług społeczeństwa informacyjnego²², którego głównym lub jednym z głównych celów jest przechowywanie i udzielanie publicznego dostępu do dużej liczby chronionych prawem autorskim utworów lub innych przedmiotów objętych ochroną zamieszczanych przez użytkowników tych usług, które są przez niego organizowane i promowane w celach zarobkowych. Dostawców takich

usług społeczeństwa informacyjnego został wskazany, w szczególności, w motywie 21 dyrektywy 2000/31, wskazując, że „[...] dziedzina podlegająca koordynacji obejmuje tylko wymagania odnoszące się do działalności w trybie on-line, takie jak informacja on-line, reklama on-line, zakupy on-line, zawieranie umów on-line; nie dotyczy wymagań prawnych państw członkowskich odnoszących się do towarów, takich jak normy bezpieczeństwa, obowiązków etykietowania lub odpowiedzialności za towary ani wymagań państw członkowskich odnoszących się do dostawy lub do transportu towarów, łącznie z dystrybucją produktów leczniczych [...]” (tamże).

²² Pojęcie dostawcy usług społeczeństwa informacyjnego rozumie się jednolicie na gruncie wszystkich aktów prawnych UE regulujących świadczenie usług drogą elektroniczną. Także w dyrektywie 2019/790, podobnie jak w AUC i ARC, następuje w art. 2 pkt 5 odesłanie do art. 1 ust. 1 lit. b) dyrektywy (UE) 2015/1535.

usług, jak nienastawione na zysk encyklopedie internetowe, nienastawione na zysk repozytoria naukowe i edukacyjne, platformy tworzenia otwartego oprogramowania i platformy wymiany otwartego oprogramowania, oraz dostawców usług łączności elektronicznej zdefiniowanych w dyrektywie (UE) 2018/1972²³, internetowych platform handlowych, usług w chmurze dla przedsiębiorstw i usług w chmurze obliczeniowej, które umożliwiają użytkownikom zamieszczanie treści na własny użytek, nie uznaje się za dostawców usług udostępniania treści online w rozumieniu dyrektywy²⁴.

Dostawcy usług udostępniania treści online dokonują czynności publicznego udostępniania lub podawania do publicznej wiadomości utworu, gdy udzielają publicznego dostępu do chronionych prawem autorskim utworów lub innych przedmiotów objętych ochroną zamieszczanych przez użytkowników. W związku z tym na gruncie dyrektywy 2019/790²⁵ przyjęto, że dostawcy usług udostępniania treści online powinni uzyskać zezwolenie, w tym poprzez zawarcie umowy licencyjnej, od odpowiednich podmiotów uprawnionych (motyw 64). Biorąc pod uwagę fakt, że dostawcy usług udostępniania treści online udzielają dostępu do treści, których sami nie zamieszczają, lecz które są zamieszczane przez ich użytkowników, do celów dyrektywy 2019/790 przyjęto, że należy przewidzieć odrębny mechanizm odpowiedzialności w przypadkach, gdy nie udzielono zezwolenia. Nie powinno to naruszać środków prawnych przewidzianych w prawie krajowym w przypadkach innych niż odpowiedzialność za naruszenia prawa autorskiego ani możliwości wydawania nakazów przez sądy krajowe lub organy administracji zgodnie z prawem Unii. W konsekwencji dopuszczalne jest zastosowanie wobec dostawcy treści online nakazów sądowych, podobnie jak jest to możliwe w odniesieniu do pośredników internetowych na gruncie art. 4–6 AUC.

²³ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (wersja przekształcona) (Dz.U. UE L Nr 321, s. 36 z późn. zm.).

²⁴ Art. 2 pkt 6 dyrektywy DSM.

²⁵ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790 z dnia 17 kwietnia 2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE (Dz.U. UE L Nr 130, s. 92), <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32019L0790> (dostęp: 10.10.2023) – dalej: dyrektywa DSM (ang. *Digital Single Market*) lub dyrektywa 2019/790.

Aktualny pozostaje pogląd wypowiedziany na gruncie art. 8 ust. 3 dyrektywy 2001/29²⁶ w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym, zgodnie z którym „w istocie dostawca dostępu do Internetu, który umożliwia swoim klientom dostęp do przedmiotów objętych ochroną publicznie udostępnionych w Internecie przez osoby trzecie, jest pośrednikiem, którego usługi są wykorzystywane w celu naruszenia praw autorskich lub pokrewnych”²⁷. W myśl tego przepisu państwa członkowskie zapewnią, aby podmioty praw autorskich mogły wnioskować o wydanie nakazu przeciwko pośrednikom, których usługi są wykorzystywane przez stronę trzecią w celu naruszenia praw autorskich lub pokrewnych. W wyroku z dnia 22 czerwca 2021 r. TSUE stwierdził, że podmiot praw autorskich może na podstawie prawa krajowego uzyskać nakaz sądowy przeciwko pośrednikowi, którego usługi zostały wykorzystane przez osobę trzecią do naruszenia przysługujących mu praw bez wiedzy owego pośrednika dopiero wówczas, gdy przed wszczęciem postępowania sądowego ów pośrednik został powiadomiony o tym naruszeniu i nie podjął niezwłocznie działań, aby usunąć dane treści lub zablokować do nich dostęp i zapewnić, by takie naruszenia nie powtarzały się. Do sądów krajowych należy jednakże zapewnienie, aby stosowanie takiego warunku nie powodowało opóźnień rzeczywistego zaprzestania naruszenia w sposób powodujący nieproporcjonalną szkodę dla tego podmiotu²⁸. Zarazem jednak przepisy dyrektywy 2000/31 w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywę o handlu elektronicznym) należy interpretować w ten sposób, że nie ma ona zastosowania w dziedzinie ochrony poufności porozumiewania się i osób fizycznych w związku z przetwarzaniem danych osobowych w ramach usług społeczeństwa informacyjnego, ponieważ ochrona ta jest w zależności od przypadku regulowana przez dyrektywę 2002/58 o prywatności i łączności elektronicznej, zmienioną dyrektywą 2009/136, lub przez rozporządzenie 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem

²⁶ Dyrektywa 2001/29/WE Parlamentu Europejskiego i Rady z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym (Dz.U. UE L Nr 167, s. 10 z późn. zm.).

²⁷ Wyrok TS w sprawie UPC Telekabel Wien, poz. I-192.

²⁸ Wyrok TS w sprawie Frank Peterson przeciwko Google.

danych osobowych i w sprawie swobodnego przepływu takich danych. Art. 23 ust. 1 rozporządzenia 2016/679 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 Karty praw podstawowych należy interpretować w ten sposób, że stoi on na przeszkodzie przepisom krajowym nakładającym na dostawców dostępu do usług internetowej komunikacji publicznej i na dostawców usług hostingowych obowiązek uogólnionego i niezróżnicowanego zatrzymywania między innymi danych osobowych dotyczących tych usług²⁹. Uzupełnienie tego stanowiska stanowi wyrok Trybunału w sprawie L'Oréal SA i in. przeciwko eBay International AG i in.³⁰ Trybunał w tym wyroku stwierdził, że operator rynku elektronicznego online, nawet jeśli nie odgrywa czynnej roli w przechowywaniu lub udostępnianiu treści, a jego przedmiotem działalności jest świadczenie usług objętych zakresem stosowania wyłączenia odpowiedzialności pośredników internetowych³¹, w okolicznościach sprawy, która może zakończyć się zasądzeniem odszkodowania, nie może powołać się na zwolnienie z odpowiedzialności przewidziane w tym przepisie, jeżeli wiedział o stanie faktycznym lub okolicznościach, na podstawie których przedsiębiorca wykazujący należyłą staranność powinien stwierdzić bezprawność danych ofert sprzedaży, i w przypadku posiadania takiej wiedzy nie podjął niezwłocznie działań polegających na zablokowaniu dostępu do treści.

Status dostawcy udostępniania treści online jest determinowany rodzajem i charakterem świadczonej usługi. Usługi objęte dyrektywą 2019/790 są usługami, których głównym lub jednym z głównych celów jest przechowywanie i umożliwianie użytkownikom zamieszczania i udostępniania dużej ilości treści chronionych prawem autorskim w celach zarobkowych, bezpośrednio lub pośrednio, dzięki ich organizacji i promowaniu w celu przyciągnięcia większej liczby odbiorców, w tym poprzez ich klasyfikację i wykorzystywanie ukierunkowanych działań promocyjnych w ramach tych usług. Usługi te nie powinny obejmować usług, których głównym celem nie

²⁹ Wyrok TS z dnia 6 października 2020 r. w sprawie La Quadrature du Net i in. przeciwko Premier ministre i in., C-511/18, LEX nr 3095381, <https://sip.lex.pl/#/jurisprudence/523189077/1/c-511-18-udostepnianie-danych-przez-dostawcow-uslug-telekomunikacyjnych-la-quadrature-du-net-i-in..?cm=RELATIONS> (dostęp: 2.10.2023).

³⁰ Wyrok TS w sprawie L'Oréal przeciwko eBay, pkt 124.

³¹ W ówczesnym stanie prawnym chodziło o art. 14 ust. 1 dyrektywy 2000/31, którego odpowiednikiem jest obecnie art. 4 AUC.

jest umożliwianie użytkownikom zamieszczania i udostępniania dużej ilości treści chronionych prawem autorskim w celach zarobkowych (motyw 62 dyrektywy 2019/790). Ocena tego, czy dostawca usług udostępniania treści online przechowuje i udziela dostępu do dużej ilości treści chronionych prawem autorskim, powinna być dokonywana indywidualnie dla każdego przypadku i powinna uwzględniać połączenie elementów takich jak odbiorcy usługi oraz liczba plików zawierających treści chronione prawem autorskim zamieszczanych przez użytkowników usługi (motyw 63).

Dostawca usług udostępniania treści online ma status zbliżony do pośrednika internetowego. Podobnie jak pośrednicy, nie ma on – co do zasady – obowiązku monitorowania treści i nadzoru, niemniej ciąży na nim obowiązek dochowania należytej staranności. Obowiązki ustanowione w dyrektywie 2019/790 nie powinny zatem, jak postanowiono w art. 2 ust. 8, prowadzić do nakładania przez państwa członkowskie ogólnego obowiązku w zakresie nadzoru, jednakże przy dokonywaniu oceny, czy dostawca usług udostępniania treści online dołożył wszelkich starań zgodnie z wysokimi standardami staranności zawodowej w sektorze, postuluje się, by wziąć pod uwagę to, czy dostawca usług podjął wszystkie kroki, jakie podjąłby staranny podmiot dla osiągnięcia celu dotyczącego zapobiegania dostępności nieobjętych zezwoleniem utworów lub innych przedmiotów objętych ochroną na swojej stronie internetowej (motyw 66).

C. Strażnicy dostępu

Terminu „strażnicy dostępu” Komisja Europejska użyła w treści wniosku do Parlamentu Europejskiego z dnia 12 grudnia 2020 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym (akt o rynkach cyfrowych, ARC)³². Pojęcie kontestowalności jest w literaturze definiowane na różne sposoby, zawsze jednak jest odnoszone do jednej z zasadniczych cech rynków gospodarczych, tj. konkurencyjności. Za rynek kontestowalny uznawany jest

³² ARC.

zatem rynek „potencjalnie konkurencyjny”³³. Jest to rynek oligopolistyczny, na którym nie istnieją bariery wejścia, a „łatwość wtargnięcia na taki rynek powoduje, że przedsiębiorstwa na nim obecne zachowują się tak, jakby działały w warunkach konkurencji doskonałej”³⁴. Według innej definicji jest to rynek, na którym nie ma żadnych ograniczeń ani kosztów związanych z wejściem lub wyjściem. Powoduje to, że podmioty funkcjonujące na danym rynku znajdują się pod presją potencjalnych wejść³⁵. Warunkiem kontestowalności rynku są niskie koszty utopione³⁶.

Zauważono, że kilka dużych platform w coraz większym stopniu pełni funkcję punktów dostępu lub strażników dostępu w kontaktach między użytkownikami biznesowymi a użytkownikami końcowymi oraz osiągnęło ugruntowaną i trwałą pozycję, często będącą wynikiem tworzenia konglomeratowych ekosystemów wokół świadczonych podstawowych usług platformowych, co zwiększa istniejące bariery wejścia³⁷.

Celem przyjęcia przez Parlament Europejski i Radę w rozporządzenia w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym (ARC) było, jak wskazano w treści wniosku Komisji oraz w art. 1 ust. 1 ARC:

przyczynienie się do prawidłowego funkcjonowania rynku wewnętrznego poprzez ustanowienie zharmonizowanych przepisów służących zapewnieniu wszystkim przedsiębiorstwom kontestowalnych i uczciwych rynków w sektorze cyfrowym w całej Unii, na których działają strażnicy dostępu, z korzyścią dla użytkowników biznesowych i użytkowników końcowych.

³³ Hasło: *rynek kontestowalny*, [w:] *Encyklopedia PWN*, <https://encyklopedia.pwn.pl/haslo/rynek-kontestowalny;3970469.html> (dostęp: 13.03.2024).

³⁴ Hasło: *rynek potencjalnie konkurencyjny, rynek sporny*, [w:] *Encyklopedia PWN*, <https://encyklopedia.pwn.pl/haslo/rynek-potencjalnie-konkurencyjny;3970477.html> (dostęp: 13.03.2024).

³⁵ N.G. Mankiw, M.P. Taylor, *Mikroekonomia*, Warszawa 2022, s. 528, cyt. za: Hasło: *rynek kontestowalny*, [w:] Wikipedia, https://pl.wikipedia.org/wiki/Rynek_kontestowalny#cite_note-2 (dostęp: 13.03.2024).

³⁶ N.G. Mankiw, M.P. Taylor, *Mikroekonomia*, Warszawa 2022, s. 740, cyt. za: Hasło: *koszty utopione*, [w:] Wikipedia, https://pl.wikipedia.org/wiki/Koszty_utopione#cite_note-1 (dostęp: 13.03.2024).

³⁷ Tamże, s. 1.

Potwierdzono zatem, że warunkiem rozwoju sektora gospodarki cyfrowej jest zapewnienie wysokiej kontestowalności (konkurencyjności) rynku usług cyfrowych, ale także potwierdzono, co wydaje się zasadnicze, obecność na tym rynku podmiotów mających status strażników dostępu, a w konsekwencji ustalono dla nich szczególne zadania i powierzono im szczególną rolę (misję) do wypełnienia.

Strażnikami dostępu zostały nazwane podmioty świadczące podstawowe usługi platformowe, jeżeli:

1. wywierają znaczący wpływ na rynek wewnętrzny,
2. obsługują co najmniej jeden istotny punkt dostępu umożliwiający dotarcie do konsumentów oraz
3. osiągnęły lub oczekuje się, że osiągną ugruntowaną i trwałą pozycję w zakresie prowadzonej działalności³⁸.

Wszystkie wskazane powyżej czynniki są ze sobą powiązane i stanowią zestaw kumulatywnie stosowanych przesłanek służących Komisji Europejskiej do dokonywania systematycznej oceny statusu przedsiębiorstw świadczących podstawowe usługi platformowe.

Podstawowe usługi platformowe obejmują:

1. usługi pośrednictwa internetowego (w tym np. platformy handlowe, sklepy z aplikacjami i usługi pośrednictwa internetowego w innych sektorach, takich jak mobilność, transport lub energia),
2. wyszukiwarki internetowe,
3. serwisy społecznościowe,
4. usługi platformy udostępniania wideo,
5. usługi łączności interpersonalnej niewykorzystujące numerów,
6. systemy operacyjne,
7. usługi w chmurze oraz
8. usługi reklamowe, w tym sieci reklamowe, giełdy reklamowe oraz wszelkie pozostałe usługi pośrednictwa w zakresie reklam, w przypadku gdy takie usługi reklamowe są związane z co najmniej jedną z pozostałych podstawowych usług platformowych wymienionych powyżej³⁹.

³⁸ Art. 3 ust. 1 lit. a–c ARC.

³⁹ Art. 2 pkt 2 ARC.

Strażnikami dostępu są podmioty, które „obsługują co najmniej jeden istotny punkt dostępu”⁴⁰. Punkt dostępu oznacza usługę platformową zapewniającą usługobiorcy docieranie do użytkowników końcowych. Odzwierciedleniem pełnienia funkcji „punktu dostępu” jest potencjał usługi w zakresie jej monetyzacji. Potencjalny poziom monetyzacji wynika z kolei z liczby jej odbiorców i wysokiego obrotu uzyskiwanego z tytułu świadczenia tej usługi (motyw 17 ARC). W konsekwencji „posiadanie bardzo dużej liczby użytkowników biznesowych, którzy są zależni od podstawowej usługi platformowej, aby docierać do bardzo dużej liczby aktywnych miesięcznie użytkowników końcowych, umożliwia przedsiębiorstwu świadczącemu tę usługę wpływanie – z korzyścią dla siebie – na działalność znacznej części użytkowników biznesowych oraz zasadniczo wskazuje na to, że przedsiębiorstwo to stanowi ważny punkt dostępu” (motyw 20 ARC).

Nie każdy podmiot świadczący usługi platformowe będzie mieć status strażnika dostępu, lecz tylko ten, który spełnia kryteria ilościowe. Kluczowe dla ustalenia statusu strażnika dostępu nie jest bowiem stwierdzenie, jakie rodzaje usług (podstawowe usługi platformowe) świadczy podmiot, ale to, jakie znaczenie jego działalność ma dla innych użytkowników internetu. Chodzi zatem o ustalenie, czy działalność tego podmiotu ma wpływ na stopień kontestowalności rynku cyfrowego.

Na gruncie ARC przyjęto, że strażnika dostępu można ustalić poprzez zastosowanie wyraźnie określonych i odpowiednich wskaźników ilościowych, które mogą służyć jako przesłanki stanowiące domniemanie wzruszalne w celu ustalenia statusu strażnika dostępu w przypadku konkretnych dostawców, albo na podstawie oceny jakościowej przeprowadzanej w poszczególnych przypadkach w drodze badania rynku⁴¹. Wskaźniki ilościowe i sposób dokonywania ich pomiaru, a także obowiązek powiadamiania Komisji Europejskiej w razie zaistnienia tych wskaźników, zostały opisane w art. 3 ARC.

Domniemywa się, że przedsiębiorstwo nabywa status strażnika dostępu, który formalnie potwierdza Komisja Europejska⁴², jeżeli zostały spełnione kumulatywnie następujące warunki:

⁴⁰ ARC, s. 2.

⁴¹ ARC, s. 3.

⁴² Art. 3 ust. 4 ARC, zgodnie z którym „Komisja – bez zbędnej zwłoki i najpóźniej w terminie 45 dni roboczych od dnia otrzymania kompletnych informacji, o których

1. przedsiębiorstwo uzyskało roczny obrót w Unii wynoszący co najmniej 7,5 mld EUR w każdym z ostatnich trzech lat obrotowych lub jeżeli jego średnia kapitalizacja rynkowa lub równoważna rzeczywista wartość rynkowa wynosiła co najmniej 75 mld EUR w ostatnim roku obrotowym oraz świadczy tę samą podstawową usługę platformową w co najmniej trzech państwach członkowskich (art. 3 ust. 2 lit. a ARC), a zarazem
2. jeżeli świadczy podstawową usługę platformową, z której w ostatnim roku obrotowym korzystało co najmniej 45 mln aktywnych miesięcznie użytkowników końcowych mających siedzibę lub miejsce pobytu w Unii oraz co najmniej 10 000 aktywnych rocznie użytkowników biznesowych z siedzibą w Unii, przy czym użytkowników tych identyfikuje się i oblicza się ich liczbę zgodnie z metodyką i wskaźnikami określonymi w załączniku do ARC (art. 3 ust. 1 lit. b ARC), a ponadto (art. 3 ust. 2 lit. b ARC)
3. jeżeli wyżej wskazane progi zostały osiągnięte w każdym z ostatnich trzech lat obrotowych (art. 3 ust. 2 lit. c ARC).

Punkt dostępu oznacza zatem świadczenie jednej ze wskazanych w art. 2 ust. 2 lit. a–j ARC podstawowych usług platformowych, jeśli generuje obrót, o którym mowa w art. 3 ust. 2 lit. a ARC przy założeniu, że liczba odbiorców usługi wynosi tyle, ile wskazano w 3 ust. 2 lit. b ARC, przez czas nie krótszy niż 3 lata obrotowe, na który wskazano w art. 3 ust. 2 lit. c ARC. Spełnienie kryteriów ilościowych pozwala zarazem na przyjęcie domniemania natury jakościowej, tj. potwierdzenie, że przedsiębiorstwo wywiera znaczący wpływ na rynek wewnętrzny. Znaczący wpływ na rynku wewnętrznym jest używany – jak przyjmuje KE⁴³ – dzięki efektowi sieciowemu⁴⁴, tworzeniu własnych ekosystemów usług platformowych, pośredniczeniu w większości

mowa w ust. 3 – wskazuje jako strażnika dostępu przedsiębiorstwo świadczące podstawowe usługi platformowe, które osiągnęło wszystkie progi ustanowione w ust. 2”.

⁴³ ARC, s. 2. Hasło: *rynek kontestowalny*, [w:] Encyklopedia PWN, <https://encyklopedia.pwn.pl/haslo/rynek-kontestowalny;3970469.html> (dostęp: 13.03.2024).

⁴⁴ Efekt sieciowy to efekt ekonomiczny, który opisuje produkt lub usługę zyskującą na wartości wraz z coraz większą liczbą użytkowników. Gdy jest on obecny, każdy nowy użytkownik dodaje wartość produktowi poprzez wejście do sieci. To z kolei zachęca kolejnych użytkowników do skorzystania z produktu, co dalej zwiększa jego wartość; zob. *Czym Jest Efekt Sieciowy?*, 4.01.2021, Binance Academy, <https://academy.binance.com/pl/articles/what-is-a-network-effect> (dostęp: 11.03.2024).

transakcji pomiędzy klientami biznesowymi a użytkownikami końcowymi. Natomiast uzyskanie trwałej i ugruntowanej pozycji na rynku usług cyfrowych wynika z prowadzonej przez strażnika dostępu gospodarki danymi i zarządzania nimi, a w szczególności jest rezultatem śledzenia, profilowania oraz budowania „konglomeratowych ekosystemów wokół świadczonych przez niego usług”⁴⁵. Przedsiębiorca uzyskuje status strażnika dostępu wówczas, kiedy choćby jedna ze świadczonych przez niego podstawowych usług platformowych spełnia kryteria wskazane w art. 3 ust. 2 lit. a–c.

Dnia 6 września 2023 r. Komisja Europejska wyznaczyła po raz pierwszy sześciu strażników – Alphabet (Google Maps, Zakupy Google, Wyszukiwarka Google, YouTube, Android Mobile, Usługa reklamowa Alphabet online; Google Chrome), Amazon (platforma sprzedażowa, usługa reklamowa), Apple (AppStore, iOS, Safari), ByteDance (TikTok), Meta (Facebook Marketplace, Facebook, Instagram, WhatsApp, Messenger, Meta Ads), Microsoft (LinkedIn, system operacyjny Windows PC). W sumie wyznaczono 22 podstawowe usługi platformy świadczone przez tych strażników⁴⁶.

Zgodnie z art. 33 ust. 4 AUC o wyznaczeniu dostawcy usługi jako strażnika dostępu Komisja Europejska postanawia na podstawie informacji przekazanych przez dostawcę usługi lub informacji żądanych przez KE na podstawie art. 24 ust. 3 lub wszelkich innych informacji dostępnych Komisji. Nadto KE może przyjmować akty delegowane zgodnie z art. 87 po konsultacji z Radą Usług Cyfrowych, aby uzupełnić przepisy rozporządzenia poprzez ustanowienie metodyki obliczania średniej liczby aktywnych miesięcznie odbiorców usługi w Unii do celów ustalenia, czy dostawca usługi należy do kategorii strażników dostępu, zapewniając, aby w metodyce tej uwzględniono zmiany rynkowe i technologiczne (art. 33 ust. 3 AUC). Platformy zostały wyznaczone na podstawie danych dotyczących użytkowników, które musiały zostać opublikowane przez dostawców usług do 17 lutego 2023 r.⁴⁷ Przedsiębiorca uzyskuje status strażnika dostępu wówczas, kiedy choćby jedna ze świadczonych przez niego podstawowych usług platformowych spełnia wskazane powyżej kryteria.

⁴⁵ ARC, s. 1.

⁴⁶ *Strażnicy dostępu*, Komisja Europejska, https://digital-markets-act.ec.europa.eu/gatekeepers_en?ettrans=pl&prefLang=pl (dostęp: 19.03.2024).

⁴⁷ Komunikat KE z dnia 25 kwietnia 2023 r., https://ec.europa.eu/commission/presscorner/detail/pl/ip_23_2413 (dostęp: 28.08.2023).

Komisja i Parlament Europejski przyjmując rozwiązania zawarte w Akcie o rynkach cyfrowych (ARC)⁴⁸, wyraziły stanowisko, zgodnie z którym należało opracować na poziomie prawa europejskiego wspólne dla wszystkich państw członkowskich UE mechanizmy regulacyjne. Wskazały po pierwsze na potrzebę zapewnienia, że rynki, na których działają strażnicy dostępu, będą i pozostaną kontestowalne i uczciwe, niezależnie od rzeczywistych, potencjalnych lub domniemanych skutków praktyki danego strażnika dostępu (motyw 11 ARC), a po drugie, uznając, że celu tego nie da się osiągnąć bez interwencji organu publicznego, który będzie wyposażony w instrumenty i narzędzia pozwalające na interwencję wówczas, gdy kontestowalność rynków cyfrowych byłaby zagrożona.

Rozważano trzy warianty rozwiązań: wariant 1 – polegający na uprzednim, sztywnym określeniu wykazu strażników dostępu i automatycznym przypisaniu im obowiązków, wariant 2 – polegający na przyjęciu częściowo elastycznych ram wyznaczania dostawców podstawowych usług platformowych jako strażników dostępu i zasadzie aktualizowania obowiązków, w tym w ramach dialogu regulacyjnego ze strażnikami⁴⁹ oraz wariant 3 – polegający na zastosowaniu w pełni elastycznych narzędzi zapewniających dynamiczny mechanizm aktualizacji umożliwiający włączenie dodatkowych podstawowych usług platformowych i dodatkowych obowiązków, jeżeli takie włączenie zostałoby uznane za właściwe i uzasadnione w wyniku badania rynku. Zakres tego wariantu opiera się wyłącznie na progach jakościowych⁵⁰. W ramach wszystkich wariantów przewiduje się wdrażanie, nadzór oraz egzekwowanie przepisów na szczeblu UE przez Komisję jako właściwy organ regulacyjny⁵¹.

Ostatecznie zdecydowano się na realizację drugiego wariantu opartego na dialogu regulacyjnym z przedsiębiorcami świadczącymi podstawowe usługi platformowe i wykorzystaniu elastycznych narzędzi ingerencji zarówno

⁴⁸ ARC.

⁴⁹ Tamże, s. 11.

⁵⁰ Dokument roboczy służb Komisji: Sprawozdanie ze streszczenia oceny skutków, towarzyszący dokumentowi: Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym (akt o rynkach cyfrowych), <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A52020SCo364> (dostęp: 18.03.2024).

⁵¹ ARC, s. 11.

w odniesieniu do ustalania zakresu usług, jak i zakresu obowiązków ciążących na strażnikach. Preferowany wariant (wariant 2) obejmuje:

- a) zamknięty wykaz podstawowych usług platformowych,
- b) połączenie ilościowych i jakościowych kryteriów w celu wyznaczenia dostawców podstawowych usług platformowych jako strażników dostępu,
- c) mające bezpośrednie zastosowanie obowiązki, w tym niektóre obowiązki, w przypadku których dialog regulacyjny może ułatwić ich skuteczne wdrażanie, oraz
- d) możliwość aktualizowania przez Komisję instrumentu po przeprowadzeniu badania rynku, jeżeli chodzi o obowiązki strażników dostępu, za pośrednictwem aktów delegowanych w zakresie, w jakim zostaną zidentyfikowane nowe praktyki, które są równie nieuczciwe, i które mogą z dużym prawdopodobieństwem zakłócać kontestowalność, a także za pośrednictwem wniosków w sprawie zmiany przepisów w pozostałych przypadkach.

Badania rynku mogą również wskazać na potrzebę zmiany wykazu podstawowych usług platformowych⁵².

Celem preferowanego wariantu było określenie odpowiedniego podziału obowiązków w walce z nielegalnymi treściami w internecie między dostawców usług pośrednich, odbiorców tych usług i organy. Wariant ten cechuje asymetryczne podejście do obowiązków w zakresie należytej staranności nałożonych na bardzo duże platformy internetowe. Jest to:

nadzorowane podejście do zarządzania ryzykiem, w którym ważną rolę odgrywa system zarządzania dotyczący egzekwowania przepisów. Asymetryczne obowiązki nakłada się wyłącznie na bardzo duże platformy internetowe, które zgodnie z aktualnymi danymi mają nie tylko najszerszy zasięg, ale są również dużymi przedsiębiorstwami osiągającymi znaczące obroty⁵³.

⁵² Tamże, s. 12.

⁵³ Tamże, s. 13.

Obowiązki strażników dostępu zostały opisane w rozdziale III ARC. W szczególności określa się w nim automatycznie wykonywane obowiązki (art. 5) oraz obowiązki podlegające doprecyzowaniu (art. 6), które dostawcy wyznaczeni jako strażnicy dostępu powinni spełnić w odniesieniu do każdej ze swoich podstawowych usług platformowych wymienionych w odpowiedniej decyzji o wyznaczeniu. Ponadto ustanawia się w nim ramy możliwego dialogu między dostawcą podstawowych usług platformowych (wyznaczonym jako strażnik dostępu) a Komisją w odniesieniu do środków, które strażnik dostępu wdraża lub zamierza wdrożyć w celu spełnienia obowiązków określonych w art. 6 (art. 7). Określa się w nim również warunki zawieszenia obowiązków dotyczących poszczególnych podstawowych usług platformowych w wyjątkowych okolicznościach (art. 8) lub udzielenia zwolnienia ze względu na interes publiczny (art. 9)⁵⁴.

Na strażników dostępu nałożono w ARC zarówno obowiązki pozytywne, jak i negatywne. Strażnicy dostępu nie będą mogli:

- a) pozycjonować swoich usług i produktów wyżej niż usługi i produkty oferowane przez inne podmioty rynkowe,
- b) uniemożliwiać sprzedawcom aplikacji korzystania z zewnętrznych platform płatniczych,
- c) przetwarzać danych osobowych użytkowników do celów reklamy ukierunkowanej, chyba że wyrazili na to zgodę,
- d) ustanawiać nieuczciwych warunków dla użytkowników biznesowych,
- e) preinstalować pewnych aplikacji ani uniemożliwiać użytkownikom łatwego ich odinstalowania,
- f) stosować ograniczeń wobec użytkowników biznesowych korzystających z platform⁵⁵.

Strażnicy będą musieli:

- a) oferować szerszy wybór, np. możliwość wyboru określonego oprogramowania w systemie operacyjnym użytkownika,
- b) zapewnić, aby rezygnacja z subskrypcji podstawowych usług platformowych była równie łatwa jak sama subskrypcja,

⁵⁴ Tamże, s. 15.

⁵⁵ Art. 5 ust. 2 ARC.

- c) przekazywać informacje o liczbie użytkowników, którzy odwiedzają ich platformy, dzięki czemu można będzie ustalić, czy dana platforma jest strażnikiem dostępu,
- d) zapewnić użytkownikom biznesowym dostęp do własnych danych na temat wyników działań marketingowych lub reklamowych na platformie,
- e) informować Komisję Europejską o przeprowadzanych przez siebie fuzjach i przejęciach,
- f) zapewnić interoperacyjność podstawowych funkcji usług komunikacji natychmiastowej, tj. umożliwić użytkownikom wymianę i/lub wysyłanie wiadomości tekstowych, głosowych lub plików⁵⁶.

W przypadku, gdy strażnik dostępu narusza te przepisy, może zostać obciążony grzywną w wysokości do 10% swojego łącznego światowego obrotu. Jeśli dochodzi do ponownego naruszenia, wysokość grzywny może wzrosnąć do 20% łącznego światowego obrotu. W przypadku systematycznego nieprzestrzegania aktu o rynkach cyfrowych – to znaczy, gdy strażnik dostępu naruszy przepisy co najmniej 3 razy w ciągu 8 lat – Komisja Europejska może rozpocząć badanie rynku i, w razie potrzeby, zastosować behawioralne lub strukturalne środki zaradcze⁵⁷.

Strażnik dostępu jest zobowiązany do wypełniania wszystkich obowiązków w odniesieniu do każdej z podstawowych usług platformowych wymienionych w decyzji o wskazaniu go przez KE jako strażnika dostępu (art. 6 ust. 1 ARC). Podobnie jak obowiązki z art. 5 ARC, obowiązki z art. 6 ARC znajdują zastosowanie w odniesieniu do każdej podstawowej usługi platformowej świadczonej przez strażnika dostępu, która została wymieniona w decyzji o wskazaniu. Jednocześnie nie stosuje się ich do innych usług świadczonych przez strażnika dostępu, w tym do podstawowych usług platformowych, które nie zostały wymienione w decyzji o wskazaniu⁵⁸. Doprecyzowaniu (doregulowaniu) podlegają obowiązki wymienione w art. 6 ARC. Oznacza to, że Komisja w drodze aktu wykonawczego (decyzji) może określić środki, które dany strażnik dostępu ma wdrożyć w celu skutecznego wypełnienia

⁵⁶ Art. 5 ust. 4–10 oraz art. 6 ARC.

⁵⁷ Art. 30 ARC.

⁵⁸ I. Małobęcka-Szwast, *Komentarz do art. 6 ARC*, [w:] *Rynek cyfrowy. Akt o usługach cyfrowych. Akt o rynkach cyfrowych. Rozporządzenie platform-to-business. Komentarz*, M. Grochowski (red.), Warszawa 2024, pkt 2.

obowiązków ustanowionych w tym przepisie⁵⁹. Określając takie środki, Komisja powinna zapewnić, by skutecznie przyczyniały się one do osiągnięcia celów DMA i celu, w jakim ustanowiono dany obowiązek, oraz były proporcjonalne w określonej sytuacji strażnika dostępu i odpowiedniej usługi⁶⁰.

Strażnik dostępu zapewnia wypełnianie obowiązków ustanowionych w art. 5, 6 i 7 ARC i wykazuje ich wypełnianie. Środki, jakie strażnik dostępu wdraża, aby zapewnić przestrzeganie tych artykułów, muszą skutecznie przyczyniać się do osiągnięcia celów rozporządzenia⁶¹ i celu, w jakim ustanowiono dany obowiązek (art. 8 ust. 1 ARC). Artykuły 8–10 ARC wyznaczają ramy dialogu regulacyjnego, jaki może toczyć się pomiędzy strażnikiem dostępu a Komisją Europejską. W wyniku uwzględnienia wniosku przedsiębiorcy będącego strażnikiem dostępu albo z własnej inicjatywy KE może: zawiesić (art. 9 i art. 10 ust. 4), zmienić lub ograniczyć obowiązki nałożone na strażnika, a także zwolnić strażnika z realizacji obowiązków wskazanych w decyzji o wyznaczeniu (art. 10 ust. 1). Zwolnienia można udzielić wyłącznie ze względów zdrowia publicznego lub bezpieczeństwa publicznego (art. 10 ust. 3).

2. Rodzaje usług cyfrowych – usługi społeczeństwa informacyjnego

Pojęcie usług cyfrowych jest wykorzystywane w aktach prawnych regulujących różne sektory działalności. Pojawia się jako przedmiot normowania zarówno stosunków prywatnoprawnych, jak i publicznoprawnych. Usługi

⁵⁹ Komisja może – z własnej inicjatywy lub na wniosek strażnika dostępu na podstawie art. 8 ust. 3 – wszcząć postępowanie na podstawie art. 20. Komisja może przyjąć akt wykonawczy określający środki, które dany strażnik dostępu ma wdrożyć w celu skutecznego wypełnienia obowiązków ustanowionych w art. 6 i 7 (art. 8 ust. 2 ARC).

⁶⁰ I. Małobęcka-Szwast, *Komentarz...*, pkt 3.

⁶¹ Wskazuje się, że obowiązki nałożone na strażników dostępu w art. 5, 6 i 7 DMA stanowią istotę i fundament rozporządzenia DMA. Mają one na celu zabezpieczenie kontestowalności i uczciwości podstawowych usług platformowych świadczonych przez strażników dostępu na rynku wewnętrznym, czyli osiągnięcie dwóch głównych celów komentowanego rozporządzenia; zob. I. Małobęcka-Szwast, *Komentarz...*, s. 16.

cyfrowe są definiowane przy zastosowaniu kryterium podmiotowego, a zatem ze względu na kategorie dostawców usług albo ze względu na przedmiot świadczenia, a w szczególności charakter lub rodzaj świadczonej usługi. Niejednokrotnie ten sam podmiot świadczy usługi cyfrowe różnego rodzaju (np. usługi pośrednictwa internetowego i usługi dostarczania treści albo usługi udostępniania treści online). Świadczenie usług cyfrowych jest determinowane technologicznie, co oznacza, że mogą one być wykonywane wyłącznie w środowisku cyfrowym i w zdigitalizowanej postaci. Ich wspólną cechą jest niematerialna postać wymagająca stosowania urządzeń i nośników informacyjnych do celów ich wykonywania i odbioru.

Usługi cyfrowe mają wspólny rodowód. Wywodzą się z terminu „usługi społeczeństwa informacyjnego”. Definicja usług społeczeństwa informacyjnego obowiązuje w prawie wspólnotowym od 22 czerwca 1998 r., kiedy została przyjęta w dyrektywie 98/34/WE Parlamentu Europejskiego i Rady ustanawiającej procedurę udzielania informacji w zakresie norm i przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego⁶², a następnie powtórzona w dyrektywie 98/84/WE Parlamentu Europejskiego i Rady z dnia 20 listopada 1998 r. w sprawie prawnej ochrony usług opartych lub polegających na warunkowym dostępie⁶³. Aktualne jej brzmienie zostało zawarte w art. 1 ust. 1 lit. b dyrektywy 2015/1535⁶⁴.

Pojęcie usługi społeczeństwa informacyjnego zostało zdefiniowane w art. 15 dyrektywy 2015/1535⁶⁵ i oznacza każdą usługę normalnie świadczoną za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy. „Na odległość” oznacza, że usługa świadczona jest bez równoczesnej obecności stron. „Drogą elektroniczną” oznacza, iż usługa jest wysyłana i odbierana w miejscu przeznaczenia za pomocą sprzętu elektronicznego do przetwarzania (włącznie z kompresją cyfrową) oraz przechowywania

⁶² Dyrektywa 98/34/WE Parlamentu Europejskiego i Rady z dnia 22 czerwca 1998 r. ustanawiająca procedurę udzielania informacji w zakresie norm i przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz.U. L Nr 204, s. 37). Dyrektywa zmieniona dyrektywą 98/48/WE (Dz.U. L Nr 217 z 1998 r., s. 18).

⁶³ Dyrektywa 98/84/WE Parlamentu Europejskiego i Rady z dnia 20 listopada 1998 r. w sprawie prawnej ochrony usług opartych lub polegających na warunkowym dostępie (Dz.U. L Nr 320, s. 54).

⁶⁴ Dyrektywa w sprawie usług społeczeństwa informacyjnego.

⁶⁵ Tamże.

danych, i która jest całkowicie przesyłana, kierowana i otrzymywana za pomocą kabla, fal radiowych, środków optycznych lub innych środków elektromagnetycznych. „Na indywidualne żądanie odbiorcy usług” oznacza, że usługa świadczona jest poprzez przesyłanie danych na indywidualne żądanie (art. 1 ust. 1 dyrektywy w sprawie usług społeczeństwa informacyjnego)⁶⁶.

Zakres pojęcia „usługi społeczeństwa informacyjnego” jest szeroki i – w świetle stanowiska Trybunału Sprawiedliwości – obejmuje wszelkie usługi cyfrowe, o ile ich wykonywanie następuje drogą elektroniczną (przez internet), na odległość oraz na indywidualne żądanie odbiorcy usługi. Rzecznik Generalny UE na tle dotychczasowej wykładni tego terminu dokonywanej przez TSUE przyjął, że „usługami społeczeństwa informacyjnego” są – jak napisał – „po prostu usługi przez Internet, umożliwiające nie tylko przedsiębiorcom, ale także osobom nieprowadzącym działalności gospodarczej, oferowanie konsumentom usług o różnym charakterze poprzez umożliwienie kontaktu między nimi z drugimi”⁶⁷.

Dostawcą usług społeczeństwa informacyjnego są zatem zarówno tzw. pośrednicy internetowi, których status reguluje rozporządzenie – akt o usługach cyfrowych (AUC), jak też dostawcy usług udostępniania treści online, o których mowa w dyrektywie 2019/790, a także dostawcy treści cyfrowych, zgodnie z zasadami określonymi w tzw. dyrektywie konsumenckiej (dyrektywa 2019/770⁶⁸). Usługi pośrednictwa internetowego, jak również usługi udostępniania treści online, a także usługi dostarczania treści cyfrowych są wykonywane, co do zasady, przez podmioty będące przedsiębiorcami w ramach zorganizowanej działalności nastawionej na zysk. Termin „dostarczanie usług społeczeństwa informacyjnego” jest jednak pojęciem, które zakresem przedmiotowym obejmuje nie tylko działalność przedsiębiorców,

⁶⁶ Trybunał stwierdził, że art. 2 lit. b) dyrektywy 2000/31 definiuje pojęcie „usługi społeczeństwa informacyjnego” poprzez odesłanie do art. 1 ust. 2 dyrektywy 98/34, który dotyczy każdej usługi „normalnie świadczonej za wynagrodzeniem”, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług (Wyrok TS w sprawie *Sotiris Papasavvas przeciwko O Fileleftheros Dimosia Etaireia Ltd.*).

⁶⁷ Opinia Rzecznika Generalnego z dnia 7 lipca 2022 r. w sprawie *Airbnb Ireland UC, Airbnb Payments UK Ltd przeciwko Agenzia delle Entrate*, C-83/21, <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:62021CC0083> (dostęp: 28.08.2023).

⁶⁸ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/770 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych i usług cyfrowych (Dz.U. UE L Nr 136, s. 1 z późn. zm.).

lecz także użytkowników internetu, których aktywność jest nakierowana na publiczne udostępnianie oraz kreowanie treści cyfrowych i ich przechowywanie w celach innych niż uzyskanie wynagrodzenia bezpośrednio od osoby korzystającej z tych usług. Zatem podmioty uzyskujące wynagrodzenie z tytułu reklam zamieszczanych w otoczeniu udostępnianych przez nie treści albo uzyskujące – w miejsce świadczonej usługi – zezwolenie usługobiorcy na przetwarzanie jego danych osobowych, należą do kategorii dostawców usług społeczeństwa informacyjnego.

Problem kryterium odpłatności za usługę jako warunku *sine qua non* kwalifikowania usługi do kategorii usług społeczeństwa informacyjnego był przedmiotem rozstrzygnięcia Trybunału Sprawiedliwości w wyroku z dnia 11 września 2014 r. w sprawie, w której Trybunał odpowiadał m.in. na pytanie o to, czy definicje „usług społeczeństwa informacyjnego” i „usługodawcy” w rozumieniu art. 2 (dyrektywy 2000/31) i art. 1 ust. 2 (dyrektywy 98/34) obejmują usługi informacyjne online, które nie są płatne bezpośrednio przez odbiorcę tych usług, tylko są odpłatne pośrednio dzięki reklamom pojawiającym się na stronie internetowej⁶⁹.

Odnosnie do kwestii, czy wynagrodzenie to powinno koniecznie być przekazane przez samego adresata usługi, Trybunał podniósł, że taka przesłanka jest wyraźnie wykluczona przez motyw 18 dyrektywy 2000/31, w świetle którego należy interpretować art. 2 lit. a) dyrektywy 2000/31 i który uściśla, że usługi społeczeństwa informacyjnego rozciągają się, o ile stanowią one działalność gospodarczą, na usługi, „które nie są wynagradzane przez tych, którzy je otrzymują, takie jak usługi polegające na oferowaniu informacji online lub informacji handlowych”. Ta wykładnia odpowiada wykładni pojęcia „usług” w rozumieniu art. 57 TFUE, która również nie wymaga, aby za usługę płaciła osoba z niej korzystająca⁷⁰. W świetle powyższego Trybunał stwierdził, że pojęcie usług społeczeństwa informacyjnego obejmuje usługi polegające na oferowaniu informacji online, za które usługodawca otrzymuje

⁶⁹ Wyrok TS w sprawie Sotiris Papasavvas przeciwko O Fileleftheros Dimosia Etairia Ltd.

⁷⁰ Wyrok TS z dnia 26 kwietnia 1988 r. w sprawie Bond van Adverteerders i in. przeciwko Państwu Holenderskiemu, 352/85, poz. 2085, s. 16.

wynagrodzenie nie od usługobiorcy, lecz z przychodów uzyskiwanych z reklam emitowanych na stronie internetowej⁷¹.

Trybunał zaliczył do podmiotów świadczących usługi społeczeństwa informacyjnego w szczególności:

1. przedsiębiorcę dokonującego sprzedaży przez internet soczewek kontaktowych⁷²,
2. wydawcę tytułu prasowego oferującego usługi informacyjne online, które nie są płatne bezpośrednio przez odbiorcę tych usług, tylko są odpłatne pośrednio dzięki reklamom pojawiającym się na stronie internetowej⁷³,

⁷¹ Wyrok TS w sprawie Sotiris Papasavvas przeciwko O Fileleftheros Dimosia Etaireia Ltd.

⁷² Zagadnieniem wymagającym rozstrzygnięcia przedstawionym Trybunałowi przez sąd węgierski były pytania: 1) Czy sprzedaż soczewek kontaktowych stanowi konsultację medyczną wymagającą fizycznego badania pacjenta, a zatem jest wyłączona z zakresu stosowania dyrektywy [o handlu elektronicznym]?; 2) Jeżeli sprzedaż soczewek kontaktowych nie stanowi konsultacji medycznej wymagającej fizycznego badania pacjenta, czy wykładni art. 30 WE należy dokonywać w ten sposób, że sprzeczne z jego postanowieniami jest uregulowanie państwa członkowskiego, które stanowi, że soczewki kontaktowe mogą być sprzedawane wyłącznie w specjalistycznych punktach sprzedaży wyrobów medycznych?. Trybunał stwierdził, że przepisy krajowe dotyczące sprzedaży soczewek kontaktowych należą do zakresu zastosowania dyrektywy 2000/31 w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym), jako że dotyczą sprzedaży tych soczewek przez internet, to znaczy w szczególności oferowania online oraz zawierania umów drogą elektroniczną (Wyrok TS z dnia 2 grudnia 2010 r. w sprawie Ker-Optika bt przeciwko ÁNTSZ Dél-dunántúli Regionális Intézet, C-108/09, poz. I-12213).

⁷³ Trybunał udzielił pozytywnej odpowiedzi na pytanie: „Czy definicje »usług społeczeństwa informacyjnego« i »usługodawcy« w rozumieniu art. 2 dyrektywy [2000/31] i art. 1 ust. 2 dyrektywy [98/34] obejmują usługi informacyjne online, które nie są płatne bezpośrednio przez odbiorcę tych usług, tylko są odpłatne pośrednio dzięki reklamom pojawiającym się na stronie internetowej?» (Wyrok TS w sprawie Sotiris Papasavvas przeciwko O Fileleftheros Dimosia Etaireia Ltd.). Podobne stanowisko Trybunał zajął w wyroku z dnia 15 września 2016 r., kiedy stwierdził, że z motywów 2 i 19 dyrektywy 98/48 zmieniającej dyrektywę 98/34, a także art. 1 pkt 2 dyrektywy 98/34 wynika, że usługi społeczeństwa informacyjnego, o których mowa w art. 12 ust. 1 dyrektywy 2000/31, to wyłącznie usługi normalnie świadczone za wynagrodzeniem. Jednakże nie można wnioskować na tej podstawie, że świadczenie o charakterze gospodarczym realizowane bezpłatnie nie mogłoby nigdy stanowić »usług społeczeństwa informacyjnego« w rozumieniu art. 12 ust. 1 dyrektywy 2000/31. Wynagrodzenie za usługę świadczoną przez usługodawcę w ramach jego działalności gospodarczej niekoniecznie jest bowiem wypłacane przez osoby, które z nich korzystają. Jest tak w szczególności, gdy bezpłatnie realizowane świadczenie jest wykonywane przez usługodawcę w takich celach reklamowych, gdyż koszt tej działalności jest wówczas zawarty w cenie sprzedaży tych dóbr lub usług (Wyrok TS w sprawie Tobias Mc Fadden przeciwko Sony Music Entertainment Germany GmbH).

3. podmiot świadczący usługę pośrednictwa, która za pomocą aplikacji na smartfon umożliwia przekazywanie informacji dotyczących rezerwacji usługi przewozowej między pasażerem a niebędącym zawodowym kierowcą właścicielem pojazdu, który ma zrealizować ten przewóz⁷⁴,
4. podmiot świadczący usługę pośrednictwa, która polega na umożliwieniu, za wynagrodzeniem, nawiązania za pośrednictwem platformy elektronicznej kontaktu pomiędzy potencjalnymi najemcami a wynajmującymi (będącymi bądź niebędącymi przedsiębiorcami) oferującymi usługę krótkoterminowego zakwaterowania, czemu towarzyszy świadczenie również szeregu usług dodatkowych w stosunku do tej usługi pośrednictwa⁷⁵.

Przykładowy wykaz usług nieobjętych definicją „usług społeczeństwa informacyjnego” został określony w załączniku nr I dyrektywy 2015/1535. W załączniku usystematyzowano wyjątki w ten sposób, że odrębnie wskazano przykłady usług, które nie spełniają kryteriów technologicznych, tj. kryterium:

1. świadczenia na odległość,
2. świadczenia drogą elektroniczną,
3. świadczenia na indywidualne żądanie odbiorcy usługi.

⁷⁴ Trybunał odpowiadał na pytanie: „czy działalność pośrednictwa pomiędzy właścicielami pojazdów a osobami chcącymi przebyć trasę miejską prowadzona przez [Uber Systems Spain] w celach zarobkowych przy wykorzystaniu urządzeń informatycznych – interfejsu i oprogramowania (»inteligentnych telefonów i platformy technologicznej« wedle sformułowania [Uber Systems Spain]) – które umożliwiają skontaktowanie się tych osób, należy uznać za działalność przewozową, za elektroniczną usługę pośrednictwa czy też za właściwą usługę społeczeństwa informacyjnego w rozumieniu art. 1 pkt 2 [dyrektywy 98/34]?”. Trybunał zastrzegł, że usługa przedsiębiorstwa Uber nie obejmuje wyłącznie usługi umożliwiającej porozumienie między właścicielem pojazdu a klientem, ponieważ „Uber określa – za pomocą aplikacji o tej samej nazwie – przynajmniej maksymalną cenę danego przewozu, że przedsiębiorstwo to pobiera tę cenę od klienta, a następnie przekazuje jej część właścicielowi pojazdu niebędącemu zawodowym kierowcą i że sprawuje ono pewną kontrolę w odniesieniu do jakości pojazdów i ich kierowców, a także do zachowania tych ostatnich, przy czym kontrola taka może w stosownym wypadku skutkować wykluczeniem danego kierowcy ze świadczenia usług przewozowych”. W tym drugim zakresie, niezwiązanym z wykorzystaniem komunikacji elektronicznej do nawiązania kontaktu, usługa przedsiębiorstwa Uber stanowi usługę przewozową (Wyrok TS z dnia 20 grudnia 2017 r. w sprawie Asociación Profesional Elite Taxi przeciwko Uber Systems Spain SL, C-434/15, poz. I-981).

⁷⁵ Wyrok TS z dnia 19 grudnia 2019 r. w sprawie Postępowanie karne przeciwko X, C-390/18, LEX nr 2753786.

Zgodnie z zawartym w załączniku wykazem przyjęto, że kryterium „świadczona „na odległość” nie spełniają usługi świadczone w fizycznej obecności dostawcy i odbiorcy, nawet jeżeli są związane z wykorzystaniem urządzeń elektronicznych, np.:

- a) badanie lekarskie lub wykonywanie zabiegów w gabinecie lekarskim z zastosowaniem sprzętu elektronicznego, przy fizycznej obecności pacjenta,
- b) wgląd do elektronicznego katalogu w sklepie przy fizycznej obecności klienta,
- c) rezerwacja biletu lotniczego w biurze podróży za pomocą sieci komputerowej przy fizycznej obecności klienta,
- d) udostępnienie gier elektronicznych w salonie przy fizycznej obecności użytkownika.

Usługi, które nie są świadczone „drogą elektroniczną”, to – jak wskazano w załączniku – „usługi o charakterze materialnym, nawet jeżeli świadczone są z wykorzystaniem urządzeń elektronicznych: a) dystrybucja banknotów i biletów przez automaty (banknoty, bilety kolejowe); b) dostęp do płatnych dróg, parkingów itp., nawet jeżeli przy wjeździe lub wyjeździe funkcje kontroli wjazdu lub uiszczenia należności sprawują urządzenia elektroniczne”, a także usługi offline: „dystrybucja CD-ROM-ów lub oprogramowania na dyskiecie” oraz „usługi, które nie są świadczone z wykorzystaniem elektronicznego systemu przetwarzania i przechowywania danych”, takie jak:

usługi telefonii głosowej; usługi telefaksowe/teleksowe; usługi świadczone przez telefonię głosową lub telefaksem; telefoniczne/telefaksowe porady lekarskie; telefoniczne/telefaksowe porady prawne; telefoniczny/telefaksowy marketing bezpośredni.

Nie są także usługami społeczeństwa informacyjnego usługi, które nie spełniają kryterium świadczenia „na indywidualne żądanie odbiorcy usług”. Chodzi zatem o usługi świadczone w formie przesyłania danych bez indywidualnego zamówienia i przeznaczone do równoczesnego odbioru przez nieograniczoną liczbę odbiorców (transmisja z „punktu do wielu punktów”):

- a) usługi rozpowszechniania telewizyjnego (włącznie z usługami sekwencyjnego udostępniania audycji),

- b) usługi audiowizualne, o których mowa w dyrektywie 2010/13/UE⁷⁶, usługi przesyłania sygnału radiowego,
- c) teletext (telewizyjny).

Dostawcą usług społeczeństwa informacyjnego może być zarówno przedsiębiorca, jak i podmiot nieprowadzący działalności gospodarczej. Nie ma także znaczenia, czy usługi są świadczone odpłatnie czy nieodpłatnie, a w szczególności, czy świadczenie usługi jest uzależnione od uiszczenia opłaty przez jej odbiorcę (adresata). Usługi społeczeństwa informacyjnego obejmują zarówno dostarczanie treści cyfrowych, jak i pośrednictwo internetowe w dostarczaniu treści lub usług cyfrowych na indywidualne żądanie odbiorcy. Usługą społeczeństwa informacyjnego jest też udzielanie dostępu do treści wówczas, gdy w zamian za świadczenie usługi usługobiorca przekazuje swoje dane osobowe i zezwala usługodawcy na ich przetwarzanie w zakresie i celu przez niego określonym.

O zakwalifikowaniu podmiotu do grona „dostawców usług społeczeństwa informacyjnego” nie rozstrzyga ani cel świadczenia usługi, ani jej termin, treść, odpłatność lub brak odpłatności, ani częstotliwość bądź systematyczność (okresowość, periodyczność) świadczenia, ani też nie rozstrzyga o tym typ usługodawcy, ani rodzaj usługobiorcy. O zakwalifikowaniu podmiotu do kategorii dostawców usług społeczeństwa informacyjnego przesądza bowiem jej techniczny (technologiczny) komponent, tj. sposób świadczenia usługi.

⁷⁶ W dyrektywie Parlamentu Europejskiego i Rady 2010/13/UE z dnia 10 marca 2010 r. w sprawie koordynacji niektórych przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich dotyczących świadczenia audiowizualnych usług medialnych (dyrektywa o audiowizualnych usługach medialnych), wersja ujednolicona (Dz.U. UE L Nr 95, s. 1 z późn. zm.) usługę audiowizualną zdefiniowano jako: usługę, której głównym celem lub celem jej dającej się oddzielić części jest dostarczanie ogółowi odbiorców – poprzez sieci łączności elektronicznej w rozumieniu art. 2 lit. a) dyrektywy 2002/21/WE – audycji, za które odpowiedzialność redakcyjną ponosi dostawca usług medialnych, w celach informacyjnych, rozrywkowych lub edukacyjnych; taka audiowizualna usługa medialna jest przekazem telewizyjnym albo audiowizualną usługą medialną na żądanie (art. 1 ust. 1 lit. a dyrektywy 2010/13). Przekazem telewizyjnym (tzn. linearna audiowizualna usługa medialna) jest usługa umożliwiająca równoczesny odbiór audycji na podstawie układu audycji (art. 1 ust. 1 lit. e). Audiowizualną usługą na żądanie (tzn. nielinearna audiowizualna usługa medialna) jest usługa medialna świadczona przez dostawcę usług medialnych, umożliwiającą użytkownikowi odbiór audycji w wybranym przez niego momencie i na jego życzenie z wykorzystaniem katalogu audycji przygotowanego przez dostawcę usług medialnych (art. 1 ust. 1 lit. g).

Determinantą usług społeczeństwa informacyjnego i ich cechą relewantną jest technologia świadczenia usługi, a nie jej treść, zakres ani adresat.

Specyfikację usług społeczeństwa informacyjnego, której rezultatem stało się szczegółowe normowanie niektórych kategorii tych usług, zawiera dyrektywa o handlu elektronicznym (dyrektywa 2000/31). W dyrektywie tej wskazano po raz pierwszy na szczególny, wymagający odmiennego podejścia normatywnego, status pośredników internetowych. Potwierdzono wówczas, że usługi społeczeństwa informacyjnego obejmują szeroki zakres rodzajów działalności gospodarczej prowadzonych w trybie online, przy czym nie każda usługa cyfrowa polega na dostarczaniu treści, a nadto zadanie usługodawcy polega niekiedy wyłącznie na zapewnieniu możliwości wykonania usługi w środowisku internetowym przez inny podmiot odpowiedzialny – w efekcie – za treść lub przedmiot usługi. Usługi cyfrowe nie obejmują zatem rodzajów działalności takich jak dostawa towarów jako taka lub świadczenie usług offline (motyw 18 dyrektywy 200/31). Usługi społeczeństwa informacyjnego nie ograniczają się wyłącznie do usług dających sposobność do zawierania umów online, ale, o ile stanowią one działalność gospodarczą, dotyczą także usług, które nie są wynagradzane przez tych, którzy je otrzymują, np. usług polegających na oferowaniu informacji online lub informacji handlowych lub zapewniających narzędzia umożliwiające szukanie, dostęp oraz pozyskiwanie danych. Do usług społeczeństwa informacyjnego zaliczają się także usługi, które polegają na przekazywaniu informacji poprzez sieć komunikacyjną, na zapewnianiu możliwości dostępu do sieci komunikacyjnej lub na hostingu informacji przekazywanych przez usługobiorcę (motyw 18 dyrektywy 2000/31).

Z zakresu terminu usług społeczeństwa informacyjnego wyłączone zostały transmisje telewizyjne w rozumieniu dyrektywy 89/552/EWG oraz transmisje radiowe. Stwierdzono, że nie są usługami społeczeństwa informacyjnego, ponieważ nie są one świadczone na indywidualne żądanie, natomiast usługi przekazywane punkt-punkt, takie jak usługi wideo na żądanie lub przekazywanie informacji handlowych pocztą elektroniczną stanowią usługi społeczeństwa informacyjnego. Jednakże używanie poczty elektronicznej lub innych równorzędnych środków do przekazywania informacji indywidualnych np. przez osoby fizyczne działające poza zakresem ich działalności handlowej, gospodarczej lub zawodowej, łącznie z używaniem ich

w celu zawarcia umowy między tymi osobami, nie jest usługą społeczeństwa informacyjnego. Podobnie stosunek umowny między pracownikiem a jego pracodawcą nie jest usługą społeczeństwa informacyjnego. Nie są usługą społeczeństwa informacyjnego także działania, które ze względu na swój charakter nie mogą być wykonane na odległość lub drogą elektroniczną, takie jak ustawowa kontrola ksiąg rachunkowych lub konsultacja medyczna wymagająca fizycznego badania pacjenta (motyw 18 dyrektywy 2000/31).

Na gruncie rozporządzenia 2022/2065 o usługach cyfrowych (AUC) i rozporządzenia 2022/1925 o rynkach cyfrowych (ARC) przyjęto, że wszystkie usługi objęte regulacjami zawartymi w tych aktach prawnych należą do kategorii usług społeczeństwa informacyjnego. Jednakże niektóre z usług społeczeństwa informacyjnego opisane w AUC i ARC, ze względu zarówno na specyfikę, cel, sposób świadczenia, jak też zakres oddziaływania, wymagają szczegółowej regulacji. Potrzeba stworzenia szczegółowej regulacji dotyczy usług pośredników internetowych. Usługi pośrednictwa internetowego stanowią subkategorię usług społeczeństwa informacyjnego.

Potrzeba ochrony dóbr z zakresu własności intelektualnej legła u podstaw uregulowania zasad świadczenia i korzystania z usługi udostępniania treści online, przesądzając zarazem o wyodrębnieniu nowej kategorii usług cyfrowych. Warunki świadczenia tych usług i zasady ponoszenia odpowiedzialności przez dostawców operujących na rynku praw na dobrach niematerialnych zostały określone w dyrektywie 2019/790⁷⁷. Jako *ratio legis* dyrektywy wskazano, że ma ona przyczynić się do funkcjonowania rynku wewnętrznego, zapewniając wysoki poziom ochrony podmiotów uprawnionych, ułatwiając weryfikację praw i tworząc ramy, w których może odbywać się eksploatacja utworów i innych przedmiotów objętych ochroną (motyw 2 dyrektywy 2019/790). Rozporządzenia AUC i ARC zawierają reguły kolizyjne, co potwierdza nienaruszalność postanowień dyrektywy 2019/790. W motywie 11 AUC wskazano, że rozporządzenie pozostaje bez uszczerbku dla prawa Unii w zakresie prawa autorskiego i praw pokrewnych, w tym dyrektyw Parlamentu Europejskiego i Rady 2001/29/WE, 2004/48/WE i (UE) 2019/790, ustanawiających szczególne zasady i procedury, które powinny pozostać nienaruszone. Podobne postanowienie zostało zawarte w motywie 12 aktu o rynkach cyfrowych.

⁷⁷ Dyrektywa DSM.

Odrębną klasyfikację usług cyfrowych ze względu na cel identyfikowany jako zapewnienie bezpieczeństwa w cyberprzestrzeni zawiera dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. – NIS 2⁷⁸. W dyrektywie dokonano podziału usług na usługi kluczowe i usługi dostarczane przez „podmioty ważne”. Zauważono, że podmiot może jednocześnie spełniać kryteria bycia podmiotem kluczowym i podmiotem ważnym lub może jednocześnie prowadzić działania, z których jedne są objęte zakresem stosowania niniejszej dyrektywy, a inne są z niego wyłączone (motyw 21). Podmioty kluczowe i ważne powinny zapewniać bezpieczeństwo sieci i systemów informatycznych, których używają w swojej działalności, a także mieć obowiązki w zakresie zgłaszania incydentów bezpieczeństwa w cyberprzestrzeni i reagowania na nie. Komisji Europejskiej pozostawiono kompetencję do wskazywania podmiotów, w tym pośredników internetowych świadczących usługę bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych, które należą do kategorii „podmiotów ważnych”, a w konsekwencji podlegają obowiązkom wynikającym z dyrektywy 2022/2555 NIS 2. Komisja powinna ocenić, czy dostawcy objęci zakresem dyrektywy wyznaczeni jako bardzo duże platformy internetowe w rozumieniu art. 33 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 24 mogą zostać wskazani jako podmioty kluczowe na mocy niniejszej dyrektywy (motyw 140 dyrektywy NIS 2).

A. Usługi pośredników internetowych

Usługi pośrednictwa internetowego zostały zdefiniowane zarówno w Akcie o usługach cyfrowych, jak i w Akcie o rynkach cyfrowych, a zakresy tych aktów normatywnych się uzupełniają.

W Akcie o usługach cyfrowych (AUC) wymieniono w art. 3 pkt g trzy kategorie usług pośrednich, tj. 1) zwykły przekaz; 2) caching oraz 3) hosting,

⁷⁸ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.U. UE L Nr 333, s. 80).

wskazując, że każda z nich stanowi usługę pośrednictwa internetowego. Bez znaczenia pozostaje status usługodawcy i status usługobiorcy. Pośrednikiem internetowym może być zatem każdy podmiot niezależnie od formy organizacyjnoprawnej prowadzonej przez niego działalności i niezależnie od tego, czy działalność ta ma charakter zarobkowy, a nadto bez znaczenia pozostaje na czyją rzecz usługi są świadczone. Odbiorcą usługi może być zatem zarówno osoba fizyczna, jak i osoba prawna, a także jednostka organizacyjna nieposiadająca osobowości prawnej. Treść zawartej w AUC definicji nie przesądza o tym, czy korzystanie przez odbiorcę z usługi pośrednictwa wymaga zawarcia umowy. Jednakże ocena, czy konkretna usługa jest zwykłym przekazem, cachingiem lub hostingiem zależy od jej funkcji technicznych (które mogą się zmieniać) i musi być prowadzona w odniesieniu do każdego przypadku indywidualnie⁷⁹. W AUC wskazano podstawowe obowiązki mające zastosowanie do wszystkich dostawców usług pośrednich, a także dodatkowe obowiązki dostawców usług hostingu, w szczególności dostawców platform internetowych oraz bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych. Jeśli dostawcy usług pośrednich należą do kilku różnych kategorii z uwagi na charakter świadczonych usług i wielkość, powinni wypełniać wszystkie odpowiednie obowiązki wynikające z niniejszego rozporządzenia w odniesieniu do tych usług (motyw 41).

W akcie o rynkach cyfrowych (ARC) ustawodawca, w miejsce używanego w AUC terminu „usługi pośrednie”, operuje pojęciem „usługi pośrednictwa internetowego”. Definicja usług pośrednictwa ma charakter blankietowy i następuje poprzez odesłanie do art. 2 pkt 2 rozporządzenia (UE) 2019/1150⁸⁰.

⁷⁹ M. Piech, *Wyłączenie odpowiedzialności...*, s. 44.

⁸⁰ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1150 z dnia 20 czerwca 2019 r. w sprawie propagowania sprawiedliwości i przejrzystości dla użytkowników biznesowych korzystających z usług pośrednictwa internetowego (Dz.U. UE L Nr 186, s. 57).

Zgodnie z tym przepisem „usługi pośrednictwa internetowego” oznaczają usługi, które spełniają wszystkie (łącznie) następujące wymogi: a) stanowią usługi społeczeństwa informacyjnego w rozumieniu art. 1 ust. 1 lit. b) dyrektywy 2015/1535 Parlamentu Europejskiego i Rady; b) umożliwiają użytkownikom biznesowym oferowanie towarów lub usług konsumentom z zamiarem ułatwienia inicjowania transakcji bezpośrednich między tymi użytkownikami biznesowymi a konsumentami, niezależnie od tego, gdzie te transakcje są ostatecznie zawierane; c) są świadczone użytkownikom biznesowym na podstawie stosunków umownych między dostawcą tych usług a użytkownikami biznesowymi, którzy oferują towary lub usługi konsumentom.

Podstawą świadczenia usługi pośrednictwa internetowego w rozumieniu ARC jest stosunek umowny, przy czym jest to umowa zawarta między profesjonalistami (przedsiębiorcami), gdzie jedna ze stron (odbiorca usługi) pozostaje lub może pozostawać w stosunkach umownych z konsumentami. W myśl art. 2 pkt 3 ARC „dostawcą usług pośrednictwa internetowego” może być każda osoba fizyczna lub prawna, która świadczy usługi pośrednictwa internetowego lub oferuje ich świadczenie użytkownikom biznesowym⁸¹. Na potrzeby aktu o rynkach cyfrowych przyjęto, że usługi pośrednictwa są świadczone wyłącznie na potrzeby użytkowników biznesowych.

Konsekwencją powyższej regulacji było uwzględnienie usług pośrednictwa internetowego we wskazanym w art. 2 pkt 2 ARC pakiecie „podstawowych usług platformowych”. Usługi pośrednictwa internetowego uzyskały samodzielny status jako odrębna kategoria usług cyfrowych, podlegając zarazem bardziej szczegółowemu podziałowi na usługi: zwykłego przekazu (mere conduit), cachingu oraz hostingu. Należy jednocześnie poczynić spostrzeżenie, że mając na uwadze specyfikację usług cyfrowych zawartą w art. 2 pkt 2, termin „usługa pośrednictwa” uzyskał węższy zakres niż, używane na gruncie ARC, pojęcie podstawowych usług platformowych. Usługi pośrednictwa internetowego zostały bowiem uwzględnione w definicji podstawowych usług platformowych (motyw 14 ARC).

W literaturze wskazano, że mimo dużego zróżnicowania usług pośredników oraz odmiennych modeli biznesowych, na podstawie których prowadzą

⁸¹ Tamże, art. 2 pkt 1 i 2.

oni działalność, ich wspólną cechą jest służebny stosunek wobec treści pochodzących od użytkowników⁸².

a. USŁUGA ZWYKŁEGO PRZEKAZU

Usługa zwykłego przekazu jest usługą pośrednią i polega na „transmisji w sieci telekomunikacyjnej informacji przekazanych przez odbiorcę usługi lub na zapewnianiu dostępu do sieci telekomunikacyjnej” (art. 3 lit. g AUC). Zasady świadczenia usługi zwykłego przekazu, a także pozostałych usług pośrednich, do czasu wejścia w życie aktu o usługach cyfrowych, co nastąpi z dniem 17 lutego 2024 r., były uregulowane w dyrektywie o handlu elektronicznym (dyrektywa 2000/31), w szczególności w sekcji 4 w art. 12–15⁸³. Ustalenie charakteru świadczenia usługi zwykłego przekazu (mere conduit) następowało zatem na gruncie art. 12 dyrektywy 2000/31. Mając na uwadze, że – jak zauważono w literaturze – w rozporządzeniach cyfrowych (AUC i ARC) nie zmienia się ani opis istoty, ani prawna charakterystyka tych usług, ustalenia doktryny i orzecznictwa dokonywane na gruncie rozwiązań przyjętych w dyrektywie o handlu elektronicznym nie tracą aktualności. W AUC do usług pośrednich polegających na zwykłym przekazie zaliczono „generyczne kategorie usług, takie jak punkty wymiany ruchu internetowego, punkty dostępu bezprzewodowego, wirtualne sieci prywatne, usługi i resolwery DNS, rejestry nazw domen najwyższego poziomu, rejestratorzy, organy certyfikacji wydające certyfikaty cyfrowe, telefonia internetowa i inne usługi łączności interpersonalnej” (motyw 29 AUC).

Działanie polegające na zwykłym przekazie ma charakter czysto techniczny, automatyczny i bierny. Ponadto ani z innych przepisów dyrektywy 2000/31, ani z celów przez nią zamierzonych nie wynika, by zapewnianie dostępu do sieci telekomunikacyjnej powinno spełniać dodatkowe warunki, takie jak istnienie stosunku umownego między usługobiorcą a usługodawcą tej usługi lub ponoszenie przez usługodawcę nakładów reklamowych w celu

⁸² M. Piech, *Wprowadzenie*, [w:] *Pośrednicy internetowi...*

⁸³ Dyrektywa o handlu elektronicznym.

promowania wspomnianego świadczenia⁸⁴. Rola dostawcy sprowadza się co do zasady wyłącznie do pośredniczenia w uzyskaniu dostępu do sieci i w przekazaniu określonej informacji. W doktrynie stwierdza się, że istotą zwykłego przekazu jest bierny udział dostawcy usług sieciowych w transmisji danych za pośrednictwem sieci teleinformatycznej⁸⁵. Choć art. 12 odnosi się do zapewnienia połączenia i transmisji danych poprzez sieć telekomunikacyjną, uznaje się, że za zwykły przesył należy uznać zapewnianie takiej usługi także przy wykorzystaniu innych technologii, jak np. sieć bezprzewodowa (WLAN)⁸⁶.

Zapewnienie zwykłego przekazu oznacza jednak „niezakłóconą transmisję”, a zatem może generować po stronie dostawcy usługi obowiązki, w szczególności związane z zastosowaniem adekwatnych środków technicznych, które zabezpieczą transmisję przed zakłóceniami.

Na gruncie orzecznictwa TSUE (wcześniej ETS) należy stwierdzić, że na usługę zwykłego przekazu składają się dwa rodzaje czynności, tj. po pierwsze udzielenie dostępu do publicznej sieci teleinformatycznej (internet) oraz – po drugie – zapewnienie niezakłóconej transmisji danych lub informacji na żądanie odbiorcy usługi. TSUE stwierdził, że wykonanie pierwszego z obowiązków może zostać objęte sądowym nakazem⁸⁷. Nakaz ten wymaga od dostawcy, pod rygorem grzywny, udzielenia dostępu do sieci telekomunikacyjnej pozwalającej ogółowi na łączenie się z internetem i uniemożliwienia osobom trzecim publicznego udostępniania za pomocą tego łącza internetowego określonego utworu lub jego części chronionych prawem autorskim, w tym do pobierania poprzez internetową giełdę wymiany (peer-to-peer), gdy dostawca ten ma wybór co do tego, jakich środków technicznych użyć, aby zastosować się do tego nakazu, nawet jeśli wybór ten ogranicza się do jednego środka polegającego na zabezpieczeniu łącza internetowego hasłem, o ile użytkownicy tej sieci są zobowiązani ujawnić swoją tożsamość w celu uzyskania wymaganego hasła i nie mogą zatem działać anonimowo, czego sprawdzenie należy do sądu odsyłającego⁸⁸.

⁸⁴ Wyrok TS w sprawie Tobias McFadden przeciwko Sony Music Entertainment Germany GmbH.

⁸⁵ M. Piech, *Zwykły przekaz*, [w:] *Pośrednicy internetowi...*, s. 156.

⁸⁶ Tamże, s. 157.

⁸⁷ Wyrok TS w sprawie Tobias Mc Fadden przeciwko Sony Music Entertainment Germany GmbH, pkt 5 sentencji.

⁸⁸ Tamże.

Niewykonanie przez dostawcę usługi mere conduit obowiązku zapewnienia użytkownikom internetu dostępu do sieci internetowej rodzi ryzyko naruszenia przez dostawcę praw podstawowych, w tym art. 11 KPP gwarantującego wolność wypowiedzi i informacji. TSUE zauważył, że wykonanie nakazu udzielenia dostępu do sieci skutkuje ograniczeniem swobody prowadzenia działalności gospodarczej dostawcy takiej usługi. W wyroku w sprawie Tobias McFadden przeciwko Sony Music TSUE wskazuje, że:

w tym względzie z uwagi na to, że z jednej strony taki nakaz jest obwarowany wobec wspomnianego dostawcy dostępu przymusem, który może mieć wpływ na prowadzoną przez niego działalność gospodarczą, a z drugiej strony nakaz ten może ograniczyć przysługującą odbiorcom takiej usługi swobodę korzystania z dostępu do Internetu, narusza on prawo dostawcy do wolności prowadzenia działalności gospodarczej, chronione na mocy art. 16 Karty praw podstawowych Unii Europejskiej, oraz prawo odbiorców do wolności informacji, której ochrona jest zapewniona przez art. 11 karty. Gdy zaś kilka praw podstawowych chronionych prawem Unii konkuruje ze sobą, na danym organie lub sądzie krajowym spoczywa obowiązek zadbania o to, by zapewnić odpowiednią równowagę pomiędzy tymi prawami⁸⁹.

Trybunał weryfikował, czy zabezpieczenie dostępu do łącza internetowego hasłem, co wymagałoby od odbiorcy usługi ujawnienia jego tożsamości stanowi nieproporcjonalną ingerencję w prawa podstawowe, w tym prawo do anonimowej wypowiedzi. Dokonując ważenia interesów, tj. interesu uprawnionego z tytułu praw wyłącznych do utworu oraz prawa do nieanonimowej wypowiedzi użytkownika internetu, a także biorąc pod uwagę nakaz adresowany do dostawcy usługi polegający na zapewnieniu dostępu do sieci, Trybunał stwierdził, że niezabezpieczenie łącza internetowego prowadziłoby do pozbawienia prawa podstawowego do własności intelektualnej wszelkiej ochrony, co byłoby sprzeczne z koncepcją odpowiedniej równowagi. W tych okolicznościach środek mający na celu zabezpieczenie łącza internetowego

⁸⁹ Tamże.

hasłem należy uznać za konieczny w celu zapewnienia skutecznej ochrony prawa podstawowego do ochrony własności intelektualnej⁹⁰.

Wyrok ETS z dnia 15 września 2016 r. Tobias McFadden przeciwko Sony Music Entertainment zapoczątkował zmianę podejścia do ustalania zakresu i interpretacji obowiązków pośredników internetowych. Za niewystarczające uznano bowiem bierne zachowanie się pośrednika świadczącego usługę zwykłego przesyłu, oczekując, by zapewnił on środki pozwalające na ochronę przed zakłóceniami transmisji. Wraz z upływem czasu, jak słusznie zauważył M. Polański, obserwować można było stopniowe przekształcanie modelu odpowiedzialności pośredników w kierunku stopniowego wprowadzania nakazu aktywnego filtrowania przesyłanych i przechowywanych danych⁹¹. Przykładem jest wprowadzony przez Francję obowiązek odcinania dostępu do internetu internautom, którzy zostali trzykrotnie poinformowani o fakcie naruszenia przez nich prawa autorskiego (tzw. ustawa HADOPI)⁹².

Rozwiązania zawarte w AUC dowodzą, że pośrednicy świadczący usługę zwykłego przekazu podlegać będą takim samym obowiązkom, w szczególności wymogom należytej staranności, jakie są adresowane do pozostałych pośredników internetowych. O ile zatem – jak wskazano w motywie 30 AUC – żadnego z przepisów rozporządzenia nie należy interpretować jako nałożenia ogólnego obowiązku monitorowania ani ogólnego obowiązku aktywnego ustalania faktów, ani też jako nałożenia na dostawców ogólnego obowiązku podejmowania aktywnych działań w odniesieniu do nielegalnych treści, to jednak stosowanie takich środków nie tylko jest dozwolone, ale ponadto może

⁹⁰ Tamże.

⁹¹ P.P. Polański, *Odpowiedzialność prawna za treści rozpowszechniane w Internecie*, Warszawa 2012, s. 21.

⁹² Ustawa z dnia 28 października 2009 r. dotycząca ochrony karnej własności literackiej i artystycznej w Internecie, znana jako „Hadopi 2”, <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000021208046> (dostęp: 4.09.2023), przyznaje organowi l'Arcom (wcześniej: HADOPI) zgodę na wysyłanie ostrzeżeń do zainteresowanych abonentów internetu w przypadku wykrycia faktów, które mogą stanowić naruszenie nałożonego na wszystkich abonentów obowiązku zapewnienia zgodnego z prawem korzystania z dostępu do internetu. Powiadomieni przez Hadopi abonenci, których dostęp mimo to jest nadal kilkakrotnie wykorzystywany do popełnienia aktów naruszenia, mogą zostać skazani przez sąd karny na karę grzywny do 1500 euro oraz zawieszenie dostępu do internetu (*Presentation*, HADOPI, <https://www.hadopi.fr/organisation/presentation>, dostęp: 4.09.2023).

być powoływane przez dostawcę usługi na potwierdzenie dochowania przez niego wymogów należytej staranności.

b. CACHING

Caching stanowi usługę automatycznego, pośredniego i krótkotrwałego przechowywania transmitowanej informacji, dokonywanego wyłącznie w celu usprawnienia lub lepszego zabezpieczenia późniejszej transmisji informacji na żądanie innych odbiorców usługi. Sposób, w jaki usługa cachingu została opisana w art. 5 ust. 1 AUC, odpowiada także treści art. 13 ust. 1 dyrektywy 2000/31. Na gruncie prawa autorskiego, w tym dyrektywy 2019/790⁹³ oraz dyrektywy 2001/29⁹⁴, równoległe z terminem caching stosuje się pojęcie browsing. Browsing oznacza przejściowe zwielokrotnianie utworów, które następuje w toku przeglądania materiałów zamieszczonych w sieci. Caching – krótkotrwałe i czasowe zapisywanie i magazynowanie zwielokrotnionych utworów w podręcznej pamięci komputera w celu przyspieszenia ponownego dostępu⁹⁵. Przykłady usług pośrednich polegających na cachingu obejmują wyłącznie zapewnianie dostarczania treści, odwrotnych serwerów proxy lub serwerów proxy adaptacji treści. Takie usługi mają kluczowe znaczenie dla zapewnienia sprawnej i efektywnej transmisji informacji dostarczanych w internecie (motyw 29 AUC).

Usługa cachingu ma charakter akcesoryjny w stosunku do transmisji danych⁹⁶.

⁹³ Dyrektywa DSM.

⁹⁴ Dyrektywa 2001/29/WE Parlamentu Europejskiego i Rady z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym (Dz.U. UE L Nr 167, s. 10 z późn. zm.).

⁹⁵ Z. Zawadzka, *Tymczasowe zwielokrotnianie utworu*, [w:] *Prawo własności intelektualnej. Teoria i praktyka*, J. Sieńczyło-Chłabcz (red.), Warszawa 2021, s. 221.

⁹⁶ M. Piech, *Wyłączenie odpowiedzialności...*, s. 44.

C. HOSTING

Usługa hostingu może być wykonywana w dwojaki sposób, tj. albo jako usługa realizująca funkcję infrastruktury, albo jako usługa platformy internetowej, która obok funkcji infrastruktury realizuje funkcję publicznego rozpowszechniania treści (motyw 13 AUC).

Wprowadzenie w AUC pojęcia publicznego rozpowszechniania jako podstawy wyróżnienia w ramach hostingu usługi platform internetowych oraz wyodrębnienie tej subkategorii ma znaczenie praktyczne i pozwala na bardziej precyzyjne ustalenie mechanizmu ponoszenia odpowiedzialności przez te podmioty⁹⁷. Inne zatem zasady ponoszenia odpowiedzialności należy zastosować od usługodawców świadczących usługi hostingu, a inne do usługodawców świadczących usługę platformy internetowej. Nadal jednak usługa platformy internetowej mieści się w pojęciu hostingu, stanowiąc podkategorię tej usługi. Przykładowe usługi hostingu obejmują także kategorie usług takie jak przetwarzanie w chmurze, web hosting, odpłatne usługi odsyłania czy usługi umożliwiające wymianę informacji i treści online, w tym przechowywanie i udostępnianie plików (motyw 29 AUC). Usługi te, o ile pełnią funkcję infrastruktury, np. jako podstawa infrastruktury do świadczenia usług przechowywania i przetwarzania danych w aplikacji internetowej, na stronie lub na platformie internetowej, same w sobie nie powinny być postrzegane jako publiczne rozpowszechnianie informacji przechowywanych lub przetwarzanych na żądanie odbiorcy aplikacji, strony lub platformy internetowej, dla której jest ona hostem.

Pojęcie publicznego rozpowszechniania powinno obejmować udostępnianie informacji potencjalnie nieograniczonej liczbie osób, czyli zapewnienie łatwego dostępu do informacji ogółowi odbiorców usługi bez konieczności podejmowania dalszych działań przez odbiorcę usługi zapewniającej te informacje, niezależnie od tego, czy osoby te faktycznie korzystają z dostępu do tych informacji. W związku z tym w przypadku, gdy dostęp do informacji wymaga rejestracji lub dopuszczenia do udziału w grupie odbiorców usługi, informacje te należy uznawać za publicznie rozpowszechniane jedynie wtedy, gdy odbiorcy usługi poszukujący dostępu do informacji są

⁹⁷ Tamże, s. 44.

automatycznie rejestrowani lub dopuszczani do udziału w grupie odbiorców usługi bez konieczności podejmowania decyzji lub dokonywania wyboru przez człowieka co do tego, komu przyznać taki dostęp. Usługi łączności interpersonalnej zgodnie z definicją w dyrektywie Parlamentu Europejskiego i Rady (UE) 2018/1972²⁴, takie jak poczta elektroniczna lub usługi przesyłania wiadomości prywatnych, nie są objęte definicją platform internetowych, ponieważ są one wykorzystywane w celu łączności interpersonalnej między ograniczoną liczbą osób określoną przez nadawcę komunikatu. Określone w niniejszym rozporządzeniu obowiązki dostawców platform internetowych mogą jednak mieć zastosowanie do usług, które umożliwiają udostępnianie informacji potencjalnie nieograniczonej liczbie odbiorców, nieokreślonej przez nadawcę komunikatu, np. poprzez publiczne grupy lub otwarte kanały. Informacje należy uznawać za publicznie rozpowszechniane w rozumieniu niniejszego rozporządzenia wyłącznie wówczas, gdy rozpowszechnianie ma miejsce na bezpośrednie żądanie odbiorcy usługi, który przekazał te informacje (motyw 14 AUC).

Usługę hostingu wykonywaną w łączności z publicznym rozpowszechnieniem informacji należy odróżnić od sytuacji, w której dostawca usługi uczestniczy aktywnie w generowaniu, moderowaniu i kształtowaniu rozpowszechnianych treści. W wyroku ETS z dnia 11 września 2014 r. w sprawie *Sotiris Papasavvas przeciwko O Fileleftheros Dimosia Etaireia Ltd.*⁹⁸ Trybunał ustalał, czy spółka będąca wydawcą prasowym dysponująca stroną internetową, na której publikowana jest elektroniczna wersja dziennika redagowanego przez zatrudnionych tam albo niezależnych dziennikarzy, przy czym spółka ta ponadto otrzymuje wynagrodzenie z przychodów z reklam handlowych emitowanych na tej stronie, ma status pośrednika, a zatem, czy w stosunku do takiej spółki będącej wydawcą tytułu prasowego mogą znaleźć zastosowanie wyłączenia odpowiedzialności wskazane w art. 12–14 dyrektywy 2000/3. Trybunał wskazał, że wyłączenia mogą zostać zastosowane tylko wówczas, gdy zachowanie usługodawcy ogranicza się do zachowania „usługodawcy będącego pośrednikiem”⁹⁹. Ustanowione w dyrektywie (obecnie powtórzone

⁹⁸ Wyrok TS w sprawie *Sotiris Papasavvas przeciwko O Fileleftheros Dimosia Etaireia Ltd.*

⁹⁹ Tamże, pkt 39.

w art. 4–6 AUC) wyłączenia w dziedzinie odpowiedzialności obejmują jedynie przypadki, w których działalność podmiotu świadczącego usługi społeczeństwa informacyjnego przybiera charakter czysto techniczny, automatyczny i bierny, który zakłada, że wspomniany podmiot nie posiada wiedzy o przekazywanych lub przechowywanych informacjach ani kontroli nad nimi¹⁰⁰. W celu sprawdzenia, czy odpowiedzialność podmiotu świadczącego usługę mogłaby zostać ograniczona na podstawie art. 14 dyrektywy 2000/31, należy zbadać, czy rola tego podmiotu jest neutralna, czyli jego zachowanie ma charakter czysto techniczny, automatyczny i bierny, co oznacza brak jego wiedzy o przechowywanych informacjach i brak nad nimi kontroli¹⁰¹. Na ustalenie statusu pośrednika nie ma natomiast wpływu okoliczność, czy dostawca pobiera za wykonanie usługi wynagrodzenie. Przesłanka istnienia albo braku odpłatności za usługę jest indyferentna i nie przesądza o dopuszczalności albo jej braku zastosowania wyłączenia odpowiedzialności wskazanych w art. 12–14 dyrektywy 2000/31. Sama okoliczność, iż usługa odsyłania jest odpłatna, że usługodawca określa warunki płatności czy udziela on klientom informacje o charakterze ogólnym, nie może skutkować pozbawieniem tego podmiotu możliwości skorzystania z przewidzianych w dyrektywie 2000/31/WE wyłączeń w dziedzinie odpowiedzialności¹⁰². Istotna jest natomiast rola odgrywana przez podmiot świadczący usługi przy sporządzaniu przekazu reklamowego towarzyszącego linkowi reklamowemu lub przy określaniu i wyborze słów kluczowych. Podobnie jeżeli podmiot świadczący usługi udziela wsparcia, które polega w szczególności na optymalizacji prezentacji danych ofert sprzedaży lub na ich promocji, należy stwierdzić, że nie zachowuje on neutralnej pozycji między danym klientem (sprzedającym) a potencjalnymi nabywcami, lecz odgrywa czynną rolę, która może pozwolić mu na powzięcie wiedzy o danych dotyczących poszczególnych ofert lub na sprawowanie nad nimi kontroli¹⁰³. W konsekwencji w przypadku, gdy spółka będąca wydawcą prasowym publikującym na swojej stronie internetowej elektroniczną wersję dziennika ma co do zasady wiedzę na temat publikowanych przez siebie informacji i sprawuje

¹⁰⁰ Wyrok TS w sprawach połączonych Google France i Google, pkt 113.

¹⁰¹ Tamże, pkt 114; a także Wyrok TS w sprawie L'Oréal przeciwko eBay, pkt 113.

¹⁰² Wyrok TS w sprawie Sotiris Papasavvas przeciwko O Fileleftheros Dimosia Etaireia Ltd., pkt 42.

¹⁰³ Wyrok TS w sprawie L'Oréal przeciwko eBay, pkt 113.

nad nimi kontrolę, nie powinna być uznana za usługodawcę będącego pośrednikiem w rozumieniu art. 12–14 dyrektywy 2000/31, niezależnie od tego, czy dostęp do strony jest odpłatny. Ostatecznie prowadziło to Trybunał do wyrażenia stanowiska, zgodnie z którym:

ograniczenia odpowiedzialności cywilnej, o których mowa w art. 12–14 dyrektywy 2000/31, nie dotyczą spółki będącej wydawcą prasowym, dysponującym stroną internetową, na której publikowana jest elektroniczna wersja dziennika, przy czym spółka ta ponadto otrzymuje wynagrodzenie z przychodów z reklam handlowych emitowanych na tej stronie, w przypadku gdy ma ona wiedzę o publikowanych informacjach i sprawuje nad nimi kontrolę, niezależnie od sytuacji, czy gdy dostęp do strony jest odpłatny¹⁰⁴.

Stanowisko zbieżne z orzecznictwem ETS wyrażały sądy krajowe na gruncie art. 12–15 ustawy o świadczeniu usług drogą elektroniczną¹⁰⁵. Okoliczność, że podmioty świadczące usługi hostingu – podobnie jak podmioty umożliwiające sprawny dostęp do portali internetowych – tylko pośredniczą w udostępnianiu drogą elektroniczną treści pochodzących od osób trzecich, rzutuje na ukształtowanie zasad ich odpowiedzialności za naruszenie praw podmiotowych osób trzecich lub naruszenie obowiązujących przepisów prawa w związku z treścią przechowywanych danych. W świetle art. 12–15 ustawy z 2002 r. o świadczeniu usług drogą elektroniczną podmioty pośredniczące są zwolnione z odpowiedzialności cywilnoprawnej, administracyjnej oraz karnej za zawartość udostępnionych materiałów, nie są one – zgodnie z art. 15 pow. ustawy – zobowiązane do sprawdzania (monitorowania) przekazywanych, przechowywanych lub udostępnianych danych. Niewiedza o treści udostępnionych informacji jest zasadniczym warunkiem uchylenia odpowiedzialności tych podmiotów¹⁰⁶. Zarazem jednak uzyskanie wiedzy przez administratora o zamieszczeniu pod artykułem komentarzy naruszających

¹⁰⁴ Wyrok TS w sprawie Sotiris Papasavvas przeciwko O Fileleftheros Dimosia Etai-
reia Ltd.

¹⁰⁵ Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną
(t.j. Dz.U. z 2020 r., poz. 344).

¹⁰⁶ Wyrok SA w Łodzi z dnia 13 stycznia 2017 r., I ACa 884/16, LEX nr 2250053.

dobra osobiste osób trzecich jest wystarczającą przesłanką zaktualizowania się jego odpowiedzialności¹⁰⁷.

Usługa hostingu (obok zwykłego przekazu i cachingu) jest usługą pośrednictwa internetowego i została wskazana jako jedna z „podstawowych usług platformowych” wymienionych w art. 2 pkt 2 ARC. Kategorię podstawowych usług platformowych wyodrębniono ze względu na szczególne cechy tych usług wynikające przede wszystkim z faktu, że są one świadczone przez bardzo duże platformy internetowe i bardzo duże wyszukiwarki internetowe w rozumieniu art. 33 ust. 1 AUC (strażnicy dostępu). Podstawowe usługi platformowe zostały zatem wyodrębnione przede wszystkim ze względu na kryterium podmiotowe, co oznacza, że chodzi o usługi cyfrowe świadczone przez strażników dostępu. Są to wysoce skoncentrowane, wielostronne usługi, w przypadku których jedna duża platforma cyfrowa lub bardzo ograniczona liczba dużych platform cyfrowych ustala warunki handlowe, mając w tym zakresie znaczną autonomię. Mogą być świadczone także w ten sposób, że kilka dużych platform cyfrowych pełni funkcję punktów dostępu umożliwiających użytkownikom biznesowym dotarcie do konsumentów i odwrotnie. Uprawnienia strażnika dostępu takich dużych platform cyfrowych są często nadużywane, co przejawia się nieuczciwym postępowaniem wobec ekonomicznie zależnych użytkowników biznesowych i konsumentów¹⁰⁸. Podstawowe usługi platformowe mają następujące cechy: ekstremalne korzyści skali, które często wynikają z niemal zerowych kosztów krańcowych pozyskiwania użytkowników biznesowych lub użytkowników końcowych. Inne cechy podstawowych usług platformowych to bardzo silne efekty sieciowe, zdolność łączenia wielu użytkowników biznesowych z wieloma użytkownikami końcowymi dzięki wielostronności tych usług, znaczny stopień zależności zarówno użytkowników biznesowych, jak i użytkowników końcowych, efekty uzależnienia od jednego dostawcy, brak stosowania przez użytkowników końcowych multihomingu do tego samego celu, integracja pionowa oraz zalety oparte na danych¹⁰⁹.

¹⁰⁷ Wyrok SN z dnia 22 września 2020 r., I CSK 632/18, LEX nr 3060767.

¹⁰⁸ Wniosek AUC, s. 2.

¹⁰⁹ Motyw 2 ARC.

Do podstawowych usług platformowych należą, obok usług pośrednictwa internetowego:

1. wyszukiwarki internetowe,
2. internetowe serwisy społecznościowe,
3. usługi platformy udostępniania wideo,
4. e-usługi łączności interpersonalnej niewykorzystujące numerów,
5. systemy operacyjne,
6. przeglądarki internetowe,
7. wirtualni asystenci,
8. usługi przetwarzania w chmurze,
9. internetowe usługi reklamowe, w tym sieci reklamowe, giełdy reklamowe i inne usługi pośrednictwa w zakresie reklam, świadczone przez przedsiębiorstwo, które świadczy dowolne podstawowe usługi platformowe (art. 2 pkt 2 ARC).

Platformy internetowe, takie jak serwisy społecznościowe, platformy udostępniania treści lub internetowe platformy handlowe, zostały zdefiniowane jako dostawcy usług hostingu, którzy nie tylko przechowują informacje przekazane przez odbiorców usługi na ich żądanie, ale także rozpowszechniają publicznie te informacje, ponownie na ich żądanie (motyw 13 AUC).

Kryterium kwalifikowania do kategorii dostawców platform internetowych nie zawsze stanowi publiczne rozpowszechnianie treści. Nie będą do tej kategorii kwalifikowani pośrednicy świadczący usługę hostingu, nawet jeśli ze świadczeniem tej usługi jest połączone publiczne rozpowszechnianie treści, o ile hosting jest zaledwie nieznaczną i wyłącznie poboczną funkcją innej usługi (motyw 13 AUC). Obejmuje to zatem sytuacje, kiedy funkcji publicznego rozpowszechniania, z obiektywnych względów technicznych, nie można wykorzystywać bez usługi hostingu, a włączenie takiej funkcji nie jest sposobem na obejście stosowania przepisów rozporządzenia mających zastosowanie do platform internetowych. Taką funkcję może stanowić sekcja gazety internetowej przeznaczona na komentarze, w przypadku której jest oczywiste, że ma ona charakter poboczny w stosunku do głównej usługi, jaką jest publikowanie wiadomości, za które odpowiedzialność redakcyjną ponosi wydawca¹¹⁰.

¹¹⁰ Motyw 13 AUC.

Podsumowując, jeśli usługa hostingu, w podstawowym kształcie oznacza funkcję przechowywania, to w połączeniu z inną usługą (publicznego rozpowszechniania) lub ze względu na kategorię podmiotu świadczącego tę usługę (strażnicy dostępu) albo szczególną cechę usługi (podstawowe usługi platformowe) będzie ona odmiennie kategoryzowana, co powoduje, że do oceny sytuacji prawnej dostawcy będą znajdować zastosowanie odmiennie regulacje prawne zawarte w innych aktach prawnych.

d. USŁUGA WYSZUKIWARKI INTERNETOWEJ

Zgodnie z art. 3 lit. j AUC usługa wyszukiwarki internetowej to usługa cyfrowa, która umożliwia użytkownikom wprowadzanie zapytań w celu wyszukiwania, co do zasady, wszystkich stron internetowych lub wszystkich stron internetowych w danym języku za pomocą zapytania na jakikolwiek temat przez podanie słowa kluczowego, zapytania głosowego, wyrażenia lub innej wartości wejściowej, i która podaje wyniki wyszukiwania w dowolnym formacie, w którym można znaleźć informacje związane z zadaniem zapytaniem. Definicję wyszukiwarki internetowej zaczerpnięto¹¹¹ z rozporządzenia 2019/1150 z 20 czerwca 2019 r. w sprawie propagowania sprawiedliwości i przejrzystości dla użytkowników biznesowych korzystających z usług pośrednictwa internetowego¹¹². Usługa wyszukiwarki została zaliczona do pakietu podstawowych usług platformowych jako usługa, która może „mieć wpływ zarówno na dużą liczbę użytkowników końcowych, jak i na przedsiębiorstwa, co pociąga za sobą ryzyko nieuczciwych praktyk biznesowych” (motyw 13 ARC).

Usługa wyszukiwarki internetowej nazwana jest w orzecznictwie usługą odpłatnego odsyłania¹¹³. W opinii Rzecznika Generalnego UE podmiot świadczący usługę odpłatnego odsyłania nie może być uznany za świadczącego usługę społeczeństwa informacyjnego polegającą na przechowywaniu informacji przekazanych przez usługobiorcę w rozumieniu art. 14 dyrektywy

¹¹¹ M. Piech, *Wyłączenie odpowiedzialności...*, s. 44.

¹¹² Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1150 z dnia 20 czerwca 2019 r. w sprawie propagowania sprawiedliwości i przejrzystości dla użytkowników biznesowych korzystających z usług pośrednictwa internetowego, (Dz.U. L Nr 186, s. 57).

¹¹³ Wyrok TS w sprawach połączonych Google France i Google.

2000/31/WE z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym)¹¹⁴.

Usługa wyszukiwarki nie stanowi zatem usługi hostingu. M. Piech zauważa, że AUC, choć w motywie 28 wymienia usługę wyszukiwarki wśród nowych rodzajów usług pośrednich, nie zawiera przepisów normatywnych ani wskazówek interpretacyjnych co do kategorii usług pośrednich, do których należałoby przypisać wyszukiwarkę. Prawodawca unijny pozostawił więc bez rozstrzygnięcia kwestie warunków wyłączenia odpowiedzialności i obowiązków będących wyrazem działania dostawcy wyszukiwarki z należytą starannością¹¹⁵.

Czynność wpisywania słów kluczowych w wyszukiwarce internetowej stała się częścią naszej kultury, a jej wyniki są nam natychmiast znane. Natomiast mechanizm wewnętrzny, w jaki sposób generowane są rezultaty, rzecz można, pozostaje dla większej części społeczeństwa nieznany¹¹⁶. Rzecznik Generalny UE wyraził pogląd, że wyszukiwarka Google nie jest niczym więcej niż narzędziem¹¹⁷. Stanowisko to jest wyrazem przekonania o całkowicie neutralnej i zautomatyzowanej metodzie działania wyszukiwarki. Korzystanie z tego narzędzia nie może uzasadniać zarzutu pod adresem dostawcy usługi dotyczącego wprowadzania w błąd użytkowników, a tym bardziej zarzutu manipulowania opinią publiczną. W opinii w połączonych sprawach ze skargi Google przeciwko podmiotom domagającym się ochrony praw własności intelektualnej, w szczególności znaków towarowych¹¹⁸, Rzecznik stwierdził,

¹¹⁴ Opinia Rzecznika Generalnego M. Poiaresa Madura przedstawiona w dniu 22 września 2009 r., sprawy połączone C-236/08, C-237/08 i C-238/08 Google France Google Inc. przeciwko Louis Vuitton Malletier; Google France przeciwko Viaticum Luteciel; Google France przeciwko CNRRH, Pierre'owi-Alexisowi Thonetowi, Brunonowi Raboinowi Tiger, francyzobiorca Unicis, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=73281&pageIndex=0&doclang=PL&mode=lst&dir=&occ=first&part=1&cid=1323044> (dostęp: 17.08.2023).

¹¹⁵ M. Piech, *Wyłączenie odpowiedzialności...*, s. 44.

¹¹⁶ Opinia Rzecznika Generalnego M. Poiaresa Madura...

¹¹⁷ Tamże, pkt 1.

¹¹⁸ Sprawy te dotyczyły trzech wniosków o wydanie orzeczenia w trybie prejudycjalnym złożonych przez francuski Cour de cassation (francuski sąd najwyższy), których przedmiotem jest system ogłoszeń spółki Google, „AdWords”. Spółka Google eksploatuje również system reklam zwany „AdWords”, który umożliwia wyświetlanie reklam jako odpowiedź na słowa kluczowe obok naturalnych rezultatów. Reklamy zazwyczaj składają się z krótkiego przekazu reklamowego oraz linku do strony reklamodawcy; różnią się one

że „związek, jaki ustanawia pomiędzy słowami kluczowymi zbieżnymi ze znakami towarowymi a naturalnymi rezultatami, nawet w przypadku najbardziej trafnych stron, nie jest wystarczający do wprowadzenia w błąd. Internauci mogą wyrobić sobie zdanie co do pochodzenia towarów lub usług oferowanych na tych stronach dopiero po przeczytaniu ich opisu, a ostatecznie, przez wyjście z wyszukiwarki Google i wejście na te strony”¹¹⁹. W opinii Rzecznika internet funkcjonuje bez jakiegokolwiek centralnej kontroli i być może to stanowi klucz do jego rozwoju i powodzenia: jest on całkowicie zależny od treści wprowadzanych do niego swobodnie przez poszczególnych użytkowników. Słowa kluczowe są jednym z instrumentów, jeśli nie głównym, za pomocą którego informacje te zostają zorganizowane i udostępnione internautom. Wobec powyższego słowa kluczowe są same w sobie treściowo neutralne: umożliwiają one internautom dotarcie do stron powiązanych z takimi słowami. Istnienie wielu z tych stron jest całkowicie uzasadnione i zgodne z prawem, nawet jeżeli nie są to strony uprawnione do znaku towarowego¹²⁰.

Z opinią Rzecznika Generalnego nie sposób się zgodzić. Jak zauważono w literaturze, mechanizm działania wyszukiwarki należy opisać, odwołując się do trzech narzędzi: szperacza, indeksu oraz systemu wykonawczego¹²¹. A. Dziekan-Łanucha opisuje mechanizm działania wyszukiwarek następująco: „Szperacze to specjalistyczne programy, nazywane inaczej robotami sieciowymi, pajakami albo botami indeksującymi, które metodycznie przeszukują sieć WWW, nieustannie odwiedzają strony internetowe, zbierając informacje

od naturalnych rezultatów tym, że są zaprezentowane w rubryce „linki komercyjne” u góry strony na żółtym tle albo po prawej stronie. Główni konkurenci spółki Google (Microsoft i Yahoo!) eksploatują podobne systemy reklamowe. Poprzez system AdWords spółka Google umożliwia reklamodawcom dokonanie wyboru słów kluczowych, co powoduje, że ich reklamy wyświetlają się internautom jako odpowiedź na wprowadzenie tych słów kluczowych do wyszukiwarki Google. Za każde kliknięcie linku reklamy przez internautę spółka Google otrzymuje wynagrodzenie zgodnie z wcześniej uzgodnioną ceną („cena za kliknięcie”). Nie ma żadnych ograniczeń co do liczby reklamodawców, którzy mogą wybrać dane słowo kluczowe, a jeżeli nie wszystkie reklamy związane ze słowem kluczowym mogą zostać wyświetlone w tym samym czasie, to są one ustawiane w kolejności wynikającej z ceny za kliknięcie oraz liczby wcześniejszych kliknięć danego linku reklamy przez internautów (Zob. Opinia Rzecznika Generalnego M. Poiaresa Madura..., pkt 10–11.

¹¹⁹ Tamże, pkt 89.

¹²⁰ Tamże, pkt 110.

¹²¹ A. Dziekan-Łanucha, *Od personalizacji do profilowania. Opis konsekwencji korzystania z wyszukiwarki internetowej Google*, „Studia Socialia Cracoviensia” 2016, nr 1, s. 123.

o ich zawartości, a następnie odsyłają te informacje do indeksu, czyli gigantycznej bazy danych. W indeksie następuje takie opracowanie gromadzonych informacji, aby poszczególne adresy URL (czyli w uproszczeniu poszczególne strony internetowe) były kojarzone z określonymi słowami kluczowymi. Następnie takie dane ulegają przekształceniu, a dokładniej odwróceniu: tworzy się listę słów, które odpowiadają konkretnym adresom URL. Kiedy zatem użytkownik wyszukiwarki wpisze jakieś słowo kluczowe, otrzyma spis adresów URL wszystkich stron, na których to słowo się znajduje”¹²².

Założeniem Google było uporządkowanie internetowych zasobów informacji. Google nie ujawnia szczegółowych kryteriów wyszukiwania, są chronione tajemnicą firmy¹²³. Wyniki pojawiające się w rezultatach wyszukiwania mają odpowiadać oczekiwaniom użytkownika. Google zatem dostosowuje rezultaty wyszukiwania do indywidualnych potrzeb każdego z użytkowników¹²⁴. Aktywność internetowa użytkowników po przeanalizowaniu jej przez odpowiednie wykorzystywane przez Google programy daje podstawy do podsuwania odpowiednich dla niego wyników wyszukiwania¹²⁵. Zjawisko zamykania internautów w świecie własnych zainteresowań, poglądów, wiedzy zostało nazwane bardziej obrazowo zjawiskiem bańki filtrowej (bańki informacyjnej)¹²⁶. Zjawisko to wywołane dążeniem do dostarczania informacji dostosowanych do indywidualnych potrzeb zakończyło etap jednego i wspólnego dla wszystkich internetu. Obecnie mamy do czynienia ze spersonalizowanym internetem¹²⁷. Spersonalizowane świadczenie usługi wyszukiwarki internetowej polegające na wyświetleniu użytkownikom internetu odmiennych rezultatów w wynikach wyszukiwania ze względu na stworzone przez usługodawcę profile¹²⁸ tych użytkowników, pomimo że używali oni tych samych

¹²² Tamże, s. 124.

¹²³ W. Orliński, *Internet. Czas się bać*, Warszawa 2013, s. 72.

¹²⁴ A. Dziekan-Łanucha, *Od personalizacji...*, s. 126.

¹²⁵ Tamże, s. 126.

¹²⁶ E. Pariser, *The filter bubble: what the Internet is hiding from you*, Nowy Jork 2011; cyt. za: A. Dziekan-Łanucha, *Od personalizacji...*, s. 127.

Tamże, s. 126.

¹²⁷ Tamże, s. 127.

¹²⁸ Profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów jej pracy, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji,

słów kluczowych, stanowi ograniczenie dostępu do informacji, a w konsekwencji narusza swobodę przepływu informacji i wolność wypowiedzi.

Działalność wyszukiwarek internetowych wykorzystujących profilowanie jako warunek świadczenia usługi stanowi nowy typ ingerencji w wolność wypowiedzi. Stosowana przez dostawców wyszukiwarek internetowych metoda świadczenia usługi prowadzi do ograniczenia wyników wyszukiwania, porządkowania ich według nieznanych odbiorcy usługi kryteriów, a w konsekwencji dyskryminacji w dostępie do informacji ze względu na posiadane przez użytkownika cechy osobiste, zainteresowania oraz jego aktywność w internecie.

Dostawca usługi wyszukiwarki internetowej nie tylko ma status pośrednika internetowego, ale jest także administratorem danych osobowych w rozumieniu art. 4 pkt 7 RODO¹²⁹. Świadczenie usługi wyszukiwania stanowiące odpowiedź na zapytanie pochodzące od osoby fizycznej stanowi czynność przetwarzania danych osobowych. ETS w wyroku w sprawie Google Spain przeciwko González¹³⁰ wskazał, że działalność wyszukiwarki internetowej polega na zlokalizowaniu informacji opublikowanych lub zamieszczonych w internecie przez osoby trzecie, indeksowaniu ich w sposób automatyczny, czasowym przechowywaniu takich informacji i wreszcie ich udostępnianiu internautom w sposób uporządkowany zgodnie z określonymi preferencjami. W sytuacji, gdy takie informacje zawierają dane osobowe, należy uznać za „przetwarzanie danych osobowych”¹³¹. ETS stwierdził, że działalność wyszukiwarki internetowej może znacząco oddziaływać na prawa podstawowe¹³². Ustalając, które z praw podstawowych mogą doznać uszczerbku, wskazał na prawo do prywatności¹³³. Zważywszy na stosowane obecnie metody profilowania oraz ich konsekwencje polegające na udzielaniu

zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się (art. 4 pkt 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. UE L Nr 119, s. 1 z późn. zm.)).

¹²⁹ Tamże.

¹³⁰ Wyrok TS w sprawie Google Spain przeciwko González.

¹³¹ Tamże, pkt 1 sentencji.

¹³² Tamże.

¹³³ Tamże.

dostępu do wyselekcjonowanych przez dostawcę usługi wyników wyszukiwania i różnicowania wyników ze względu na profil użytkownika, uszczerbku doznawać może nie tylko prawo do prywatności, lecz także swoboda wypowiedzi oraz prawo do równego traktowania w sferze dostępu do informacji¹³⁴. Zwrócono ponadto uwagę, że wyniki wyszukiwania mogą się różnić nie tylko pomiędzy różnymi użytkownikami, lecz także pomiędzy różnymi lokalnymi (krajowymi) wersjami tej samej wyszukiwarki. Zatem wprowadzenie ograniczeń w jednej wersji niekoniecznie musi oznaczać ich zastosowanie w innej, lokalnej wersji wyszukiwarki. Obecnie nie wiadomo, w jakim stopniu Google będzie stosował narzędzia wymuszające korzystanie z wyszukiwarki przeznaczonej dla konkretnego kraju¹³⁵.

E. USŁUGI PRZETWARZANIA W CHMURZE

Zgodnie z art. 2 pkt 13 ARC „usługa przetwarzania w chmurze” oznacza usługę przetwarzania w chmurze zdefiniowaną w art. 4 pkt 19 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 (dyrektywa NIS). Zważywszy, że dyrektywa ta została uchylona i w jej miejsce przyjęto dyrektywę NIS 2¹³⁶, prawidłowe wydaje się stosowanie używanego w dyrektywie NIS 2 terminu

¹³⁴ Paradoksalnie w sprawie Google Spain przeciwko González, Google broniąc się przed zarzutem naruszenia prawa prywatności obywatela Hiszpani Mario Costeji González w związku z odmową usunięcia z kolejki wyszukiwania linków prowadzących do materiałów zawierających nieprawdziwe o nim informacje, podnosiło, że ewentualne nakazanie przez ETS usunięcia linków z wyników wyszukiwania stanowiłoby nieproporcjonalne naruszenie wolności wypowiedzi i prawa użytkowników internetu do informacji (pkt 133 wyroku). Obecnie w rezultatach wyszukiwania pojawiają się odesłania wyselekcjonowane przez dostawcę usługi i w wybranej przez niego kolejności. Pomimo że udzielenie dostępu do wybranych wyników ogranicza prawo użytkownika do informacji, mechanizm ten jest powszechnie stosowany.

¹³⁵ Ł. Goździaszek, *Prawo do bycia zapomnianym w wyszukiwarce internetowej – glosa do wyroku Trybunału Sprawiedliwości z 13.05.2014 r. w sprawie C-131/12 Google Spain SL i Google Inc. przeciwko Agencia de Protección de Datos (AEPD) i Mario Costeja González*, „Europejski Przegląd Sądowy” 2015, nr 2, s. 41–48.

¹³⁶ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.U. UE L Nr 333, s. 80).

„usługi chmurowe” w nadanym mu przez nią znaczeniu. W dyrektywie tej przyjęto, że usługi chmurowe powinny obejmować usługi cyfrowe umożliwiające administrowanie na żądanie skalowalnym i elastycznym zbiorem rozproszonych zasobów obliczeniowych do wspólnego wykorzystywania oraz szeroki dostęp zdalny do tego zbioru, w tym gdy takie zasoby są rozmieszczone w kilku lokalizacjach. Zasoby obliczeniowe obejmują zasoby takie jak sieci, serwery lub inna infrastruktura, systemy operacyjne, oprogramowanie, pamięć masowa, aplikacje i usługi.

Do modeli usług chmurowych należą m.in. infrastruktura jako usługa (IaaS), platforma jako usługa (PaaS), oprogramowanie jako usługa (SaaS) oraz sieć jako usługa (NaaS). Modele rozmieszczenia usług chmurowych powinny obejmować chmury prywatne, zbiorowe, publiczne i hybrydowe. Modele usług chmurowych i modele rozmieszczenia oznaczają to samo, co usługi i modele ich realizacji zdefiniowane w normie ISO/IEC 17788:2014. Zdolność użytkowników usług chmurowych do jednostronnego zapewnienia sobie możliwości obliczeniowych, takich jak czas serwera lub magazyn sieciowy, bez żadnej interakcji z udziałem człowieka ze strony dostawcy usług chmurowych można określić jako administrowanie na żądanie (motyw 33 dyrektywy NIS 2).

Terminu „szeroki dostęp zdalny” używa się do opisu sytuacji, gdy zasoby chmurowe są udostępniane przez sieć, a dostęp do nich jest możliwy za pośrednictwem mechanizmów sprzyjających wykorzystywaniu różnorodnych platform typu *thin client* lub *thick client*, w tym telefonów komórkowych, tabletów, laptopów oraz stacji roboczych. Termin „skalowalne” odnosi się do zasobów komputerowych, które są elastycznie przydzielane przez dostawcę usługi niezależnie od położenia geograficznego zasobów w reakcji na fluktuacje zapotrzebowania. Terminu „elastyczny zbiór” używa się do opisu zasobów obliczeniowych, które są dostarczane i uwalniane według zapotrzebowania, aby szybko zwiększać i zmniejszać dostępne zasoby w zależności od obciążenia. Terminu „wspólnie wykorzystywane” używa się do opisu zasobów obliczeniowych udostępnianych wielu użytkownikom, którzy dzielą wspólny dostęp do usługi, jednak przetwarzanie odbywa się oddzielnie dla każdego z nich, choć usługa jest świadczona z tego samego sprzętu elektronicznego. Terminu „rozproszone” używa się do opisu zasobów obliczeniowych zlokalizowanych na różnych komputerach lub urządzeniach

połączonych w sieć, które komunikują się ze sobą i koordynują swoją pracę przez przekazywanie komunikatów (motyw 33 dyrektywy NIS 2).

Usługi chmurowe mogą być świadczone w sposób wysoce rozproszony, jeszcze bliżej miejsca generowania lub gromadzenia danych, co będzie wiązać się z przejściem od modelu tradycyjnego do modelu wysoce rozproszonego – przetwarzanie danych na obrzeżach sieci (motyw 34 dyrektywy NIS 2).

Usługi chmurowe, co do stosowanej technologii, w przeciwieństwie do usług wyszukiwarek, nie ingerują bezpośrednio w sferę wolności wypowiedzi, jednak – ze względu na stosowane przez dostawców tych usług strategie handlowe – mogą ograniczać swobodę dysponowania zasobami danych zgromadzonymi w chmurze obliczeniowej. Zwrócono uwagę w literaturze, że strategia dostawców tych usług polega na uzależnieniu klienta od usługi chmurowej dostarczanej przez konkretnego dostawcę¹³⁷. Strategia zniechęcania do zmiany dostawcy, a w konsekwencji swobodnego dysponowania zasobami zgromadzonymi w chmurze, polega – na płaszczyźnie technologii – na utrzymywaniu przez dostawców niskiego stopnia interoperacyjności usługi, a także stosowanego formatu zapisu danych, co skutkuje ich nieprzenoszalnością¹³⁸. Skutek polegający na utracie danych albo utracie nad nimi kontroli może powstać, jeśli warunki umowy o świadczenie usługi lub regulaminy zawierają nieprecyzyjne postanowienia dotyczące potwierdzenia własności danych, ich lokalizacji, zasad zwrotu danych w wypadku zakończenia świadczenia usługi oraz niszczenia danych, blokowania do nich dostępu¹³⁹.

Usługi chmurowe generują nową kategorię zagrożeń dla wolności wypowiedzi. Zagrożenia te dotyczą nie tyle ograniczania zakresu swobody ekspresji, co utraty kontroli nad wypowiedzią (danymi). Utrata kontroli może oznaczać brak możliwości ustalenia lokalizacji danych, niemożność ich przeniesienia, utratę prawa do zwrotu danych, ograniczenie ich dostępności ze względu na stosowane przez dostawcę formaty oraz brak rozliczalności, a także poufności ich przetwarzania. O ile zatem z dużym prawdopodobieństwem można

¹³⁷ Ł. Węgrzyn, *Mechanizmy kontraktowe ograniczające uzależnienie się od dostawcy usług chmurowych dostarczanych w modelu SaaS (Software as a Service)*, „Monitor Prawniczy” 2020, nr 20, s. 122.

¹³⁸ Tamże, s. 122.

¹³⁹ Ł. Węgrzyn zwraca uwagę na potrzebę precyzyjnego uregulowania z dostawcą usług chmurowych wskazanych powyżej warunków umownych (Zob. Ł. Węgrzyn, *Mechanizmy kontraktowe...*, s. 123).

stwierdzić, że ze strony dostawcy usług chmurowych nie wystąpi zagrożenie polegające na uszczuplaniu (ograniczaniu zakresu) treści (danych) umieszczanych w chmurze, co zresztą stałoby w oczywistej sprzeczności z interesem gospodarczym dostawcy usługi, to jednak metoda wykonania usługi może generować ryzyko naruszenia swobody dysponowania danymi (treściami). O ile usługobiorca posiada tytuł do danych (treści) przetwarzanych w chmurze, to pozbawienie go albo ograniczenie mu przez dostawcę kontroli nad nimi stanowić będzie ingerencję w sferę wolności wypowiedzi użytkownika.

B. Usługi udostępniania treści online

a. USŁUGA UDOSTĘPNIANIA TREŚCI ONLINE

W katalogu usług cyfrowych konieczne jest wyodrębnienie usługi udostępniania treści online jako samoistnego rodzaju usług cyfrowych. Potrzeba ta wynika zarówno ze względu na cechy tych usług, jak i na ich przedmiot, a także z uwagi na status usługodawcy. Dostawca usługi udostępniania treści online nie jest bowiem ani pośrednikiem internetowym, ani dostawcą treści cyfrowych.

Usługi udostępniania treści online zostały wyodrębnione i zdefiniowane jako samodzielna kategoria usług społeczeństwa informacyjnego w dyrektywie 2019/790¹⁴⁰. Usługi te należą do kategorii usług społeczeństwa informacyjnego, podobnie jak usługi pośrednictwa internetowego (mere conduit, caching, hosting) i usługi dostarczania treści cyfrowych¹⁴¹. Istotą usługi udostępniania treści online jest świadczenie polegające na „umożliwieniu publicznego dostępu” do szczególnego rodzaju treści cyfrowych, tj. takich, które są objęte ochroną z tytułu praw wyłącznych, w szczególności praw autorskich lub praw pokrewnych. W dyrektywie 2019/790 uregulowane zostały zasady udzielania dostępu do treści objętych ochroną praw wyłącznych w taki

¹⁴⁰ Dyrektywa DSM.

¹⁴¹ W motywie 62 dyrektywy 2019/790 usługi udostępniania treści online zostały jednoznacznie skategoryzowane jako usługi społeczeństwa informacyjnego. Stwierdzono tam, że „W ramach zwykłego korzystania z niektórych usług społeczeństwa informacyjnego przewidziane jest udzielanie publicznego dostępu do zamieszczanych przez użytkowników tych usług chronionych prawem autorskim treści lub innych przedmiotów objętych ochroną”.

sposób, by dostęp ten mógł być realizowany za pośrednictwem publicznie dostępnej sieci teleinformatycznej bez pokrzywdzenia podmiotów uprawnionych i zapewnienie im respektowania przysługujących im praw osobistych i majątkowych. W motywie 61 dyrektywy wskazano, że „usługi udostępniania treści online zapewniające dostęp do dużej ilości treści chronionych prawem autorskim zamieszczanych przez użytkowników stały się głównym źródłem dostępu do treści online”. Konieczne stało się zatem dostosowanie niektórych wyjątków i ograniczeń w zakresie ochrony praw autorskich i praw pokrewnych do środowiska cyfrowego i transgranicznego, jak również środków ułatwiających niektóre praktyki w zakresie licencjonowania dotyczących w szczególności, lecz nie wyłącznie, rozpowszechniania niedostępnych w obrocie handlowym utworów i przedmiotów objętych ochroną oraz dostępności w internecie utworów audiowizualnych na platformach wideo na żądanie w celu zapewnienia szerszego dostępu do treści (motyw 3). Zasady te i wyjątki zostały wskazane w dyrektywie 2019/790. Celem tej regulacji jest „osiągnięcie sprawiedliwej równowagi między prawami i interesami twórców i innych podmiotów uprawnionych, z jednej strony, a prawami i interesami użytkowników, z drugiej strony” (motyw 6).

Usługi udostępniania treści online obejmują kategorię usług, które – zważywszy na treść motywów 62–64 dyrektywy 2019/790 – mają łącznie następujące cechy:

1. obejmują treści chronione, w tym objęte ochroną prawnoautorską,
2. „odgrywają ważną rolę na rynku treści online”,
3. głównym lub jednym z głównych celów świadczonej usługi jest przechowywanie i umożliwianie użytkownikom zamieszczania i udostępniania treści,
4. usługodawcy nie są twórcami udostępnianych treści,
5. usługodawcy nie modyfikują treści ani w żaden inny sposób nie ingerują w ich treść,
6. usługodawcy nie są dostawcami treści,
7. działalność usługodawcy obejmuje „dużą ilość treści chronionych”,
8. usługodawca działa w celu zarobkowym,

9. usługodawca podejmuje działania polegające na organizowaniu treści i ich klasyfikowaniu w celu przyciągnięcia większej liczby odbiorców, w tym poprzez ich klasyfikację i wykorzystywanie ukierunkowanych działań promocyjnych.

O ile niesporny wydaje się termin „treści chronione”, który ustawodawca europejski identyfikuje z dobrami niematerialnymi stanowiącymi przedmiot ochrony praw autorskich i praw pokrewnych, o tyle doprecyzowania wymaga, w jaki sposób rozumieć należy zawarte w motywie 62 dyrektywy przesłanki nakazujące, by pojęciem „usługi udostępniania treści online” obejmować tylko takie usługi, które „odgrywają ważną rolę na rynku usług”, a nadto tylko wówczas, gdy obejmują „dużą ilość treści chronionych”. W odniesieniu do ustalenia kryterium „dużej ilości” udostępnianych treści wskazano, że:

ocena tego, czy dostawca usług udostępniania treści online przechowuje i udziela dostępu do dużej ilości treści chronionych prawem autorskim, powinna uwzględniać połączenie elementów takich jak odbiorcy usługi oraz liczba plików zawierających treści chronione prawem autorskim zamieszczanych przez użytkowników usługi (motyw 63).

W dyrektywie nie sprecyzowano natomiast przesłanek, od których uzależniona powinna być ocena, czy usługi udostępniania treści online – w odniesieniu do konkretnego dostawcy – rzeczywiście odgrywają „ważną rolę na rynku usług”. Nie jest zatem jasne, czy wynik tej oceny powinien być uzależniony od „dużej ilości” udostępnianych treści, czy może np. od renomy usługodawcy albo od charakteru udostępnianych treści lub liczby użytkowników, którzy z tych treści korzystają. Zważywszy, że przesłanka „ważnej roli na rynku usług” jest nieprecyzyjna, a zarazem stanowi element konstrukcyjny definicji terminu „usługi udostępniania treści online”, ustalenie zakresu tego terminu *de facto* zostało pozostawione orzecznictwu i doktrynie.

W potocznym rozumieniu dostawca usługi udostępniania treści online „pośredniczy” pomiędzy użytkownikami internetu a podmiotami posiadającymi tytuł prawny do treści. Pośrednictwo to polega na dwojakiego rodzaju czynnościach, tj. po pierwsze na udzieleniu miejsca na serwerze i zgromadzeniu treści, które – co do zasady – *ex lege* podlegają ochronie oraz po drugie stworzeniu warunków organizacyjnych (regulaminy) i technicznych

(system autoryzacji i uwierzytelniania, system mikropłatności) umożliwiającym użytkownikom internetu zapoznanie się z treścią. Określenie „usługa udostępniania treści” oznacza, że podmiot świadczący usługę „pośredniczy” pomiędzy uprawnionym z tytułu praw autorskich lub praw pokrewnych a użytkownikiem w zakresie udzielenia dostępu do chronionej treści. Z tego powodu termin „usługa udostępniania treści online” może wprowadzać w błąd co do jej kwalifikacji jako usługi pośrednictwa internetowego, co należy uznać za nieprawidłowe.

Usługodawca świadczący usługę udostępniania treści online, pomimo że „pośredniczy” w udostępnianiu treści, to nie należy do kategorii pośredników internetowych w rozumieniu dyrektywy 2000/31. W motywie 65 dyrektywy 2019/790 przesądono, że odnoszący się do pośredników internetowych art. 14 ust. 1 dyrektywy 2000/31/WE nie powinien mieć zastosowania do odpowiedzialności dostawców usług udostępniania treści online. Dostawca takich usług nie może więc powoływać się na ustanowiony w dyrektywie 2000/31 mechanizm wyłączania odpowiedzialności. Jeśli zatem w odniesieniu do pośredników internetowych przesłanką *sine qua non* wyłączenia odpowiedzialności jest, na gruncie art. 14 dyrektywy 2000/31, pasywne zachowanie pośrednika, który nie ingeruje w treść transmitowanych lub przechowywanych wiadomości, to w odniesieniu do dostawcy usług udostępniania treści online mechanizm ten nie znajdzie zastosowania. Przeciwnie, od dostawcy usług udostępniania treści online wymagać się będzie zachowania „wysokiego standardu staranności”, który obejmuje m.in. czynności monitorowania treści pod kątem ewentualnego naruszenia praw wyłącznych jeszcze przed ich publicznym udostępnieniem (*ex ante*). Jak wskazano w motywie 66:

dostawcy usług udostępniania treści online powinni dołożyć wszelkich starań zgodnie z wysokimi standardami staranności zawodowej w sektorze, aby zapobiegać dostępności w swoich serwisach nieobjętych zezwoleniem utworów i innych przedmiotów objętych ochroną zidentyfikowanych przez odpowiednie podmioty uprawnione.

Przy dokonywaniu oceny, czy dostawca usług udostępniania treści online dołożył wszelkich starań zgodnie z wysokimi standardami staranności zawodowej w sektorze, należy wziąć pod uwagę to, czy dostawca usług podjął wszystkie kroki, jakie podjąłby staranny podmiot dla osiągnięcia

celu dotyczącego zapobiegania dostępności nieobjętych zezwoleniem utworów lub innych przedmiotów objętych ochroną na swojej stronie internetowej, przy uwzględnieniu najlepszych praktyk stosowanych w sektorze i skuteczności podjętych kroków w świetle wszystkich istotnych czynników i rozwoju sytuacji oraz zasady proporcjonalności (motyw 66).

Jeśli więc przesłanka zachowania neutralności przesądza o uzyskaniu statusu pośrednika internetowego, to, jak się wydaje, dostawca usług udostępniania treści online, z racji wymaganej od niego *ex lege* postawy aktywnego współdziałania z podmiotami uprawnionymi, w szczególności w zakresie pozyskiwania od nich zezwoleń na publiczne udostępnianie treści, nie pozwala na zakwalifikowanie go do grona pośredników internetowych¹⁴².

Ryzyko wadliwej kwalifikacji usług udostępniania treści online poprzez przypisanie ich do nieodpowiedniej kategorii usług cyfrowych wywołuje także zawarta w motywie 4 dyrektywy 2019/790 reguła interpretacyjna, zgodnie z którą „dyrektywa ta opiera się na zasadach określonych w dyrektywach obowiązujących obecnie w tej dziedzinie, w szczególności dyrektywach 2001/29 i 2000/31”. Skoro definiowanie oraz ustalenie zasad świadczenia usług udostępniania treści online należy „oprzec” na dyrektywie regulującej działalność pośredników internetowych (2000/31) oraz harmonizującej ramy prawne w zakresie korzystania z treści objętych ochroną prawnoautorską (2001/29), to może to prowadzić do wadliwego ustalenia statusu dostawców usług udostępniania treści online i nieprawidłowego przyjęcia, że do usług udostępniania treści online znajdują zastosowanie zawarte w art. 13–15 dyrektywy 2000/31 mechanizmy wyłączania odpowiedzialności prawnej pośredników. Mając na uwadze wskazane powyżej ryzyko zaistnienia uproszczonej, wadliwej wykładni, celowe jest ustalenie przesłanek przesądzających o odrębności usług udostępniania treści online w katalogu usług cyfrowych.

¹⁴² Należy się zgodzić z wyrażanym w doktrynie stanowiskiem, zgodnie z którym istotnym aspektem wpływającym na możliwość uznania usługodawcy świadczącego usługi społeczeństwa informacyjnego za pośrednika jest jego stosunek wobec treści użytkowników. Musi on bowiem pozwolić na odróżnienie jego działalności – umożliwiania udostępniania treści innym podmiotom – od usług polegających na udostępnianiu własnych treści (Zob. M. Piech, *Usługodawcy przechowujący i udostępniający treści użytkowników jako pośrednicy*, [w:] *Pośrednicy internetowi...*, s. 256).

Definiowanie usług udostępniania treści online następuje w dyrektywie 2019/790 nie tyle poprzez wskazanie cech tych usług, co poprzez ustalenie statusu podmiotów świadczących ten rodzaj usług, a nadto poprzez skatalogowanie wyłączeń i wyjątków¹⁴³. Katalog wyłączeń obejmuje usługi, które pomimo zbliżonego charakteru, nie są – z mocy przepisu dyrektywy – zaliczone do kategorii usług udostępniania treści online¹⁴⁴. Katalog wskazany w art. 3–7 dyrektywy 2019/790 obejmuje wyjątki, które są istotne z punktu widzenia badań naukowych, innowacji, nauczania i zachowania dziedzictwa kulturowego, a także ograniczenia w odniesieniu do korzystania z technologii eksploracji tekstów i danych, zilustrowania w ramach nauczania w środowisku cyfrowym oraz do celów zachowania dziedzictwa kulturowego (motyw 5).

O ile zatem w art. 2 pkt 6 dyrektywy zdefiniowano termin „dostawca usług udostępniania treści online”, o tyle w motywie 62 opisano cechy tych usług, nie definiując jednak *explicite* tego terminu. W dyrektywie wskazano natomiast na rodzaje usług, które zostały wyłączone z katalogu usług udostępniania treści online. Nie uznaje się za usługi udostępniania treści online takich usług, jak:

1. nienastawione na zysk encyklopedie internetowe,
2. nienastawione na zysk repozytoria naukowe i edukacyjne,

¹⁴³ W motywie 3 dyrektywy wskazano, że „Dyrektywa ustanawia zasady dotyczące dostosowania niektórych wyjątków i ograniczeń w zakresie praw autorskich i praw pokrewnych do środowiska cyfrowego i transgranicznego, jak również środki ułatwiające niektóre praktyki w zakresie licencjonowania dotyczące w szczególności, lecz nie wyłącznie, rozpowszechniania niedostępnych w obrocie handlowym utworów i przedmiotów objętych ochroną oraz dostępności w internecie utworów audiowizualnych na platformach wideo na żądanie w celu zapewnienia szerszego dostępu do treści”.

¹⁴⁴ Do tej drugiej kategorii usług należą np. usługi łączności elektronicznej w rozumieniu dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/772 14, a także dostawcy usług w chmurze dla przedsiębiorstw oraz usług w chmurze obliczeniowej, które umożliwiają użytkownikom zamieszczanie treści na własny użytek, takich jak cyberschowki lub internetowe platformy handlowe, których główną działalnością jest sprzedaż detaliczna online, a nie dostęp do treści chronionych prawem autorskim. Z definicji dostawcy usług udostępniania treści online powinni być wyłączeni również dostawcy usług takich jak: tworzenie otwartego oprogramowania i platformy wymiany, nienastawione na zysk repozytoria naukowe lub edukacyjne, a także nienastawione na zysk internetowe encyklopedie internetowe. Wreszcie, aby zapewnić wysoki poziom ochrony prawa autorskiego, mechanizm wyłączenia odpowiedzialności, o którym mowa w niniejszej dyrektywie, nie powinien mieć zastosowania do dostawców usług, których głównym celem jest podejmowanie lub ułatwianie piractwa prawa autorskiego (motyw 62).

3. platformy tworzenia otwartego oprogramowania i platformy wymiany otwartego oprogramowania,
4. dostawców usług łączności elektronicznej zdefiniowanych w dyrektywie (UE) 2018/1972,
5. internetowych platform handlowych oraz
6. usług w chmurze dla przedsiębiorstw i usług w chmurze obliczeniowej, które umożliwiają użytkownikom zamieszczanie treści na własny użytek (art. 2 pkt 6 akapit drugi dyrektywy 2019/790).

Z drugiej natomiast strony potwierdzono, poprzez wyliczenie, że do katalogu usług udostępniania treści online należy zaliczyć niektóre nietypowe rodzaje usług, jak w szczególności usługi realizowane przez wydawców prasy (art. 15) polegające na udzielaniu publicznego dostępu do publikacji prasowych. Zgodnie z zaproponowaną w motywie 55 definicją przez pojęcie „wydawca publikacji prasowych” należy rozumieć „usługodawców, takich jak wydawcy wiadomości lub agencje informacyjne, gdy publikują one publikacje prasowe w rozumieniu dyrektywy”. Publikacją prasową jest „zbiór złożony głównie z utworów literackich o charakterze dziennikarskim, mogący jednakże obejmować także inne utwory lub inne przedmioty objęte ochroną, który łącznie spełnia następujące kryteria:

- a) stanowi odrębną całość w ramach periodycznej lub regularnie aktualizowanej pod jednym tytułem publikacji, takiej jak gazeta lub czasopismo o tematyce ogólnej lub specjalistycznej;
- b) ma na celu dostarczenie opinii społecznej informacji dotyczących aktualnych wiadomości lub innej tematyki; oraz
- c) jest publikowany w dowolnym medium z inicjatywy dostawcy usług, na jego odpowiedzialność i pod jego kontrolą” (art. 2 pkt 4 dyrektywy 2019/790).

Wydawcom prasowym zagwarantowano wyłączne prawo do decydowania o zwielokrotnianiu utworu, a także wyłączne prawo do zezwalania lub zabrania podawania do publicznej wiadomości lub publicznego udostępniania publikacji prasowych (art. 15 ust. 1 dyrektywy 2019/790 w zw. z art. 2 i art. 3 ust. 2 dyrektywy 2001/29). Czynności publicznego udostępniania lub

podawania do publicznej¹⁴⁵ wiadomości utworu jest identyfikowana z udzieleniem publicznego dostępu do chronionych prawem autorskim utworów lub innych przedmiotów objętych ochroną zamieszczanych przez użytkowników (motyw 64 dyrektywy 2019/790). Obejmuje ono:

zarządzanie w Internecie i udzielanie dostępu do platformy wymiany, która poprzez indeksację metadanych dotyczących utworów chronionych i udostępnianie wyszukiwarki umożliwia użytkownikom tej platformy wyszukanie tych utworów oraz ich wymianę w ramach sieci równorzędnej (peer-to-peer) [...] Autorskie prawo do publicznego udostępniania obejmuje każdą publiczną transmisję lub retransmisję utworów odbiorcom nieznanym się w miejscu, z którego przekazywanie pochodzi, drogą przewodową lub bezprzewodową, w tym nadawanie programów [...] ¹⁴⁶.

Aby doszło do publicznego udostępnienia utworu, wystarczy, by był on udostępniony publicznie, przy czym nie jest decydujące, czy użytkownicy internetu mieli rzeczywisty dostęp do tego utworu¹⁴⁷. Wszelkie działanie, poprzez które użytkownik świadomie udziela swoim klientom dostępu do utworów chronionych, może stanowić „czynność udostępniania” w rozumieniu art. 3 ust. 1 dyrektywy 2001/29¹⁴⁸. Nie stanowi natomiast publicznego udostępniania zamieszczenie linków odsyłających do chronionych utworów¹⁴⁹.

¹⁴⁵ Zważywszy na odesłanie zawarte w art. 15 ust. 1 dyrektywy 2019/790 do art. 2 i art. 3 ust. 2 dyrektywy 2001/29, pojęcie publicznego udostępniania należy rozumieć w sposób, w jaki termin ten został użyty na gruncie dyrektywy 2001/29. Aktualne zatem pozostają wypowiedzi TS, który kilkakrotnie dokonywał interpretacji i ustalenia zakresu tego terminu.

¹⁴⁶ Wyrok TS z dnia 14 czerwca 2017 r. w sprawie Stichting Brein przeciwko Ziggo BV i XS4ALL Internet BV, C-610/15, poz. I-456.

¹⁴⁷ Wyrok TS w sprawie UPC Telekabel Wien, s. 453.

¹⁴⁸ Wyrok TS z dnia 14 czerwca 2017 r. w sprawie Stichting Brein przeciwko Ziggo BV i XS4ALL Internet BV, C-610/15, poz. I-456.

¹⁴⁹ TS stwierdził, że art. 3 ust. 1 dyrektywy 2001/29 w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym należy interpretować w ten sposób, że nie stanowi czynności publicznego udostępnienia w rozumieniu tego przepisu udostępnienie na stronie internetowej linków, na które można kliknąć, odsyłających do utworów chronionych, ogólnie dostępnych na innej stronie internetowej (zob. Wyrok TS w sprawie UPC Telekabel Wien, s. 453).

Skonstruowane w art. 15–16 dyrektywy 2019/790 na rzecz wydawców prasowych prawa sytuują wydawców w wygodnej roli, tj. z jednej strony dostawcy treści, a z drugiej strony dostawcy usługi udostępniania tych treści. Na „publikację prasową”, w rozumieniu dyrektywy 2019/790, składają się bowiem artykuły (materiały prasowe) autorstwa wielu twórców (dziennikarzy), a także utwory współautorskie oraz dzieła zawierające elementy cudzych utworów (utwory z zapożyczeniami). Pomimo zatem, że usługi świadczone przez wydawców publikacji prasowych posiadają własną specyfikę, polegają bowiem nie tylko na udzieleniu dostępu do treści, jak ma to miejsce w odniesieniu do pozostałych dostawców usług udostępniania treści online, ale także na dostarczaniu treści własnych, to wydawcy prasowi uzyskali status dostawców usług udostępniania treści, co pozwala im na powoływanie się zarówno wobec twórców (w tym dziennikarzy), jak i innych podmiotów na upoważnienie do wykonywania „nowego prawa pokrewnego”, a nadto do wykonywania w imieniu twórców praw autorskich wskazanych w art. 15 ust. 1 dyrektywy 2019/790, tj. prawa do publicznego udostępniania i prawa do zwielokrotnienia utworu. Nadto wydawcy korzystać będą ze szczególnego, opisanego w art. 17 mechanizmu wyłączania odpowiedzialności, który ustawodawca europejski przewidział dla dostawców usług udostępniania treści online.

Jak zauważył R. Markiewicz, art. 15 dyrektywy wprowadza nowe prawo pokrewne, równoległe do praw autorskich przysługujących wydawcy (m.in. ze względu na prawo do dzieła zbiorowego, baz danych oraz publikacji prasowych, co do których nabyli autorskie prawa majątkowe), a także baz danych chronionych prawem *sui generis*. Przepis ten ustanawia prawo wyłączone wydawców, z którego wynika zakaz, bez odpowiedniego upoważnienia, reprodukcji lub publicznego udostępniania online ich publikacji¹⁵⁰. Ustanowione na rzecz wydawców nowe prawo pokrewne wyposaża wydawców w roszczenia zarówno o charakterze majątkowym, jak i niemajątkowym, skuteczne *erga omnes* wobec wszystkich korzystających z całości lub fragmentów publikacji prasowej w internecie i poza nim. Z zakazu tego wynika zarazem domniemanie zgodnego z prawem korzystania przez wydawców z praw wyłącznych przysługujących twórcom utworów wchodzących w skład

¹⁵⁰ R. Markiewicz, *Prawo pokrewne wydawców prasy*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej” 2019, nr 4, s. 5–39.

publikacji prasowej (wydania, numeru). Istnienie domniemania ustanowionego na rzecz wydawców potwierdza także treść art. 16 dyrektywy. Zgodnie z tym przepisem wydawcy są uprawnieni do udziału w rekompensacie za korzystanie z utworu stanowiącego integralną część publikacji prasowej.

Wydawcy zyskali zatem „nowe prawo pokrewne”, które mogą wykonywać w odniesieniu do publikacji prasowej – jako całości (zbiór utworów), na którą składają się pojedyncze utwory (artykuły prasowe, materiały prasowe), a nadto uzyskali upoważnienie do wykonywania niektórych praw w imieniu twórców, tj. prawa do decydowania o publicznym udostępnieniu, a także prawo do zwielokrotniania.

R. Markiewicz celnie stwierdza, że termin „publikacja prasowa” został w dyrektywie 2019/790 użyty w istocie sprzecznie ze swym znaczeniem. Nie odnosi się bowiem do artykułów zamieszczanych w czasopismach, lecz oznacza jednostkowo ujmowany „numer” danego periodyku („papierowy” lub udostępniany online). Publikacją prasową są m.in. „dzienniki, tygodniki lub miesięczniki o tematyce ogólnej lub specjalistycznej, w tym abonowane czasopisma, oraz internetowe serwisy informacyjne (motyw 56 zdanie drugie)”¹⁵¹.

Publikacja prasowa w rozumieniu dyrektywy nie odpowiada zakresowi pojęcia „materiał prasowy”, które zostało zdefiniowane w art. 7 ust. 2 ustawy Prawo prasowe. Zgodnie z tym przepisem materiałem prasowym jest każdy opublikowany lub przekazany do opublikowania w prasie tekst albo obraz o charakterze informacyjnym, publicystycznym, dokumentalnym lub innym, niezależnie od środków przekazu, rodzaju, formy, przeznaczenia czy autorstwa. Katalog tekstów, które uznaje się za materiały prasowe nie został w powyższym przepisie stworzony, a otwarta formuła charakteru tekstu (informacyjnym, publicystycznym lub inny) i środka wyrazu (niezależnie od rodzaju, formy) daje podstawę do przyjęcia, iż również np. powieść odcinkowa stanowi materiał prasowy, skoro ustawodawca przez to pojęcie rozumie „każdy opublikowany lub przekazany do opublikowania w prasie tekst”¹⁵². Materiałem prasowym jest także reklama¹⁵³.

¹⁵¹ Tamże, s. 5–39.

¹⁵² Wyrok SA w Białymstoku z dnia 19 października 1995 r., I ACr 227/95, LEX nr 62590.

¹⁵³ Wyrok SN z dnia 4 lutego 2005 r., I CK 515/04, LEX nr 558556.

O ile ze względu na szeroką definicję terminu „materiał prasowy” przypisanie autorstwa „materiału prasowego” może nastąpić zarówno dziennikarzowi, jak i innej osobie (np. osobie udzielającej wypowiedzi dla prasy), to jednak w doktrynie nie budziło wątpliwości, że status twórcy, a w konsekwencji autorskie prawa osobiste i majątkowe do materiału prasowego przysługują, co do zasady, dziennikarzom. Podobne stanowisko, pozornie, zostało wypowiedziane w art. 15 ust. 2 dyrektywy 2019/790. Postanowiono w tym przepisie, że zawarte w dyrektywie „nowe prawo pokrewne” ustanowione na rzecz wydawców nie narusza przewidzianych w prawie Unii praw twórców i innych podmiotów uprawnionych w odniesieniu do utworów i innych przedmiotów objętych ochroną zawartych w publikacji prasowej, i „nie ma na te prawa żadnego wpływu”. Nadto zastrzeżono, że na prawa przyznane wydawcom prasowym „nie można się powoływać przeciwko twórcom” (art. 15 ust. 2 dyrektywy 2019/790).

Można przypuszczać, że art. 15 ust. 2 stanowić będzie – w odniesieniu do dziennikarzy – przepis martwy. Udzielanie zezwolenia (licencji) na opublikowanie materiału prasowego stanowi bowiem warunek *sine qua non* wykonywania zawodu dziennikarza. Ustawodawca europejski założył tymczasem, jak wynika z treści art. 15 ust. 2 dyrektywy, że twórca, w tym dziennikarz, dysponuje swobodą w zakresie decydowania odnośnie do udzielenia lub odmowy udzielenia zezwolenia na publiczne udostępnienie stworzonego materiału prasowego. Nie uwzględniono, że materiały prasowe, ze względu na cel powstania, przeznaczenie, objętość, a przede wszystkim tryb eksploatacji, są – co do zasady – przeznaczone do publikacji w prasie. Skoro samodzielna eksploatacja, tj. poza prasą, materiałów, których autorami są dziennikarze, ma charakter wyjątkowy, to oznacza w konsekwencji, że sposób eksploatacji tych materiałów jest determinowany rygorami ustalonymi przez wydawcę.

Z treści stosunku prawnego łączącego dziennikarza z wydawcą wynika wprost ciążyący na dziennikarzu obowiązek przygotowywania materiałów prasowych „na rzecz redakcji”, a więc także na rzecz wydawcy. Udzielenie zezwolenia (licencji) stanowi warunek *sine qua non* wykonywania zawodu dziennikarza i tworzenia materiałów prasowych. Iluzoryczne jest zatem zawarte w art. 15 ust. 2 założenie o istnieniu partnerskiego, równoważnego stosunku pomiędzy wydawcą prasowym a dziennikarzem w zakresie ustalania rodzaju i treści udzielanego wydawcy zezwolenia na korzystanie

ze stworzonych przez dziennikarzy utworów (materiałów prasowych). Wykonywanie zawodu dziennikarza nie jest bowiem możliwe poza jednostką redakcyjną, a zadaniem dziennikarza jest tworzenie treści przeznaczonych do opublikowania w prasie. W świetle definicji „dziennikarza” zawartej w art. 7 ust. 2 pkt 5 pr. r. dziennikarzem jest każda osoba, która ma upoważnienie do działania na rzecz i w imieniu redakcji, niezależnie od tego, czy podejmowane przez nią działania są wykonywane odpłatnie czy nieodpłatnie, a także niezależnie od tego, czy osobę tę łączy z redakcją stosunek pracy¹⁵⁴. Ustawa Prawo prasowe nie zawiera regulacji dotyczących zakresu i sposobu udzielania praw lub rozporządzania prawami autorskimi przez dziennikarzy na rzecz wydawców prasowych. Należy zatem odwołać się do zasad ogólnych, w tym zawartych w ustawie o prawie autorskim i prawach pokrewnych regulujących nabywanie autorskich praw majątkowych przez pracodawcę. W świetle art. 12 ustawy o prawie autorskim i prawach pokrewnych pracodawca, a zatem także wydawca, nabywa autorskie prawa majątkowe *ex lege* w granicach wynikających z celu umowy o pracę i zgodnego zamiaru stron. Przepis ten nie osłabia praw dziennikarzy do umownego kształtowania zasad i zakresu udzielania praw wydawcom, a nadto pozostaje bez wpływu na wykonywanie przez dziennikarzy autorskich praw osobistych, w szczególności prawa do decydowania o pierwszym publicznym udostępnieniu utworu. Dyrektywa zmienia tę sytuację, konstruując w art. 15 ust. 1 i 2 na rzecz wydawców domniemanie zgodności z prawem działania polegającego na wykonywaniu prawa do decydowania o publicznym udostępnieniu i zwielokrotnieniu materiałów prasowych, kreując jednocześnie na rzecz wydawców nowe prawo pokrewne.

Wydaje się, że dyrektywa 2019/790 osłabiła pozycję prawną dziennikarzy, odbierając im możliwość samodzielnej ochrony interesów i praw, przede wszystkim w sporach z wydawcami, co było dotychczas możliwe na gruncie rozwiązań krajowych, w szczególności art. 12 pr. aut. W świetle art. 15–16 dyrektywy domniemywa się, że prawnie legitymowani do występowania z roszczeniami o ochronę praw autorskich, wskazanych w tych przepisach, stali się wydawcy publikacji prasowych.

¹⁵⁴ J. Taczkowska, *Zawód dziennikarza w Polsce: między misją a posłannictwem*, Bydgoszcz 2012, s. 234.

W dyrektywie 2019/790 przyjęto, że wszystkie opublikowane w ramach jednego numeru (wydania) artykuły prasowe, bez względu na ich autorstwo oraz niezależnie od gatunku (publicystyka, informacja, formy pograniczne), stanowią *en bloc* publikację prasową, do której prawa wyłączne w imieniu twórców może wykonywać wydawca, będąc zarazem uprawnionym z tytułu nowego prawa pokrewnego. Okoliczność ta, jak należy przypuszczać, będzie wywoływała istotne dla dziennikarzy jako autorów materiałów prasowych skutki. Dyrektywa pozbawia bowiem *de facto* dziennikarzy możliwości wykonywania praw wyłącznych, wyposażając w te uprawnienia, w miejsce dziennikarzy, wydawców prasy. Wydawcy stają się więc legitymowani czynnie do wszczęcia i prowadzenia *erga omnes* postępowań o naruszenie prawa do publicznego udostępniania, a także naruszenie prawa do zwielokrotniania utworów. Okoliczność, że wydawcy wykonują te prawa w miejsce dziennikarzy, stanowi konsekwencję, po pierwsze, ustalenia, że wydawcy nie są twórcami publikacji prasowych, po drugie, jest rezultatem decyzji o charakterze normatywnym podjętej przez europejskiego ustawodawcę.

Zatem nawet jeśli przyjąć, że artykuły prasowe mogą być kwalifikowane jako utwory nadające się do samodzielnej eksploatacji, do których dziennikarzom przysługują prawa wyłączne, co – jak się wydaje – potwierdza art. 15 ust. 2 dyrektywy, a także motyw 59¹⁵⁵, to jednak ze względu na treść art. 15 ust. 1 ograniczony został zakres podmiotowy i przedmiotowy roszczeń, jakie mogą zgłaszać dziennikarze. Wydawcy stali się bowiem wyłącznie uprawnieni do wykonywania prawa do zwielokrotniania i prawa do decydowania o publicznym udostępnieniu całości lub części publikacji prasowej. Twórcy, w tym – jak należy sądzić – dziennikarze, mogą w myśl art. 15 ust. 5 domagać się od

¹⁵⁵ Zgodnie z motywem 59 dyrektywy „Ochrona przyznana wydawcom publikacji prasowych na podstawie niniejszej dyrektywy nie powinna naruszać praw twórców i innych podmiotów uprawnionych do utworów i innych przedmiotów objętych ochroną, w tym w odniesieniu do zakresu, w jakim twórcy i inne podmioty uprawnione mogą eksploatować swoje utwory lub inne przedmioty objęte ochroną niezależnie od publikacji prasowej, w skład której wchodzi te utwory lub przedmioty. W związku z tym wydawcy publikacji prasowych nie powinni mieć możliwości powoływania się na przyznaną im w niniejszej dyrektywie ochronę wobec twórców i innych podmiotów uprawnionych, ani wobec innych użytkowników tych samych utworów lub przedmiotów objętych ochroną, którym udzielono zezwolenia. Nie powinno to naruszać ustaleń umownych zawartych między wydawcami publikacji prasowych a twórcami i innymi podmiotami uprawnionymi [...]”.

wydawców udziału w przychodach z tytułu korzystania z ich utworów¹⁵⁶. Jednak nawet i to uprawnienie może zostać ograniczone ze względu na treść łączącej strony umowy, w szczególności umowy o pracę¹⁵⁷. Szczególnie dotkliwie mogą to odczuć autorzy materiałów prasowych wówczas, gdy materiały te powstały w wyniku realizacji innej umowy niż umowa o pracę, a zatem wtedy, gdy ze względu na formę zatrudnienia nie doszło *ex lege* do przeniesienia na wydawców autorskich praw majątkowych¹⁵⁸.

W dyrektywie założono, że twórcy wykazywać będą aktywną postawę w zakresie realizacji ich praw, w szczególności prowadzić będą świadomą politykę licencyjną. Założenie to jest słuszne, ale nie znajduje racji bytu w odniesieniu do dziennikarzy. W rezultacie stwierdzić można, że dyrektywa przyznaje wydawcom generalne upoważnienie do działania w imieniu dziennikarzy, pozbawiając ich *de facto* kontroli nad eksploatowanym przez wydawców utworem. Dyrektywa pomija bowiem szczególne uwarunkowania

¹⁵⁶ W motywie 59 zdanie 4 wskazano, że „Twórcy, których utwory włączono do publikacji prasowej, mają prawo do odpowiedniego udziału w przychodach, jakie uzyskują wydawcy prasy za wykorzystanie ich publikacji prasowych przez dostawców usług społeczeństwa informacyjnego”.

¹⁵⁷ W motywie 59 zdanie 5 zastrzeżono, że prawo do udziału twórców w zyskach osiągniętych przez wydawców z tytułu eksploatacji utworów składających się na publikację prasową „nie powinno [...] naruszać przepisów krajowych dotyczących własności lub wykonywania praw w kontekście umów o pracę”. W zdaniu trzecim wskazano także, że prawo do rekompensaty „Nie powinno [...] naruszać ustaleń umownych zawartych między wydawcami publikacji prasowych a twórcami i innymi podmiotami uprawnionymi”.

¹⁵⁸ Problem ten wymaga szerszego omówienia, co wykracza poza zakres przedmiotowy niniejszej pracy. Wskazać jednak należy, że zgodnie z art. 12 ust. 1 ustawy o prawie autorskim i prawach pokrewnych (ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz.U. z 2022 r., poz. 2509)): „Jeżeli ustawa i umowa o pracę nie stanowią inaczej, pracodawca, którego pracownik stworzył utwór w wyniku wykonywania obowiązków ze stosunku pracy, nabywa z chwilą przyjęcia utworu autorskie prawa majątkowe w granicach wynikających z celu umowy o pracę i zgodnego zamiaru stron”. Pracodawca staje się zatem *ex lege* uprawniony do eksploataowania materiału prasowego oraz uzyskiwania z tego tytułu przychodów bez uzyskiwania zezwolenia dziennikarza co do każdego odrębnego przygotowanego przez niego i przekazanego do opublikowania materiału prasowego. Należy zwrócić uwagę, że zawarte w art. 12 ust. 1 pr. aut. postanowienia dotyczą wyłącznie umów o pracę, a nadto tylko wówczas, gdy „pracownik stworzył utwór w wyniku wykonywania obowiązków ze stosunku pracy”. Przejście autorskich praw majątkowych na wydawcę nie nastąpi zatem *ex lege* w odniesieniu do innych, nieobjętych umową o pracę utworów stworzonych przez pracownika, choćby powstały one w godzinach pracy. Nie dotyczy to także sytuacji, gdy strony inaczej postanowiły w umowie o pracę, a także nie obejmuje innych umów niż prawnopracownicze.

związane z wykonywaniem zawodu dziennikarza jako twórców artykułów. Na gruncie dyrektywy przyjęto zatem, że składające się na wydanie gazety (publikację prasową) artykuły stanowią integralną część utworu, do którego prawa wyłączne (nowe prawo pokrewne) przysługują wydawcy, nadto to wydawca prasy, ze względu na swój nowy status, tj. dostawcy usług udostępniania treści online, stał się zobowiązany i – jednocześnie – uprawniony do wykonywania praw autorskich w imieniu twórców. Skoro bowiem wydawcy zostali wyposażeni w wyłączne prawo do zezwalania lub zabrania na jakiekolwiek podawanie do publicznej wiadomości utworów, a także wyłączne prawo do zezwalania lub zabrania bezpośredniego lub pośredniego, tymczasowego lub stałego zwielokrotniania utworu (art. 15 ust. 1 dyrektywy 2019/790), a nadto zostali wyposażeni w prawo do egzekwowania ochrony prawnej środków technologicznych (art. 15 ust. 3 dyrektywy 2019/790 w zw. z art. 5–8 dyrektywy 2001/29), to oznacza *de facto*, że we wskazanym powyżej zakresie wydawcy wykonują prawa twórców.

Status dziennikarzy został zrównany ze statusem innych twórców, których dzieła są eksploatowane przez prasę. Zawarta w dyrektywie definicja terminu „publikacje prasowe” w powiązaniu z zakresem przyznanego wydawcom prasowym prawa o charakterze wyłącznym do eksploatacji publikacji prasowych konstytuuje na rzecz wydawców nowe prawo pokrewne. Zarazem, mając na uwadze zakres prawa wydawców do ochrony „publikacji prasowej”, a także jego bezwzględny charakter, o czym przesądza art. 16 dyrektywy 2019/790, należy wskazać, że pozycja wydawców została istotnie wzmocniona kosztem ograniczenia monopolu autorskiego twórców materiałów prasowych (utworów przeznaczonych do opublikowania w prasie). Korzystne dla wydawców prasowych jest nie tylko zastosowanie rozwiązań dotyczących zasad korzystania przez nich z praw autorskich do utworów wchodzących w skład publikacji prasowych, ale przede wszystkim uzyskanie statusu dostawcy usług udostępniania treści online, co sytuuje ich w gronie podmiotów korzystających ze szczególnego mechanizmu wyłączania odpowiedzialności (art. 17 ust. 4 dyrektywy 2019/790).

Uzasadniając potrzebę objęcia ochroną publikacji prasowych, ustawodawca europejski wskazał, że „należy uznać organizacyjny i finansowy wkład, jaki wydawcy wnoszą w produkcję publikacji prasowych i stworzyć dla nich zachęty, aby zapewnić stabilność branży wydawniczej, a tym samym zwiększyć

dostępność rzetelnych informacji (motyw 55 dyrektywy 2019/790). Na rzecz wydawców ustanowiony został zatem wyjątek polegający, z jednej strony, na potwierdzeniu gwarancji ochronnych dla publikacji prasowej i wyposażeniu wydawców w roszczenie o zapłatę rekompensaty w razie wykorzystania bez zezwolenia wydawców przez inne podmioty świadczące usługi społeczeństwa informacyjnego fragmentów bądź całości publikacji prasowej, a z drugiej konstruujący domniemanie zgodności z prawem działania wydawców w zakresie, w jakim wykonują oni w imieniu twórców prawo do decydowania o publicznym udostępnieniu utworu i prawo do zwielokrotniania.

Wyjątki polegające na ograniczeniu monopolu twórców w związku ze świadczeniem usług udostępniania treści online zostały także ustanowione w dyrektywie 2019/790 na rzecz innych podmiotów, w szczególności na rzecz organizacji badawczych i instytucji dziedzictwa kulturowego w zakresie, w jakim świadczone przez te podmioty usługi realizują cele badań naukowych, eksploracji tekstów i danych na utworach lub innych przedmiotach objętych ochroną, do których mają zgodny z prawem dostęp (art. 3 ust. 1). Artykuł 2 punkt 2 definiuje „eksplorację tekstów i danych” jako „zautomatyzowaną technikę analityczną służącą do analizowania tekstów i danych w postaci cyfrowej w celu wygenerowania informacji, obejmujących między innymi wzorce, tendencje i korelacje”. R. Markiewicz zauważa, że „eksplorację tekstów i danych” (ang. *text and data mining*, TDM) należy traktować jako postać dozwolonego użytku, który może być realizowany w dwóch wymiarach: a) „użytek badawczy TDM” realizowany przez organizacje badawcze i instytucje dziedzictwa narodowego oraz b) „komercyjny TDM” realizowany przez pozostałe podmioty w celach analizy, transformowania na wersję cyfrową, przechowywania w celu dalszych badań i zwielokrotniania¹⁵⁹.

Wyłom w ochronie praw autorskich (wyjątek) został ustanowiony także na rzecz placówek edukacyjnych, aby umożliwić cyfrowe korzystanie z utworów i innych przedmiotów objętych ochroną w celu zilustrowania w ramach nauczania, w zakresie uzasadnionym przez niekomercyjny cel (art. 5). Wyjątek przewidziano także na rzecz instytucji dziedzictwa kulturowego w celu

¹⁵⁹ R. Markiewicz, *Eksploracja tekstów i danych (art. 3 i 4)*, [w:] *Prawo autorskie na jednolitym rynku cyfrowym. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790*, Warszawa 2021.

zezwoleń tym instytucjom na wykonywanie kopii wszelkich utworów lub innych przedmiotów objętych ochroną, które znajdują się na stałe w ich zbiorach, niezależnie od formatu lub nośnika, do celów zachowania takich utworów lub innych przedmiotów objętych ochroną i w zakresie potrzebnym do tego zachowania (art. 7).

Cechą odróżniającą usługi udostępniania treści online od pozostałych usług społeczeństwa informacyjnego jest, przede wszystkim, charakter udostępnianych treści cyfrowych. Stanowią one przedmiot ochrony, do którego prawa wyłączne przysługują ich twórcom albo – w drodze ustanowionych w dyrektywie wyjątków – podmiotom wskazanym w przepisach dyrektywy. Zarazem tylko wtedy usługa kwalifikuje się do katalogu udostępniania treści online, kiedy dotyczy dużej ilości chronionych treści i jest wykonywana przez usługodawcę w ramach prowadzonej przez niego działalności gospodarczej, a nadto tylko wówczas, gdy „odgrywa ważną rolę na rynku treści online” (motyw 62). Niebagatelne znaczenie ma także, dla wyodrębnienia usług udostępniania treści online z katalogu pozostałych usług społeczeństwa informacyjnego, stosunek usługodawcy do udostępnianych przez niego treści. Dostawca usług udostępniania treści online, w przeciwieństwie do pośredników internetowych, nie może pozostawać pasywny wobec treści. Ustawodawca europejski oczekuje, by wykazywał się wysokim poziomem starannego działania, co zobowiązuje go do filtrowania i monitorowania udostępnianych treści pod kątem ewentualnych naruszeń praw wyłącznych, w tym praw autorskich.

b. USŁUGA DOSTARCZANIA TREŚCI CYFROWYCH

Ustalenie zasad dostarczania treści cyfrowych jest przedmiotem regulacji zawartych w dwóch dyrektywach (tzw. dyrektywy konsumenckie): dyrektywie Parlamentu Europejskiego i Rady (UE) 2019/770 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych i usług cyfrowych¹⁶⁰ oraz dyrektywie Parlamentu Europejskiego i Rady

¹⁶⁰ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/770 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych i usług cyfrowych (Dz.U. UE L Nr 136, s. 1 oraz Dz.U. UE L Nr 305, s. 60), dalej: dyrektywa 2019/770 albo dyrektywa o dostarczaniu treści cyfrowych.

(UE) 2019/771 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów sprzedaży towarów¹⁶¹. Zasadniczym celem obu dyrektyw było przyczynienie się do właściwego funkcjonowania rynku wewnętrznego i zapewnienie przy tym wysokiego poziomu ochrony konsumentów, przede wszystkim przez ustanowienie wspólnych przepisów dotyczących niektórych wymagań w odniesieniu do umów zawartych między przedsiębiorcami a konsumentami o dostarczanie treści cyfrowych lub usług cyfrowych, w szczególności przepisów dotyczących: zgodności treści cyfrowej lub usługi cyfrowej z umową, środków ochrony prawnej w przypadku braku zgodności treści cyfrowej lub usługi cyfrowej z umową lub ich niedostarczenia oraz sposobów korzystania z tych środków, oraz zmiany treści cyfrowej lub usługi cyfrowej, a także przez ustanowienie wspólnych przepisów dotyczących niektórych wymagań w odniesieniu do umów sprzedaży zawartych między sprzedawcą a konsumentem, w tym przepisów dotyczących zgodności towarów z umową, środków ochrony prawnej przysługujących w przypadku braku takiej zgodności, sposobów korzystania z tych środków, a także gwarancji handlowych¹⁶².

W prawie krajowym przepisy regulujące świadczenie usługi „dostarczania treści online (cyfrowych)” zostały zawarte w ustawie o ochronie praw konsumentów implementującej postanowienia dyrektyw cyfrowych¹⁶³. W uzasadnieniu do projektu ustawy krajowej wskazano, że „zagadnienia umów o dostarczanie treści cyfrowej lub usługi cyfrowej nie stanowiły dotychczas przedmiotu zainteresowania polskiego ustawodawcy, dlatego też brak punktu odniesienia dla proponowanych przepisów”¹⁶⁴.

¹⁶¹ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/771 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów sprzedaży towarów, zmieniająca rozporządzenie (UE) 2017/2394 oraz dyrektywę 2009/22/WE oraz uchylająca dyrektywę 1999/44/WE (Dz.U. UE L Nr 136, s. 28 oraz Dz.U. UE L Nr 305, s. 63), dalej: dyrektywa towarowa. Dyrektywa cyfrowa i dyrektywa towarowa weszły w życie z dniem 11 czerwca 2019 r., a państwa członkowskie zobowiązane są do przyjęcia implementujących je przepisów do dnia 1 lipca 2021 r., z mocą od dnia 1 stycznia 2022 r.

¹⁶² Rządowy projekt ustawy o zmianie ustawy o prawach konsumenta oraz niektórych innych ustaw. Uzasadnienie, Druk Sejmowy nr 2425, <https://www.sejm.gov.pl/Sejm9.nsf/druk.xsp?nr=2425> (dostęp: 4.09.2023).

¹⁶³ Ustawa z dnia 30 maja 2014 r. o prawach konsumenta (t.j. Dz.U. z 2020 r., poz. 287 z późn. zm.). Ustawa wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2019/770 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych i usług cyfrowych (Dz.U. UE L Nr 136, s. 1 oraz Dz.U. UE L Nr 305, s. 60).

¹⁶⁴ Rządowy projekt ustawy o zmianie ustawy o prawach konsumenta..., s. 10.

Ustawodawca wyłączył z zakresu stosowania ustawy model biznesowy opierający się na płatności wyłącznie danymi osobowymi. Ustawą z dnia 4 listopada 2022 r. dodany został art. 3 ust. 1 pkt 11¹⁶⁵, zgodnie z którym przepisów ustawy o prawach konsumenta nie stosuje się do umów o dostarczanie treści cyfrowej lub usługi cyfrowej, jeżeli konsument nie jest zobowiązany do świadczeń innych niż dostarczanie danych osobowych, a dane te są przetwarzane przez przedsiębiorcę wyłącznie w celu wykonania umowy lub obowiązku ustawowego. Zastosowane wyłączenie stanowi realizację zawartego w motywie 25 dyrektywy cyfrowej zalecenia mówiącego, że jeżeli treści cyfrowe lub usługi cyfrowe nie są dostarczane w zamian za zapłatę ceny, dyrektywa nie powinna mieć zastosowania. Ma to miejsce w sytuacji, gdy przedsiębiorca zbiera dane osobowe jedynie w celu dostarczenia treści cyfrowych lub usługi cyfrowej lub jedynie w celu spełnienia wymogów prawnych. Mogą to być przypadki, w których np. rejestracja konsumenta jest wymagana przez obowiązujące przepisy prawa ze względów bezpieczeństwa i na potrzeby identyfikacji. Dyrektywa nie powinna mieć także zastosowania, kiedy przedsiębiorca zbiera wyłącznie metadane, takie jak informacje dotyczące urządzenia należącego do konsumenta lub historii przeglądania, z wyjątkiem, gdy sytuacja ta jest uznawana za umowę na mocy prawa krajowego. Nie powinna ona również mieć zastosowania wówczas, gdy konsument, który nie zawarł umowy z przedsiębiorcą, musi obejrzeć reklamy wyłącznie w celu uzyskania dostępu do treści cyfrowych lub usługi cyfrowej. Państwa członkowskie powinny jednak zachować swobodę rozszerzenia stosowania dyrektywy cyfrowej na takie sytuacje lub odmiennego uregulowania takich sytuacji, które są wyłączone z zakresu stosowania niniejszej dyrektywy (motyw 25 dyrektywy cyfrowej).

Usługa dostarczania treści cyfrowych może być wykonywana w ramach jednego z dwóch modeli biznesowych, tj.:

1. modelu zakładającego, że usługi dostarczania treści cyfrowych są realizowane odpłatnie na podstawie umowy łączącej dostawcę usługi z jej odbiorcą (użytkownikiem internetu) albo
2. modelu zakładającego, że dostarczanie danych następuje na podstawie płatności danymi osobowymi.

¹⁶⁵ Ustawa z dnia 4 listopada 2022 r. o zmianie ustawy o prawach konsumenta, ustawy – Kodeks cywilny oraz ustawy – Prawo prywatne międzynarodowe (Dz.U., poz. 2337). Ustawa weszła w życie z dniem 1 stycznia 2023 r.

Modele biznesowe oparte na zapłacie za usługę cyfrową danymi występują w różnych formach na znacznej części rynku. Ustawodawca europejski dostrzega tę okoliczność w motywie 24 dyrektywy cyfrowej. Zauważa zarazem, że prawo do ochrony danych osobowych jest prawem podstawowym i nie może być traktowane jak towar (motyw 24 dyrektywy 2019/770). Stąd płatność danymi osobowymi powinna podlegać szczególnemu reżimowi prawnemu, potwierdzonemu w treści zawieranych z konsumentem umów. Podczas gdy niektóre z tych usług są finansowane z płatności użytkownika, inne są świadczone bez płatności pieniężnych ze strony konsumenta, zamiast tego finansowane są ze sprzedaży usług reklamowych online umożliwiających dotarcie do osób, których dane dotyczą. Do celów takiej reklamy zachowanie użytkownika śledzi się często w sposób, którego użytkownik nie jest świadomy i może nie wynikać bezpośrednio z charakteru świadczonej usługi, co w praktyce prawie uniemożliwia osobie, której dane dotyczą, dokonanie świadomego wyboru co do wykorzystania jej danych¹⁶⁶.

O ile zatem dopuszczalne jest realizowanie modeli biznesowych opierających się na „płatności danymi”, to jednak realizacja tego modelu, w szczególności, jeśli polega na dostarczaniu treści cyfrowych w zamian za dane osobowe, wymaga – dla potwierdzenia legalności przetwarzania danych – wykazania co najmniej jednej z katalogu przesłanek legalizujących przetwarzanie danych wymienionych w art. 6 ust. 1 RODO¹⁶⁷. Dane osobowe mogą być przekazywane przedsiębiorcy w momencie zawarcia umowy lub w późniejszym terminie, np. gdy konsument udziela przedsiębiorcy zgody na wykorzystanie danych osobowych, które może on przesyłać lub wytworzyć w związku z korzystaniem z treści cyfrowych lub z usługi cyfrowej¹⁶⁸.

¹⁶⁶ Wytyczne Europejskiej Rady Ochrony Danych Osobowych 2/2019 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. b) rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO) w kontekście świadczenia usług online na rzecz osób, których dane dotyczą, 8.10.2019 r., https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_pl.pdf (dostęp: 5.09.2023).

¹⁶⁷ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. UE L Nr 119, s. 1 z późn. zm.).

¹⁶⁸ Przykładowo niniejsza dyrektywa powinna mieć zastosowanie w przypadku, gdy konsument zakłada konto w mediach społecznościowych oraz podaje imię i nazwisko oraz

Skoro dyrektywa cyfrowa, a w jej następstwie także ustawa o prawach konsumenta, nie zawiera postanowień regulujących model biznesowy oparty na płatności danymi, to ocenę prawidłowości świadczenia usługi dostarczania treści cyfrowych należy dokonywać na podstawie ogólnych przepisów prawa, w tym zawartych w ogólnym rozporządzeniu o ochronie danych osobowych. W doktrynie pojawiło się pytanie o to, czy RODO w ogóle dopuszcza takie sytuacje, gdy dochodzi do świadczenia treści lub usług cyfrowych przez przedsiębiorcę w zamian za dane osobowe¹⁶⁹.

Warunki dostępu do treści cyfrowych, w szczególności ustalenie, że dostęp ten może odbywać się zarówno odpłatnie, jak i nieodpłatnie, określają granice swobody przepływu informacji i wolności wypowiedzi w internecie. Wobec powyższego ustalenie, że dostęp do treści cyfrowych jest możliwy tylko pod warunkiem zapłaty ceny, w szczególności wyrażonej w danych osobowych, musi prowadzić do wniosku, że cena ta ma wpływ na korzystanie z wolności wypowiedzi i jej granice. Mając na uwadze zasadnicze zagadnienie objęte analizą zawartą w niniejszej rozprawie, istotne wydaje się ustalenie, jakie konsekwencje dla wolności wypowiedzi generuje realizacja każdego ze wskazanych modeli biznesowych, tj. 1) modelu dostarczania treści w ramach umów odpłatnych w klasycznym rozumieniu oraz 2) modelu dostarczania treści w zamian za zapłatę danymi. Najdalej idące pytanie dotyczy tego, czy jest możliwe uzyskanie dostępu do treści cyfrowych nieodpłatnie, w szczególności z pominięciem zapłaty danymi osobowymi.

O ile umowy odpłatne o dostarczanie treści cyfrowych objęte szczegółową regulacją zawartą w dyrektywach cyfrowych i ustawie o prawach konsumenta nie nastroczają, w ujęciu ogólnym, powodów do twierdzenia, że naruszają wolność wypowiedzi, o tyle wątpliwości takie mogą dotyczyć umów realizowanych w ramach drugiego z modeli biznesowych, tj. dostarczania treści

adres e-mail do celów innych niż jedynie dostarczenie treści cyfrowych lub usługi cyfrowej lub innych niż spełnienie wymogów prawnych. Powinna ona również mieć zastosowanie w przypadku, gdy konsument udziela zgody na przetwarzanie przez przedsiębiorcę do celów marketingowych przesyłanych przez siebie materiałów stanowiących dane osobowe, takich jak zdjęcia lub wpisy. Państwa członkowskie powinny jednak zachować swobodę decydowania o tym, czy zostały spełnione wymogi dotyczące zawierania, istnienia i skuteczności umowy na mocy prawa krajowego (motyw 24 dyrektywy 2019/770).

¹⁶⁹ M. Gumularz, *Zapłata danymi osobowymi – co musisz wiedzieć o nowej dyrektywie o dostarczaniu treści cyfrowych i usług cyfrowych*, LEX/el. 2019.

w zamian za dane osobowe, wówczas, gdy dane te nie są niezbędne do świadczenia usługi, a nadto nie stanowią zapłaty tytułem wykonania innej usługi niż usługa główna (dostarczenie treści).

Z jednej strony istotne jest zatem, kiedy pozyskanie przez dostawcę danych jest „niezbędne” w celu wykonania usługi dostarczenia treści a, po wtóre, czy niedostarczenie treści stanowi ingerencję w wolność wypowiedzi użytkownika internetu.

Bez podjęcia szczegółowej analizy treści pojęcia „dane osobowe” oraz zasad ich przetwarzania i statusu administratora na gruncie RODO, co wykraczałoby poza ramy niniejszej rozprawy, sformułowane poniżej uwagi dotyczyć będą wyłącznie wskazanej w art. 6 ust. 1 lit. b RODO przesłanki „niezbędności” pozyskania danych do wykonania usługi polegającej na „dostarczeniu treści cyfrowych”. Zapewnienie swobodnego przepływu wypowiedzi i informacji w internecie jest bowiem ujmowane zarówno jako cel o charakterze publicznym, jak i zadanie państwa uzasadnione indywidualnym interesem jednostek realizujących prawo podstawowe do swobody ekspresji. *A contrario* odmowa dostarczenia treści cyfrowych stanowi wkroczenie w prawa podstawowe jednostki i naruszenie wartości mającej znaczenie dla realizacji celów publicznych.

Artykuł 6 ust. 1 lit. b) RODO stanowi podstawę prawną przetwarzania danych w zakresie, w jakim „przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy”. Wspiera to swobodę prowadzenia działalności gospodarczej zagwarantowaną w art. 16 Karty i odzwierciedla fakt, że czasami zobowiązań umownych wobec osoby, której dane dotyczą, nie można wykonać bez przekazania przez tę osobę pewnych danych osobowych. Jeżeli określone przetwarzanie jest nieodłączną częścią świadczonej usługi, w interesie obu stron leży przetwarzanie tych danych, ponieważ w przeciwnym razie usługa nie mogłaby zostać zrealizowana, a umowa nie mogłaby zostać zawarta ani wykonana¹⁷⁰. EROD dostrzegła potrzebę odniesienia wskazanej w art. 6 ust. 1 lit. b przesłanki do świadczenia „usług społeczeństwa informacyjnego”, które – jak w zauważono w wytycznych

¹⁷⁰ Wytyczne Europejskiej Rady Ochrony Danych Osobowych 2/2019 w sprawie przetwarzania danych osobowych...

z dnia 8 października 2019 r. (wytyczne 2.o) – obejmują usługi nieopłacane bezpośrednio przez osoby, które są ich odbiorcami¹⁷¹. W art. 5 ust. 1 lit. b) RODO przewidziano zasadę ograniczenia celu, zgodnie z którą dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami. W art. 5 ust. 1 lit. c) RODO przewidziano zasadę minimalizacji danych, tj. przetwarzania danych w zakresie ograniczonym do tego, co niezbędne do osiągnięcia celu. Ocena ta uzupełnia oceny niezbędności na podstawie art. 6 ust. 1 lit. b)¹⁷². EROD wskazała, że zasady zarówno ograniczenia celu, jak i minimalizacji danych mają szczególne znaczenie w umowach o świadczenie usług online, które zazwyczaj nie podlegają indywidualnym negocjacjom. Pojęcie tego, co jest „niezbędne do wykonania umowy”, nie stanowi jedynie oceny tego, na co zezwalają postanowienia umowy lub co obejmuje jej zakres.

Pojęcie niezbędności ma odrębne znaczenie w prawie Unii Europejskiej, które musi odzwierciedlać cele prawa o ochronie danych i ochronie życia prywatnego jako praw podstawowych¹⁷³. Zgodnie z wytycznymi EROD art. 6 ust. 1 lit. b) nie obejmuje przetwarzania, które jest przydatne, ale nie jest obiektywnie niezbędne do wykonania usługi objętej umową lub podjęcia odpowiednich działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy, nawet jeżeli jest ono niezbędne do innych celów biznesowych administratora danych. Termin „niezbędne” obejmuje połączoną, opartą na faktach ocenę przetwarzania „w odniesieniu do zamierzonego celu oraz tego, czy przetwarzanie jest mniej inwazyjne w porównaniu z innymi metodami osiągnięcia tego samego celu”¹⁷⁴. Ustalenie istnienia przesłanki niezbędności – jak wskazuje EROD – „zależy [...] nie tylko od interesów administratora danych, ale również od uzasadnionych interesów osoby, której dane dotyczą, w momencie zawierania umowy oraz od tego, czy umowę można nadal uznać za »wykonaną« bez przetwarzania takich danych”¹⁷⁵. EROD wskazała, że to, czy art. 6 ust. 1 lit. b) ma zastosowanie, można ocenić, odpowiadając na następujące pytania:

¹⁷¹ Tamże s. 4. EROD odwołała się w tym zakresie do motywu 18 dyrektywy 2000/31.

¹⁷² Tamże, s. 6.

¹⁷³ Tamże, s. 8.

¹⁷⁴ Tamże.

¹⁷⁵ Tamże, s. 10.

1. Jaki jest charakter usługi świadczonej na rzecz osoby, której dane dotyczą? Jakie są jej cechy charakterystyczne?
2. Jakie jest dokładne uzasadnienie zawarcia umowy (tj. jej istota i główny przedmiot)?
3. Jakie są istotne elementy umowy?
4. Jakie są wzajemne interesy i oczekiwania stron umowy? W jaki sposób usługa jest upowszechniana lub reklamowana osobie, której dane dotyczą? Czy zwykły użytkownik usługi może zasadnie oczekiwać, że z uwagi na charakter usługi planowane przetwarzanie będzie miało miejsce w celu wykonania umowy, której jest stroną?¹⁷⁶.

Zgodnie ze stanowiskiem EROD przesłanka niezbędności nie uzasadnia:

1. reklamy behawioralnej,
2. personalizacji treści,
3. profilowania,
4. równoważenia danych osobowych z płatnością (uprzedmiotowienie danych).

Na przesłankę niezbędności w celu zawarcia i wykonania umowy online dostawca nie będzie mógł powoływać się wówczas, gdy dane mają być przetwarzane:

1. w celu reklamy behawioralnej („przetwarzanie danych osobowych do celów reklamy behawioralnej nie jest niezbędne do wykonania umowy na usługi online. Stwierdzenie, że umowa nie została wykonana ze względu na brak reklamy behawioralnej nie jest argumentem przekonującym [...] Art. 6 ust. 1 lit. b) nie może stanowić podstawy prawnej dla internetowej reklamy behawioralnej tylko dlatego, że reklama taka pośrednio finansuje świadczenie usługi”);
2. w odniesieniu do tworzenia profilu dotyczącego upodobań i stylu życia użytkownika („konieczność przetwarzania w celu wykonania umowy nie jest odpowiednią podstawą prawną w odniesieniu do tworzenia

¹⁷⁶ Niedopuszczalne jest powołanie się przez administratora (dostawcę usługi) na przesłankę niezbędności z art. 6 ust. 1 lit. b, jeżeli administratorzy danych nie mogą wykazać, że: a) umowa istnieje, b) umowa jest ważna na mocy obowiązujących przepisów prawa umów oraz c) przetwarzanie jest obiektywnie niezbędne w celu wykonania umowy, administrator danych powinien rozważyć zastosowanie innej podstawy prawnej przetwarzania (tamże, s. 12).

- profilu dotyczącego upodobań i stylu życia użytkownika w oparciu o jego kliknięcia na stronie internetowej i zakupione przedmioty. Wynika to z tego, że administratorowi danych nie zlecono tworzenia profili, a raczej na przykład dostarczanie określonych towarów i usług¹⁷⁷);
3. jeśli przekazanie danych pozbawia użytkownika kontroli nad danymi osobowymi jako prawem osobistym niepodlegającym zrzeczeniu się lub zbyciu („danych osobowych nie można uznać za towar handlowy. Nawet jeżeli osoba, której dane dotyczą, może wyrazić zgodę na przetwarzanie danych osobowych, nie może na podstawie takiej zgody oddać przysługujących jej praw podstawowych”). EROD zauważa, że utracona kontrola nad danymi osobowymi może być nie do odzyskania, co dodatkowo przemawia za potrzebą szczególnej ich ochrony¹⁷⁸;
 4. jeśli łączy się z personalizacją treści („To, czy personalizacja stanowi nieodłączny element usługi online, zależeć będzie od charakteru świadczonej usługi, oczekiwań przeciętnej osoby, której dane dotyczą, w świetle nie tylko warunków świadczenia usługi, ale również sposobu jej reklamowania użytkownikom, jak również od tego, czy usługę można świadczyć bez personalizacji. Jeżeli personalizacja treści nie jest obiektywnie niezbędna do wykonania danej umowy, na przykład gdy spersonalizowane treści służą zwiększeniu zaangażowania użytkownika w usługę, a nie stanowią jej integralnej części, administratorzy danych powinni, w stosownych przypadkach, rozważyć zastosowanie innej podstawy prawnej¹⁷⁹).

Pozostaje do rozważenia, czy nieprzekazanie danych osobowych przez usługobiorcę obiektywnie uniemożliwia „dostarczenie treści cyfrowej”, a jeśli tak, o jakie dane osobowe chodzi, oraz czy przekazanie danych determinuje

¹⁷⁷ Grupa robocza art. 29 (2014), opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE (WP217), s. 17.

¹⁷⁸ Oprócz samego faktu, że wykorzystywanie danych osobowych podlega regulacjom RODO, istnieją dodatkowe powody, dla których przetwarzanie danych osobowych różni się pojęciowo od płatności pieniężnych, np. pieniądze są policzalne, co oznacza, że ceny można porównać na konkurencyjnym rynku, a płatności pieniężnych dokonuje się zazwyczaj z udziałem osoby, której dane dotyczą. Ponadto dane osobowe można wykorzystywać w ramach kilku usług jednocześnie. Jeżeli utraci się kontrolę nad danymi osobowymi, niekoniecznie uda się ją odzyskać (zob. Wytyczne Europejskiej Rady Ochrony Danych Osobowych 2/2019 w sprawie przetwarzania danych osobowych...).

¹⁷⁹ Tamże, s. 16.

wyrażenie zgody albo uzasadnia realizowanie innych celów w tym marketingowych przez dostawcę usług online. Inaczej mówiąc, czy udzielenie dostępu do treści cyfrowej musi wiązać się z profilowaniem, personalizacją albo oferowaniem reklamy behawioralnej. Na gruncie orzecznictwa europejskiego nie ulega wątpliwości, że dane i metadane¹⁸⁰, jeśli pozwalają – osobno lub w powiązaniu ze sobą – na zidentyfikowanie osoby fizycznej, co nie musi oznaczać ustalenia jej imienia i nazwiska¹⁸¹, stanowią dane osobowe, a w konsekwencji ich przetwarzanie powinno następować zgodnie z RODO¹⁸².

Ocena niezbędności pozyskiwania danych osobowych użytkowników była przedmiotem oceny TSUE w wyroku z dnia 4 lipca 2023 r. w sprawie Meta przeciwko Bundeskartellamt¹⁸³. Model biznesowy internetowej

¹⁸⁰ Metadane to dane powiązane z każdą opublikowaną w serwisie informacją, określające: podmiot udostępniający informację, datę wytworzenia informacji, osobę lub jednostkę, która wytworzyła informację lub odpowiada za jej treść, datę publikacji informacji i osobę ją publikującą oraz datę modyfikacji informacji i osobę ją modyfikującą; zob. *Instrukcja obsługi*, Generalny Inspektor Ochrony Danych Osobowych, <https://archiwum.giodo.gov.pl/pl/542/3726> (dostęp: 4.09.2023). W literaturze wskazuje się na różne kategorie metadanych i proponuje ich systematyzację, np. wyróżniając: metadane strukturalne, opisowe i administracyjne. Metadane opisowe służą do odnajdywania i identyfikacji kluczowych informacji, które umożliwiają lokalizację obiektu. Za przykład mogą służyć informacje o autorze, słowach kluczowych, wydawnictwie czy tytule. Metadane strukturalne opisują w szczególności budowę obiektu (np. dokumentu). Metadane administracyjne odnoszą się do informacji technicznych, w których zawarte są np. informacje o czasie i sposobie utworzenia pliku (zob. W. Mincewicz, *Metadane – cichy zabójca prywatności*, „Studia Politologiczne” 2019, nr 54, s. 235).

¹⁸¹ Nie jest wymagana znajomość nazwiska lub adresu (fizycznego) osoby odwiedzającej, ponieważ zgodnie z motywem 26 RODO takie wyróżnienie osób wystarczy, aby można było zidentyfikować osobę odwiedzającą; zob. T. Ochocki, *Czy Google Analytics jest zgodne z RODO? – decyzja CNIL*, 27.06.2022, <https://odo24.pl/blog-post.czy-google-analytics-jest-zgodne-rod-odecycja-cnil> (dostęp: 4.09.2023).

¹⁸² Identyfikatory internetowe, takie jak adresy IP lub informacje przechowywane w plikach cookie, mogą być powszechnie wykorzystywane do identyfikacji użytkownika, zwłaszcza w połączeniu z innymi podobnymi rodzajami informacji. Ilustruje to motyw 30 RODO, zgodnie z którym przypisanie identyfikatorów internetowych, takich jak adresy IP i identyfikatory plików cookie, osobom fizycznym lub ich urządzeniom może skutkować zostawianiem śladów, które w szczególności w połączeniu z unikatowymi identyfikatorami i innymi informacjami uzyskanymi przez serwery mogą być wykorzystywane do tworzenia profili i do identyfikowania tych osób (zob. tamże).

¹⁸³ Wyrok TS z dnia 4 lipca 2023 r. w sprawie Meta Platforms Inc., dawniej Facebook Inc., i in. przeciwko Bundeskartellamt, C-252/21, pkt 102, LEX nr 3576613 (dalej: Wyrok TS w sprawie Meta przeciwko Bundeskartellamt). Model biznesowy internetowej sieci społecznościowej Facebook jest oparty na finansowaniu pochodzącym z reklam

sieci społecznościowej Facebook jest oparty na finansowaniu pochodzącym z reklam internetowych, które są dostosowane do indywidualnych użytkowników sieci społecznościowej, w szczególności w zależności od ich zachowań konsumenckich, zainteresowań, siły nabywczej i sytuacji życiowej. Pod względem technicznym tego typu reklama jest możliwa dzięki zautomatyzowanemu tworzeniu bardzo szczegółowych profili użytkowników tej sieci i usług internetowych oferowanych na poziomie grupy Meta. W tym celu, poza danymi dostarczonymi bezpośrednio przez użytkowników przy rejestracji w odpowiednich serwisach internetowych, zbierane są inne dane o użytkownikach i urządzeniach w ramach sieci społecznościowej i serwisów internetowych grupy Meta oraz poza nimi i łączone z poszczególnymi kontami tych użytkowników. Dokonanie całościowego przeglądu tych danych pozwala na wyciągnięcie szczegółowych wniosków na temat preferencji i zainteresowań tych użytkowników (pkt 27). Dane te są przetwarzane przez Meta Platforms Ireland na podstawie umowy w przedmiocie korzystania z tej sieci, do której użytkownicy sieci społecznościowej Facebook przystępują poprzez kliknięcia przycisku „rejestracja” i zaakceptowanie w ten sposób ustanowionych przez tę spółkę ogólnych warunków umownych. Akceptacja tych warunków jest konieczna do tego, aby móc korzystać z sieci społecznościowej Facebook. W zakresie dotyczącym przetwarzania danych osobowych te ogólne warunki odsyłają do zasad korzystania z tych danych oraz plików cookies udostępnionych przez tę spółkę. Zgodnie z powyższymi zasadami Meta Platforms Ireland zbiera dane o użytkownikach i urządzeniach dotyczące działań tych użytkowników w ramach sieci społecznościowej i poza nią i łączy je z kontami Facebook tych użytkowników. W przypadku tych ostatnich danych, dotyczących działalności prowadzonej poza siecią społecznościową (zwanych dalej

internetowych, które są dostosowane do indywidualnych użytkowników sieci społecznościowej, w szczególności w zależności od ich zachowań konsumenckich, zainteresowań, siły nabywczej i sytuacji życiowej. Pod względem technicznym tego typu reklama jest możliwa dzięki zautomatyzowanemu tworzeniu bardzo szczegółowych profili użytkowników tej sieci i usług internetowych oferowanych na poziomie grupy Meta. W tym celu, poza danymi dostarczonymi bezpośrednio przez użytkowników przy rejestracji w odpowiednich serwisach internetowych, zbierane są inne dane o użytkownikach i urządzeniach w ramach sieci społecznościowej i serwisów internetowych grupy Meta oraz poza nimi i łączone z poszczególnymi kontami tych użytkowników. Dokonanie całościowego przeglądu tych danych pozwala na wyciągnięcie szczegółowych wniosków na temat preferencji i zainteresowań tych użytkowników.

również „danymi off-Facebook”), chodzi – po pierwsze – o dane dotyczące przeglądanych stron internetowych i aplikacji osób trzecich, które są połączone z Facebookiem za pomocą interfejsów programowania – „Facebook Business Tools”, i – po drugie – o dane dotyczące korzystania z innych należących do grupy Meta usług internetowych, takich jak Instagram, WhatsApp, Oculus oraz – do dnia 13 marca 2020 r. – Masquerade (pkt 28). Federalny urząd ds. ochrony konkurencji wszczął przeciwko Meta Platforms, Meta Platforms Ireland i Facebook Deutschland postępowanie, po przeprowadzeniu którego wydaną w dniu 6 lutego 2019 r. na podstawie § 19 ust. 1 i § 32 GWB decyzją zakazał im w istocie uzależniania w ogólnych warunkach umownych korzystania z sieci społecznościowej Facebook przez zamieszkałych w Niemczech użytkowników prywatnych od przetwarzania ich danych off-Facebook i dokonywania tego przetwarzania tych danych bez ich zgody na podstawie obowiązujących wówczas ogólnych warunków umownych. Ponadto urząd ten nakazał im dostosowanie tych ogólnych warunków umownych w taki sposób, aby jasno z nich wynikało, że dane te nie będą zbierane, łączone z kontami użytkowników Facebook ani wykorzystywane bez zgody danego użytkownika, i doprecyzował, że taka zgoda jest nieważna, jeżeli stanowi ona warunek korzystania z sieci społecznościowej (pkt 29). Co prawda niemiecki Urząd Federalny uzasadnił decyzję, wskazując na nadużycie przez firmę Meta pozycji dominującej, ale przedmiotem ustaleń TSUE stały się także kwestie dotyczące ogólnych zasad i dopuszczalności zbierania i wykorzystywania danych osobowych przez Meta. Ustalenie podlegało w szczególności, czy zbieranie przez Meta danych jest rzeczywiście niezbędne w rozumieniu art. 6 ust. 1 lit. b RODO do wykonania usługi online na rzecz użytkowników sieci Facebook. Sąd niemiecki ocenił, że nie można uznać, iż użytkownicy sieci społecznościowej Facebook wyrazili zgodę na przetwarzanie, a w konsekwencji konieczne było zwrócenie się do TSUE z pytaniem, czy przetwarzanie danych przez META spełnia choć jedną z pozostałych przesłanek zgodności z prawem, o których mowa w art. 6 ust. 1 lit. b)–f) RODO (pkt 88).

W celu powołania się na przesłankę z art. 6 ust. 1 lit. b (niezbędność do wykonania umowy), jak stwierdził TSUE:

Administrator musi być w stanie wykazać, dlaczego główny cel umowy nie mógłby zostać osiągnięty bez rozpatrywanego przetwarzania [...]. Bez

znaczenia w tym względzie jest jako taka okoliczność polegająca na tym, że takie przetwarzanie jest wymienione w umowie lub że jest ono jedynie przydatne do jej wykonania. Elementem decydującym o zastosowaniu uzasadnienia, o którym mowa w art. 6 ust. 1 akapit pierwszy lit. b) RODO, jest bowiem to, że przetwarzanie danych osobowych dokonywane przez administratora ma istotne znaczenie dla prawidłowego wykonania umowy zawartej między nim a osobą, której dane dotyczą, i co za tym idzie, że nie istnieją inne dające się zastosować, mniej inwazyjne, rozwiązania (pkt 99).

Nie jest – w ocenie TSUE – wystarczającym uzasadnieniem przetwarzania danych personalizacja treści. TSUE stwierdził, że „personalizacja treści nie wydaje się konieczna do oferowania użytkownikowi usług internetowej sieci społecznościowej. Usługi te mogą być w odpowiednim przypadku świadczone na rzecz użytkownika w formie równoważnej alternatywy, która nie wiąże się z taką personalizacją, skutkiem czego nie jest ona obiektywnie niezbędna do osiągnięcia celu stanowiącego integralną część tych właśnie usług”¹⁸⁴. Wystarczającym uzasadnieniem przetwarzania nie jest także powołanie się przez Meta na obowiązek „ciągłego i niezakłóconego korzystania z usług własnych grupy Meta”. TSUE stwierdził, że korzystanie z innych usług oferowanych przez grupę Meta nie jest konieczne do świadczenia usługi dostępu do treści Facebook. TSUE przypomniał, że przesłankę, zgodnie z którą przetwarzanie musi być niezbędne, należy badać łącznie z zasadą tzw. minimalizacji danych, ustanowioną w art. 5 ust. 1 lit. c) RODO, zgodnie z którą dane osobowe muszą być „adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane”¹⁸⁵. TSUE stwierdził, że nie tylko nie zachodzą przesłanki z art. 6 ust. 1 lit. a–c, ale ponadto charakter świadczonej usługi nie pozwala powoływać się przez Meta na przesłankę wskazaną w art. 6 ust. 1 lit. f, tj. „niezbędności przetwarzania do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora”. Nieodpłatność usługi nie zawsze uzasadnia pozyskiwania przez administratora danych osobowych użytkowników. TSUE stwierdził, że:

¹⁸⁴ Wyrok TS w sprawie Meta przeciwko Bundeskartellamt, pkt 102.

¹⁸⁵ Wyrok TS z dnia 11 grudnia 2019 r. w sprawie Asociația de Proprietari bloc M5A-ScaraA, C-708/18, pkt 48.

pomimo nieodpłatności usług internetowej sieci społecznościowej takiej jak Facebook jej użytkownik nie może, racjonalnie rzecz biorąc, spodziewać się, że operator tej sieci społecznościowej będzie przetwarzał bez jego zgody jego dane osobowe w celu personalizacji reklamy. W tych okolicznościach należy uznać, że interesy i prawa podstawowe takiego użytkownika mają pierwszeństwo przed interesem, jaki ma w takiej personalizacji reklamy operator sieci społecznościowej, który finansuje za pomocą tej reklamy swoją działalność, efektem czego przetwarzanie dokonywane przez niego w takich celach nie może wchodzić w zakres zastosowania art. 6 ust. 1 akapit pierwszy lit. f) RODO (pkt 117).

TSUE wyraził ponadto wątpliwość, by wskazany przez Meta cel polegający na „potrzebie ulepszania produktu lub usługi” mógł mieć pierwszeństwo przed interesami i prawami podstawowymi takiego użytkownika (pkt 12).

Kierunek wyznaczony wyrokiem TSUE z dnia 4 lipca 2023 r., w którym Trybunał kilkakrotnie podkreślał znaczenia, jakie należy nadawać ochronie praw podstawowych, wskazując, że prawa administratora – co do zasady – muszą ustąpić przed ochroną praw podstawowych, w tym wypadku prawem do ochrony danych osobowych, pozwala zakładać, że podobne stanowisko Trybunał zająłby, konfrontując prawo użytkowników do dostępu do treści cyfrowych w relacji z przesłankami powoływanymi przez dostawców usług cyfrowych, którzy *de facto* uzależniają wykonanie usługi od przekazania im przez użytkownika jego danych osobowych. Wyrażone przez TSUE w wyroku stanowisko powinno – jak się wydaje – rzutować na sposób wykonywania usługi dostarczania treści cyfrowych, w szczególności w ten sposób, że dostęp do treści powinien zostać zapewniony także w wypadku braku potwierdzenia przez użytkownika zaznajomienia się z regulaminem przetwarzania (polityką prywatności) i niezależnie od udzielenia albo braku udzielenia zgody na przetwarzanie danych. TSUE nie miał dotychczas okazji dokonywać oceny zgodności działania dostawców usług cyfrowych z prawem do informacji, wolnością wypowiedzi i prawem do swobodnego przepływu informacji, niemniej wyrażone przez EROD i potwierdzone przez TSUE stanowisko w przedmiocie interpretacji przesłanek legalizujących przetwarzanie danych zawartych w art. 6 ust. 1 RODO pozwalają przypuszczać, że prawa te, w zetknięciu z interesami dostawców usług, spotkałyby się z należytą ochroną.

C. Usługi cyfrowe i usługi kluczowe w sektorze publicznym

Termin „usługi cyfrowe” jest wykorzystywany także w sektorze publicznym. Został zdefiniowany w art. 2 pkt 15 ustawy o krajowym systemie cyberbezpieczeństwa (UKSCB)¹⁸⁶.

Zgodnie z tym przepisem usługa cyfrowa oznacza usługę świadczoną drogą elektroniczną w rozumieniu przepisów ustawy o świadczeniu usług drogą elektroniczną¹⁸⁷, wymienioną w załączniku nr 2 do UKSCB. Ustawodawca zawęży zatem zakres pojęcia „usługi cyfrowe” do tych, które zostały wymienione i zdefiniowane w załączniku. *A contrario* oznaczać to musi, że inne usługi, choćby ich świadczenie następowało drogą elektroniczną i obejmowało dostarczanie treści cyfrowych, nie wchodzą w zakres pojęcia usług cyfrowych w rozumieniu UKSCB.

¹⁸⁶ Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2023 r., poz. 913) – dalej: UKSCB, wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. UE L Nr 194, s. 1) – dalej: dyrektywa NIS. W dyrektywie (UE) 2016/1148 wprowadzono wymogi dotyczące zdolności krajowych w dziedzinie cyberbezpieczeństwa, ustanowiono pierwsze mechanizmy zacieśniania strategicznej i operacyjnej współpracy państw członkowskich oraz wprowadzono obowiązki dotyczące środków bezpieczeństwa i zgłaszania incydentów w istotnych dla gospodarki i społeczeństwa sektorach, takich jak energetyka, transport, zaopatrzenie w wodę pitną i jej dystrybucja, bankowość, infrastruktura rynków finansowych, opieka zdrowotna, infrastruktura cyfrowa, jak też w odniesieniu do dostawców kluczowych usług cyfrowych (wyszukiwarek, usług przetwarzania w chmurze i targu internetowego). Kluczową rolę we wspieraniu wdrażania tej dyrektywy wyznaczono agencji ENISA. Cele, zakres i tryb jej działania określa rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.U. UE L Nr 151/15), <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32019R0881&qid=1693833454665> (dostęp: 10.10.2023). Dyrektywa NIS została uchylona wraz z przyjęciem dyrektywy 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.U. UE L Nr 333, s. 80).

¹⁸⁷ Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz.U. z 2020 r., poz. 344 ze zm.).

Ustawodawca ich nie wskazuje w części ogólnej USCB ani nie odwołuje się do ich rodzaju i specyfiki w kolejnych rozdziałach ustawy¹⁸⁸.

W załączniku nr 2 do ustawy wymieniono:

1. usługę internetowej platformy handlowej,
2. usługę przetwarzania w chmurze,
3. usługę wyszukiwarki internetowej¹⁸⁹.

Usługa internetowej platformy handlowej została zdefiniowana jako usługa, która umożliwia konsumentom lub przedsiębiorcom zawieranie umów drogą elektroniczną z przedsiębiorcami na stronie internetowej platformy handlowej albo na stronie internetowej przedsiębiorcy, który korzysta z usług świadczonych przez internetową platformę handlową. Usługa przetwarzania w chmurze oznacza usługę umożliwiającą dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania przez wielu użytkowników. Usługa wyszukiwarki internetowej – zgodnie z legalną definicją zawartą w załączniku – oznacza usługę, która umożliwia użytkownikom wyszukiwanie wszystkich stron internetowych lub stron internetowych w danym języku za pomocą zapytania przez podanie słowa kluczowego, wyrażenia lub innego elementu, przedstawiającą w wyniku odnośniki prowadzące do informacji związanych z zapytaniem.

Na wąski zakres, w jakim termin „usługa cyfrowa” może być stosowany na gruncie prawa publicznego, w szczególności UKSCB, wskazuje nie tylko określony w załączniku nr 2 UKSCB zakres przedmiotowy, ale także ograniczony krąg podmiotów, do których termin ten znajdzie zastosowanie. Ustawodawca krajowy, w następstwie rozwiązań przyjętych w dyrektywie NIS, wskazał w art. 17 ust. 1 UKSCB, że dostawcą usługi cyfrowej jest osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej, mająca siedzibę lub zarząd na terytorium Rzeczypospolitej Polskiej albo przedstawiciela mającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, świadcząca usługę cyfrową, z wyjątkiem mikroprzedsiębiorców i małych przedsiębiorców, o których mowa w art. 7 ust. 1 pkt 1 i 2 ustawy Prawo

¹⁸⁸ J. Taczkowska-Olszewska, *Komentarz do art. 17, [w:] Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz (red.), Warszawa 2019, s. 20.

¹⁸⁹ Załącznik nr 2 do Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2023 r., poz. 913).

przedsiębiorców¹⁹⁰. Dostawcą usługi cyfrowej może być jedynie osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej¹⁹¹. Oznacza to, że dostawcą usługi cyfrowej nie może być osoba fizyczna, w tym prowadząca działalność gospodarczą na podstawie wpisu do Centralnej Ewidencji i Informacji o Działalności Gospodarczej¹⁹².

Zakres terminu „usługa cyfrowa” został w prawie publicznym zarówno przedmiotowo, jak i podmiotowo ograniczony, co rodzi określone konsekwencje związane, w szczególności, z wąsko wyznaczonym obowiązkiem reagowania na incydenty związane z dostarczaniem usług cyfrowych wówczas, gdy dostawcą usług jest podmiot prywatny. Rzadko zatem wystąpią przypadki, kiedy organy publiczne będą zobowiązane do reagowania na incydenty bezpieczeństwa w cyberprzestrzeni, nawet jeśli istnieje zagrożenie naruszenia praw podstawowych, jak w szczególności wolność wypowiedzi¹⁹³. Konieczne jest bowiem ustalenie w pierwszej kolejności, czy usługa cyfrowa, której miałyby dotyczyć reakcja organu publicznego, mieści się w charakterystyce tego pojęcia zawartej w UKSCB¹⁹⁴. Niemniej znaczna liczba

¹⁹⁰ Ustawa z dnia 6 marca 2018 r. – Prawo przedsiębiorców (t.j. Dz.U. z 2023 r., poz. 221 z późn. zm.).

¹⁹¹ Art. 33 i 331 ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz.U. z 2018 r. poz. 1025 ze zm.).

¹⁹² M. Lewoszewski, *Wybrane obowiązki dostawców usług cyfrowych na gruncie ustawy o cyberbezpieczeństwie*, „Informacja w Administracji Publicznej” 2019, nr 1, s. 74.

¹⁹³ Incyident w rozumieniu art. 2 pkt 5 UKSCB oznacza zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo. Ustawodawca przewidział gradację incyidentów ze względu na stopień naruszenia bezpieczeństwa w cyberprzestrzeni. Wyróżnił zatem incyident poważny – incyident, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej (art. 2 pkt 7 UKSCB) oraz incyident krytyczny – incyident skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi (art. 2 pkt 6 UKSCB).

¹⁹⁴ Proponuje się obecnie poszerzenie kręgu podmiotów objętych stosowaniem dyrektywy. W nowej dyrektywie (NIS 2) obowiązkami w zakresie cyberbezpieczeństwa mają zostać objęci również mali i mikro przedsiębiorcy. Zob. dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2); <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32022L2555> (dostęp: 4.09.2023). Proponuje się także szerszą definicję usługi cyfrowej, która mogłaby obejmować także usługi zaufania czy usługi łączności

obserwowanych naruszeń w internecie dotyczyła praw podstawowych, w tym wolności wypowiedzi¹⁹⁵.

Obok pojęcia usługi cyfrowej ustawodawca posłużył się pojęciem usługi kluczowej, która także jest świadczona na odległość z wykorzystaniem systemów teleinformatycznych. Definicję usługi kluczowej zawiera art. 2 pkt 16 UKSCB, zgodnie z którym termin ten oznacza usługę mającą kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienioną w wykazie usług kluczowych. Wykaz tych usług został zawarty w przepisach wykonawczych do ustawy¹⁹⁶ i obejmuje usługi z zakresu przesyłu energii, transportu, bankowości i finansów, dostaw wody.

W ustawie wyróżniono kilka kategorii incydentów bezpieczeństwa w cyberprzestrzeni, które odpowiadają trzem poziomom szacowanej szkody, jaką mogą

elektronicznej, a także usługi, których zakłócenie mogłoby mieć wpływ na bezpieczeństwo czy zdrowie publiczne; zob. Wniosek Dyrektywa Parlamentu Europejskiego i Rady z dnia 16 grudnia 2020 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylająca dyrektywę (UE) 2016/1148, <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020PC0823> (dostęp: 4.09.2023).

¹⁹⁵ Z danych CERT Polska wynika, że najczęściej zgłaszanym typem incydentów zarejestrowanych w 2022 r. były incydenty związane z oszustwami komputerowymi, a szczególnie phishingu. CERT Polska zarejestrował 25 625 incydentów zaklasyfikowanych jako phishing, co stanowi 64% wszystkich obsługiwanych incydentów w 2022 r. Imponująca jest również liczba zgłoszeń, aż 82 830 zgłoszeń powiązanych jest z incydentami phishingu. Najpopularniejszym typem phishingu było wykorzystywanie wizerunku firmy kurierskiej InPost – 5 119 incydentów. Na podium znalazł się również serwis mediów społecznościowych Facebook – 4 370 incydentów oraz serwis ogłoszeniowy Vinted – 2 926 incydentów. Kolejnym często zgłaszanym w ubiegłym roku rodzajem incydentu było szkodliwe oprogramowanie. Na podstawie 15 433 zgłoszeń zarejestrowano 3 409 incydentów tego typu, co przekłada się na 8,59% wszystkich incydentów. Wśród zarejestrowanych incydentów aż 2 607 dotyczyło szkodliwego oprogramowania o nazwie Flubot. Trzecim typem incydentów, który występował najczęściej w 2022 r., były włamania m.in. do systemów informatycznych oraz kont pocztowych. Tego typu incydentów zarejestrowano 354, co przekłada się na 0,89% wszystkich incydentów. Incydenty zaklasyfikowane jako obraźliwe i nielegalne treści, w tym spam, również nie pozostają daleko w tyle. Pomimo iż zarejestrowano ich „zaledwie” 308 – 0,78% wszystkich incydentów, to dokonano tego na podstawie 5 257 zgłoszeń. Statystycznie przypada aż 17 zgłoszeń na jeden incydent cyberbezpieczeństwa w tej kategorii; zob. *Raport roczny z działalności CERT Polska 2022. Krajobraz bezpieczeństwa polskiego internetu*, CERT.pl, https://cert.pl/uploads/docs/Raport_CP_2022.pdf (dostęp: 10.10.2023).

¹⁹⁶ Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (Dz.U., poz. 1806).

wyrządzić, w tym także w sferze praw i wolności obywatelskich. Jak zauważa F. Radoniewicz, incydenty pierwszego poziomu to zdarzenia, które mają lub mogą mieć niekorzystny wpływ na cyberbezpieczeństwo, ale nie są na tyle poważne, by mogły zostać zakwalifikowane jako incydenty określone w ustawie. Następną grupę stanowią incydenty drugiego poziomu; będą to incydenty:

1. poważne (powodujące lub mogące spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej);
2. istotne (mające istotny wpływ na świadczenie usługi cyfrowej);
3. incydenty w podmiocie publicznym (powodujące lub mogące spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny).

Incydenty trzeciego poziomu to incydenty krytyczne¹⁹⁷.

Z reakcją organów publicznych na incydenty w zakresie dostarczania treści cyfrowych mógł, zgodnie z powyżej wskazaną systematyką, spotkać się incydent istotny. Dany incydent uznaje się za istotny, jeżeli zaistniała co najmniej jedna z następujących sytuacji:

- a) usługa świadczona przez dostawcę usług cyfrowych była niedostępna przez ponad 5 mln użytkownikówgodzin, przy czym pojęcie użytkownikówgodziny odnosi się do liczby dotkniętych incydem użytkowników w Unii przez okres sześćdziesięciu minut;
- b) incydent doprowadził do utraty integralności, autentyczności lub poufności przechowywanych lub przekazywanych bądź przetwarzanych danych lub powiązanych usług, oferowanych bądź dostępnych poprzez sieci i systemy informatyczne dostawcy usług cyfrowych, która dotknęła ponad 100 000 użytkowników w Unii;
- c) incydent spowodował ryzyko dla bezpieczeństwa publicznego lub ryzyko wystąpienia ofiar śmiertelnych;
- d) incydent wyrządził co najmniej jednemu użytkownikowi w Unii stratę materialną, której wysokość przekracza 1 mln EUR¹⁹⁸.

¹⁹⁷ F. Radoniewicz, *Komentarz do art. 2, [w:] Ustawa o krajowym...*, s. 20.

¹⁹⁸ Art. 4 rozporządzenia wykonawczego Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiającego zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ (Dz.U. UE L Nr 26, s. 48).

W nowej dyrektywie NIS 2 usługa cyfrowa została zdefiniowana poprzez odesłanie do art. 1 ust. 1 lit. b) dyrektywy 2015/1535. Przyjęto zatem, że każda usługa społeczeństwa informacyjnego stanowi, także dla realizacji celów określonych w dyrektywie, usługę cyfrową. Wskazano także na niezasadność rozróżnienia operatorów usług kluczowych i dostawców usług cyfrowych, które – jak wskazano – „okazało się nieaktualne, ponieważ nie odzwierciedla znaczenia danych sektorów lub usług dla działalności społecznej i gospodarczej na rynku wewnętrznym” (motyw 6 dyrektywy NIS 2). Zalecono, by państwa członkowskie zapewniły objęcie zakresem dyrektywy także niektóre małe i mikroprzedsiębiorstwa, które spełniają szczególne kryteria wskazujące na kluczową rolę dla społeczeństwa, gospodarki lub konkretnych sektorów lub rodzajów usług (motyw 7 dyrektywy NIS 2). Zdecydowano się zarazem na zdefiniowanie niektórych kategorii usług cyfrowych, tj.:

1. usługa ośrodka przetwarzania danych, przez co rozumie się świadczenie usługi, w skład której wchodzi struktury lub grupy struktur służące scentralizowanemu hostingowi, wzajemnym połączeniom i eksploatacji sprzętu informatycznego i sieciowego służącego do przechowywania, przetwarzania i transportu danych wraz z całością obiektów i infrastruktury zapewniających dystrybucję energii elektrycznej i kontrolę środowiskową. Terminu „usługa ośrodka przetwarzania danych” nie należy stosować w odniesieniu do wewnętrznych, korporacyjnych ośrodków przetwarzania danych będących własnością danego podmiotu i eksploatowanych przez niego na własne potrzeby;
2. usługi DNS jako usługi rejestracji nazw domen;
3. usługi internetowych platform handlowych;
4. usługi wyszukiwarek internetowych;
5. platformy usług sieci społecznościowych;
6. usługi zaufania;
7. usługi zarządzane w zakresie bezpieczeństwa.

Zauważono, że dostawcy ww. usług „powinni podlegać daleko idącej harmonizacji na poziomie Unii. Wdrażanie środków zarządzania ryzykiem w cyberbezpieczeństwie w odniesieniu do tych podmiotów należy zatem ułatwić za pomocą aktu wykonawczego” (motyw 84).

Zważywszy, że zakres stosowania dyrektywy został rozszerzony i obejmuje, pod pewnymi warunkami¹⁹⁹, także dostawców takich usług cyfrowych jak platformy handlowe, portale społecznościowe i usługi chmurowe, rozstrzygnięcia wymaga – ze względu na ryzyko wystąpienie kolizji – jakie organy należy uznać za właściwe w zakresie wykonywania kompetencji kontrolnych i nadzorczych wobec dostawców usług. Nie jest bez znaczenia, że dyrektywa NIS 2 operuje nieco inną aparaturą pojęciową niż rozporządzenia cyfrowe, np. poprzez używanie terminu „platformy handlowe”, podczas gdy w AUC wykorzystywane jest pojęcie platformy internetowej. Podobnie w dyrektywie operuje się terminem „usługa chmurowa”, natomiast w rozporządzeniach wskazuje się na „usługi w chmurze”. Wszystkie dokumenty operują już jednak pojęciem wyszukiwarki internetowej. Wydaje się, że różnice terminologiczne mogą mieć pewne znaczenie przy dokonywaniu interpretacji tych aktów prawnych, jednakże nie będą miały charakteru ważącego i rozstrzygającego ewentualnych kolizji. Zdaje się, że w dyrektywie NIS 2 udzielono Komisji Europejskiej kolejnego upoważnienia. Poza *explicite* wskazanymi w AUC i ARC uprawnieniami nadzorczymi, kontrolnymi i egzekucyjnymi, do uznania KE pozostawiono rozstrzygnięcie, w jakim zakresie i czy w ogóle do bardzo dużych platform internetowych powinny znaleźć zastosowanie regulacje zawarte w dyrektywie NIS 2. Pozostawienie KE kompetencji do dokonywania wiążącej interpretacji przepisów dyrektywy i pozostających z nimi w związku postanowień zawartych w ARC i AUC wywołuje także skutek w obszarze kompetencji państw członkowskich.

Z art. 5 dyrektywy NIS 2 wynika, że „dyrektywa nie uniemożliwia państwom członkowskim przyjęcia lub utrzymania przepisów zapewniających

¹⁹⁹ Podmioty objęte stosowaniem dyrektywy zostały podzielone na dwie grupy: podmioty kluczowe i podmioty ważne. Podmioty, które są objęte zakresem stosowania niniejszej dyrektywy w celu przestrzegania środków zarządzania ryzykiem w cyberbezpieczeństwie i obowiązków dotyczących zgłaszania incydentów, należy podzielić na dwie kategorie – podmioty kluczowe i podmioty ważne – w zależności od tego, jak bardzo ich znaczenie jest zasadnicze dla ich sektorów lub dla rodzaju świadczonych przez nie usług, a także od ich wielkości. W związku z tym właściwe organy powinny w stosownych przypadkach należycie uwzględnić odpowiednie sektorowe oszacowania ryzyka lub wskazówki. Należy zróżnicować systemy nadzoru i egzekwowania między tymi dwiema kategoriami podmiotów, aby zapewnić odpowiednią równowagę między wymogami i obowiązkami związanymi z ryzykiem a obciążeniem administracyjnym wynikającym z nadzoru nad zgodnością z przepisami (motyw 15 w zw. z art. 27 dyrektywy NIS 2).

wyższy poziom cyberbezpieczeństwa, pod warunkiem że takie przepisy są spójne z obowiązками państw członkowskich, ustanowionymi w prawie Unii” (harmonizacja minimalna). Tymczasem w art. 56 ust. 1 AUC to na rzecz Komisji Europejskiej, a nie państw członkowskich, zapewnione zostało prawo do wykonywania kompetencji wyłącznych w stosunku do bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych. W motywie 139 AUC za pożądane uznano, by KE posiadała „pewien margines uznaniowości, jeżeli chodzi o decyzje o wszczęciu postępowania przeciwko dostawcom bardzo dużych platform internetowych lub bardzo dużych wyszukiwarek internetowych”. Ostatecznie, jak wynikałoby z motywu 140 dyrektywy NIS 2, Komisja będzie rozstrzygała, w jakich okolicznościach do bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych zastosowanie znajdą postanowienia dyrektywy NIS 2, która pozostawia państwom członkowskim, co do zasady, duży margines swobody, a w jakim zakresie Komisja skorzysta z kompetencji wyłącznych na podstawie rozporządzeń cyfrowych. W dyrektywie NIS 2 postanowiono, że Komisja, w ramach okresowych przeglądów, „powinna ocenić znaczenie wielkości danych podmiotów oraz sektorów, podsektorów i rodzajów podmiotu dla funkcjonowania gospodarki i społeczeństwa w kontekście cyberbezpieczeństwa. Komisja powinna ocenić między innymi, czy dostawcy objęci zakresem niniejszej dyrektywy wyznaczeni jako bardzo duże platformy internetowe w rozumieniu art. 33 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 24 mogą zostać wskazani jako podmioty kluczowe na mocy niniejszej dyrektywy” (motyw 140).

3. Ustawowe i umowne mechanizmy ingerencji w wolność wypowiedzi

Na gruncie AUC przyjęto, że realizacja praw podstawowych przez użytkowników internetu, a więc także zasady uzyskiwania dostępu do informacji oraz zakres swobody wypowiedzania się (umieszczania treści) w internecie jest wypadkową dwojakiego rodzaju mechanizmów, tj. po pierwsze, procedur

i polityk realizowanych przez pośredników internetowych w celu wywiązania się z nałożonego na nich w AUC obowiązku należytej staranności²⁰⁰, oraz, po drugie, regulaminów korzystania z usług, ustanawianych przez pośredników internetowych, które uzależniają świadczenie usług od zaakceptowania przez użytkowników warunków zawartych w tych regulaminach.

W AUC wskazuje się zarówno na jeden, jak i drugi mechanizm, uznając, że stanowią one realizację ustawowych (wynikających z AUC) albo umownych (wynikających ze stosowanych u pośredników regulaminów²⁰¹) norm postępowania upoważniających pośrednika do ingerowania w sferę wolności wypowiedzi użytkowników. Pośrednik jest zatem upoważniony do ingerowania *ex lege* ze względu na ryzyko rozpowszechniania nielegalnych treści (*ex ante*), a także wówczas, gdy takie treści zostały publicznie udostępnione (*ex post*) oraz kiedy działanie użytkownika narusza postanowienia obowiązującego u pośrednika regulaminu. Formalną podstawę ingerencji w wolność wypowiedzi stanowić mogą zatem warunki umowy o korzystanie z usług (regulamin usług) łączącej odbiorcę usługi z pośrednikiem albo upoważnienie wynikające z AUC.

Rozporządzenia cyfrowe (AUC i ARC) potwierdzają dopuszczalność równoległego i równoważnego z zawartymi w aktach ustawodawczych, umownego normowania przez dostawców usług cyfrowych zasad i przesłanek ingerowania w wolność wypowiedzi odbiorców usług. Zawarte w rozporządzeniach cyfrowych rozwiązania w zakresie, w jakim odsyłają do warunków

²⁰⁰ Obowiązkowi dochowania należytej staranności poświęcony został cały III rozdział AUC.

²⁰¹ Przykładowo zawarcie z Google umowy na korzystanie z usług Google następuje poprzez zaakceptowanie „Warunków korzystania z usług Google” zamieszczonymi na stronie; zob. *Warunki korzystania z usług Google*, *Data wejścia w życie: 5 stycznia 2022* https://www.gstatic.com/policies/terms/pdf/20220105/it7r24p9/google_terms_of_service_pl_eu.pdf (dostęp: 30.09.2023). Wskazano tam, że „Aby korzystać z naszych usług, użytkownik musi zaakceptować niniejsze warunki, dlatego tak ważne jest, by je dobrze zrozumieć [...] Ogólnie rzecz biorąc, pozwalamy użytkownikom na korzystanie z naszych usług, o ile zgodzą się na przestrzeganie tych warunków, które odzwierciedlają działalność i sposób, w jaki zarabia Google. Kiedy wypowiadamy się w pierwszej osobie liczby mnogiej i piszemy »Google«, mamy na myśli firmę Google Ireland Limited i jej podmioty stowarzyszone” (tamże). Lista usług Google podlegająca „Ogólnym warunkom korzystania” zawiera 42 usługi, w szczególności: przeglądarka Chrome, dysk Google, Konto Google, Google Classroom. Dla niektórych usług Google, jak np. YouTube, wskazano szczególne warunki umowy (tamże).

korzystania z usług (regulaminów), mają charakter blankietowy. Ustawodawca europejski traktuje „warunki korzystania z usług” i postanowienia zawarte w rozporządzeniach cyfrowych w sposób równorzędny. Zarówno wówczas, gdy upoważnienie do ingerencji w wolność wypowiedzi znajduje podstawę w akcie ustawodawczym, jak też wtedy, gdy akt ten odsyła do umów (regulaminów) obowiązujących u dostawców usług cyfrowych, faktyczną podstawę usprawiedliwiającą ingerencję stanowią nielegalne treści albo ryzyko ich rozpowszechnienia.

W konstrukcji przepisów, których skutkiem normatywnym jest zrównanie wagi postanowień umownych zawartych w regulaminach korzystania z usług z przepisami zawartymi w rozporządzeniach cyfrowych, posłużono się wyrażeniem zawierającym alternatywę łączną, postanawiając, że ingerowanie przez pośredników internetowych w treści zamieszczane przez użytkowników internetu (odbiorców usług) jest uzasadnione ze względu na „nielegalne treści lub niezgodność z warunkami korzystania z usług” (motyw 54). Przepisy zawierające alternatywę łączną, tj. wyrażenie w brzmieniu: „nielegalne treści lub niezgodność z warunkami korzystania z usług” pojawiają się w kilku miejscach AUC, np. w: motywach 54, 58, 80, 84; art. 17 ust. 1; art. 20 ust. 1; art. 20 ust. 4; art. 34 ust. 2; art. 39 ust. 3.

Definicja nielegalnych treści została zawarta w art. 3 lit. h AUC, a zarazem zwalczanie nielegalnych treści stanowi obowiązek nałożony na dostawców usług cyfrowych, przy czym realizacja tego obowiązku może być efektywna wówczas, gdy w regulaminach ustalających warunki korzystania z usług pośrednicy internetowi zawrą postanowienia przewidujące stosowanie środków mających na celu zwalczanie nielegalnych treści. Paradoksalnie to przede wszystkim treść umów łączących pośredników internetowych z użytkownikami internetu przesądza o skuteczności zwalczania nielegalnych treści w internecie. Ustawodawca europejski dostrzega tę zależność polegającą na tym, że skuteczność realizacji zadania publicznego (zwalczanie nielegalnej treści) jest uzależnione od dobrowolności działania podmiotu prywatnego.

Ustawodawca dostrzega karykaturalność sytuacji polegającej na przeniesieniu rzeczywistego centrum władztwa ze sfery zarządzanej przez organy publiczne do sfery prywatnoprawnej, w której niewielka grupa podmiotów (strażnicy dostępu) oddziałuje na sferę opinii, a także wpływa na rozwój rynku wewnętrznego. W motywie 3 ARC zauważono, że:

Pojawiła się niewielka liczba dużych przedsiębiorstw świadczących podstawowe usługi platformowe o znaczącej sile gospodarczej, co kwalifikowałoby je do wskazania ich jako strażników dostępu. Zazwyczaj cechuje je zdolność łączenia – za pośrednictwem świadczonych usług – wielu użytkowników biznesowych z wieloma użytkownikami końcowymi, co z kolei umożliwia im wykorzystywanie przewagi, wynikającej np. z dostępu do dużych ilości danych, nabytej w jednym obszarze działalności w innym obszarze działalności. Niektóre z tych przedsiębiorstw sprawują kontrolę nad całymi ekosystemami platform w gospodarce cyfrowej i ze względów strukturalnych niezwykle trudno jest zakwestionować lub podważyć ich pozycję [...].

Pozycja „strażników dostępu” zarówno w zakresie posiadanego potencjału oddziaływania na sferę opinii²⁰², jak i w sferze gospodarczej²⁰³ jest ogromna.

²⁰² Wskazują na to cztery, zidentyfikowane w AUC, rodzaje ryzyka systemowego, tj. a) ryzyko rozpowszechniania nielegalnych treści za pośrednictwem ich usług, b) ryzyko wystąpienia faktycznych lub przewidywalnych negatywnych skutków dla wykonywania praw podstawowych, w szczególności prawa podstawowego do godności ludzkiej zapisanego w art. 1 Karty, do poszanowania życia prywatnego i rodzinnego zapisanego w art. 7 Karty, do ochrony danych osobowych zapisanego w art. 8 Karty, do wolności wypowiedzi i informacji, w tym wolności i pluralizmu mediów, zapisanego w art. 11 Karty, do niedyskryminacji zapisanego w art. 21 Karty, do przestrzegania praw dziecka zapisanego w art. 24 Karty i do wysokiej jakości ochrony konsumentów zapisanego w art. 38 Karty, c) ryzyko wystąpienia faktycznych lub przewidywalnych negatywnych skutków dla dyskursu obywatelskiego i procesów wyborczych oraz dla bezpieczeństwa publicznego, d) ryzyko wystąpienia faktycznych lub przewidywalnych negatywnych skutków w odniesieniu do przemocy ze względu na płeć, ochrony zdrowia publicznego i małoletnich, oraz poważnych negatywnych skutków dla fizycznego i psychicznego dobrostanu osoby (art. 34 ust. 1 AUC).

²⁰³ Pojawiła się niewielka liczba dużych przedsiębiorstw świadczących podstawowe usługi platformowe o znaczącej sile gospodarczej, co kwalifikowałoby je do wskazania ich jako strażników dostępu na podstawie niniejszego rozporządzenia. Zazwyczaj cechuje je zdolność łączenia – za pośrednictwem świadczonych usług – wielu użytkowników biznesowych z wieloma użytkownikami końcowymi, co z kolei umożliwia im wykorzystywanie przewagi, wynikającej na przykład z dostępu do dużych ilości danych, nabytej w jednym obszarze działalności w innym obszarze działalności. Niektóre z tych przedsiębiorstw sprawują kontrolę nad całymi ekosystemami platform w gospodarce cyfrowej i ze względów strukturalnych niezwykle trudno jest zakwestionować lub podważyć ich pozycję istniejącym lub nowym podmiotom rynkowym, niezależnie od tego, jak bardzo mogłyby one być innowacyjne i wydajne (motyw 3 ARC). Strażnicy dostępu wywierają znaczący wpływ na rynek wewnętrzny, gdyż zapewniają dużej liczbie użytkowników biznesowych punkty dostępu umożliwiające im docieranie do użytkowników końcowych w dowolnym miejscu w Unii i na różnych rynkach (motyw 6 ARC).

Zauważono zarazem, że nieskuteczne mogłyby okazać się regulacje o charakterze horyzontalnym oddziałujące na stosunki prywatnoprawne, przede wszystkim z tego powodu, że działalność strażników dostępu ma charakter transgraniczny, a znaczna ich część – co prawda – posiada siedzibę poza UE, to jednak prowadzi działalność w państwach członkowskich UE. Nieskuteczne mogłyby się okazać także normy o charakterze ściśle wertykalnym. Skuteczna regulacja musiała zatem zakładać element konsyliacji i dobrovolności po stronie podmiotów prywatnych (strażników dostępu), które *de facto* zgodziły się na realizację wskazanych w AUC i ARC zadań publicznych. W efekcie przyjęto, że zawarte w regulaminach warunki korzystania z usług zostaną powiązane z realizacją celów publicznych, w szczególności zwalczania i przeciwdziałania nielegalnym treściom. Założenie to potwierdza treść motywu 45 AUC, w którym stwierdzono, że „choć zasadniczo należy przestrzegać swobody umów przysługującej dostawcom usług pośrednich, należy ustanowić pewne zasady dotyczące treści, stosowania i egzekwowania warunków korzystania z usług tych dostawców” (motyw 45). Wielokrotnie w AUC wskazano zarazem na formalnie zagwarantowany zakaz nakładania na pośredników internetowych ogólnych obowiązków w zakresie monitorowania lub aktywnego ustalania faktów (art. 6 AUC) przy jednoczesnym potwierdzeniu dopuszczalności dobrowolnego przyjmowania praktyk polegających na moderowaniu i monitorowaniu treści (art. 7).

Mechanizm służący usprawiedliwianiu (legalizowaniu) ingerencji w wolność wypowiedzi wykorzystuje mieszane instrumenty regulacyjne właściwe dla prawa publicznego i prawa prywatnego. Instrumenty te są nierozłączne w tym znaczeniu, że żaden z nich, tj. ani umowy (regulaminy), ani też zastosowanie wyłącznie władczych rozwiązań charakterystycznych dla prawa publicznego, nie pozwoliłoby na skuteczne osiągnięcie celu regulacyjnego, jakim jest zwalczanie nielegalnych treści, w tym przeciwdziałanie rozpowszechnieniu treści uznanych *ex ante* za nielegalne. Obok celów gospodarczych, celem działania europejskiego ustawodawcy było „zapewnienie bezpiecznego, przewidywalnego i budzącego zaufanie środowiska internetowego, przeciwdziałania rozpowszechnianiu nielegalnych treści w internecie oraz zagrożeniom społecznym, jakie może stwarzać rozpowszechnianie dezinformacji lub innych treści” (motyw 9 AUC).

Walka z nielegalnymi treściami, niezależnie od tego, czy metody i środki z nią związane zostały wskazane i opisane bezpośrednio w rozporządzeniach cyfrowych, czy wskazano je w „warunkach korzystania z usług”, polega na podejmowaniu przez pośredników internetowych szeregu czynności i przedsięwzięciu środków, które zostały wskazane np. w AUC i ARC. Rozporządzenia cyfrowe nie zawierają zamkniętego katalogu czynności, których stosowanie miałyby mieć obligatoryjny charakter, ani nie stanowią wykazu skutecznych środków, których zastosowanie byłoby zalecone. Katalogi te są otwarte i – jak można zasadnie twierdzić – wypełnienie ich treścią należy do pośredników internetowych. Granicą swobody regulacyjnej pośredników w zakresie kształtowania przez nich rozwiązań zawartych w warunkach korzystania z usług i stosowanych środków w celu zwalczania nielegalnych treści jest „przejrzystość, uczciwość praktyk i brak arbitralności rozstrzygnięć podejmowanych przez dostawcę usług cyfrowych” (motyw 45). Wymaga się zatem od dostawców, by w warunkach korzystania z ich usług wyraźnie podawali i aktualizowali informacje o powodach, dla których mogą ograniczyć świadczenie swoich usług. Warunki te powinny w szczególności zawierać informacje na temat wszelkich polityk, procedur, środków i narzędzi wykorzystywanych do celów moderowania treści (motyw 45). Termin „warunki korzystania z usług” został zdefiniowany w art. 3 lit. u AUC jako „klausule, niezależnie od ich nazwy lub formy, które regulują stosunek umowny między dostawcą usług pośrednich a odbiorcami usług”.

Przy zastosowaniu kryterium celowościowego oraz – pomocniczo – biorąc pod uwagę umowny albo ustawowy charakter upoważnienia usprawiedliwiającego ingerencję w wolność wypowiedzi, środki i czynności stosowane przez pośredników można podzielić na trzy grupy, tj.:

1. moderowanie treści;
2. stosowanie systemów rekomendacji;
3. monitorowanie treści.

A. Moderowanie treści

Termin „moderowanie treści” oznacza działania podejmowane przez dostawców usług pośrednich, których celem jest, w szczególności, wykrywanie, identyfikowanie i zwalczanie nielegalnych treści lub informacji niezgodnych z warunkami korzystania z usług, bez względu na to, czy działania te są automatyzowane, czy podejmowane w wyniku oceny dokonywanej przez człowieka. Pojęcie „moderowanie treści” obejmuje też „wdrażane środki, które wpływają na dostępność, widoczność i osiągalność takich nielegalnych treści lub informacji, jak depozycjonowanie takich treści lub informacji, demonetyzacja, uniemożliwienie dostępu do nich lub ich usunięcie, lub które wpływają na możliwość przekazywania takich informacji przez odbiorców usługi, takie jak zamknięcie lub zawieszenie konta odbiorcy” (art. 3 lit. t AUC). W motywie 54 wskazano, że usunięcie treści może nastąpić zarówno wówczas, gdy pośrednik działa z własnej inicjatywy (art. 7 AUC), jak też wtedy, gdy działa na podstawie zgłoszenia (art. 16 AUC), przy czym podstawę tych czynności stanowić może zarówno nakaz wydany przez uprawniony organ (sąd, organ władzy publicznej, Komisja Europejska, Rada Usług Cyfrowych, Koordynator ds. usług cyfrowych), jak i powołanie się przez pośrednika na ogólny obowiązek starannego działania wynikający z AUC oraz wskazanie postanowień obowiązującego u dostawcy regulaminu korzystania z usług jako podstawy nakładania ograniczeń²⁰⁴.

Złożoność i różnorodność czynności oraz środków objętych zakresem terminu „moderowanie” w rozumieniu art. 3 lit. t AUC wskazują, że mogą być one podejmowane tak jawnie, jak i w sposób ukryty, niewidoczny dla

²⁰⁴ W motywie 54 AUC wskazano, że „W przypadku gdy dostawca usług hostingu decyduje się, ze względu na to, że przekazane przez odbiorców usług informacje stanowią nielegalne treści lub są niezgodne z jego warunkami korzystania z usług, usunąć informacje przekazane przez odbiorcę usługi lub uniemożliwić dostęp do nich, lub w inny sposób ograniczyć ich widoczność lub monetyzację, w sposób jasny i łatwo zrozumiały poinformować odbiorcę o swojej decyzji, powodach jej podjęcia oraz dostępnych możliwościach odwołania się od tej decyzji, mając na uwadze negatywne konsekwencje, jakie takie decyzje mogą mieć dla odbiorcy, w tym dla możliwości wykonywania przez niego prawa podstawowego do wolności wypowiedzi. Obowiązek ten powinien mieć zastosowanie niezależnie od powodów podjęcia decyzji, w szczególności niezależnie od tego, czy działanie podjęte ze względu na uznanie zgłoszonych informacji za nielegalne treści lub za informacje niezgodne z mającymi zastosowanie warunkami korzystania z usług”.

użytkowników (odbiorców usług), przy czym, zarówno jeśli chodzi o intensywność, jak i częstotliwość podejmowanych działań oraz ich źródło i podstawę, pomimo ich zróżnicowania, wywołują one taki sam skutek polegający na ingerencji w wolność wypowiedzi, albowiem to wypowiedź (treść) staje się przedmiotem moderowania.

Wielokrotnie ustawodawca europejski wskazuje na dwie niezależne od siebie podstawy usprawiedliwionego ingerowania w wolność wypowiedzi użytkownika²⁰⁵, tj. upoważnienie z AUC oraz upoważnienie mające źródło w regulaminie zawierającym warunki korzystania z usług świadczonych przez pośrednika. Z treści art. 17 ust. 1 AUC wywieść należy, że dostawca usług cyfrowych nakłada ograniczenia na odbiorcę usługi z dwóch powodów, tj. jeśli treści publikowane przez odbiorcę: 1) są niezgodne z warunkami świadczenia usług przez dostawcę albo 2) mają charakter nielegalny. W konsekwencji niezgodność działania użytkownika internetu (odbiorcy usługi) z warunkami korzystania z usług zawartymi w regulaminie ustanowionym przez dostawcę usług cyfrowych lub przekazanie przez użytkownika informacji stanowiących nielegalne treści w rozumieniu AUC upoważnia dostawcę usługi do nałożenia na użytkownika (odbiorcę usługi) ograniczeń w zakresie możliwości udostępniania i rozpowszechniania treści, prowadząc, w skrajnych wypadkach, do trwałego usunięcia treści, a nawet usunięcia konta użytkownika i pozbawienia go możliwości korzystania z usług cyfrowych.

Termin „treść”, a w szczególności „nielegalne treści” (fr. *contenu illicite*²⁰⁶, ang. *illegal content*²⁰⁷), ma na gruncie rozporządzeń cyfrowych zakres znaczeniowy tożsamy albo bardzo zbliżony do zakresu pojęcia „wypowiedź”. Chodzi bowiem o taką „zawartość” umieszczoną w internecie, za pośrednictwem której użytkownik internetu (odbiorca usługi) coś oznajmia, opisuje, ocenia, o czymś informuje lub o coś pyta.

²⁰⁵ W wielu postanowieniach, zarówno w preambule, jak i w innych miejscach AUC, wskazano, że usprawiedliwioną podstawę działania pośrednika stanowi ustalenie przez niego, że „przekazane przez odbiorców usług informacje stanowią nielegalne treści lub są niezgodne z jego warunkami korzystania z usług” (motyw 54, 58, 64, 80, 84, a także art. 3 pkt u, art. 15 ust. 1 lit. d AUC).

²⁰⁶ AUC, wersja francuskojęzyczna, <https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32022R2065> (dostęp: 4.10.2023).

²⁰⁷ AUC, wersja anglojęzyczna, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2065> (dostęp: 4.10.2023).

Termin „treści”, występujący zarówno w wyrażeniu „treści nielegalne”, jak i w wyrażeniu „treści cyfrowe”, jest interpretowany szeroko i obejmuje wszelkiego rodzaju – werbalne oraz niewerbalne – zachowania oraz aktywności użytkowników internetu. W motywie 12 AUC wskazano, że pojęcie nielegalnych treści „należy zdefiniować szeroko, tak by obejmowało informacje dotyczące nielegalnych treści, produktów, usług i działań” (motyw 12 AUC). „Nielegalne treści” to „informacje, które same w sobie lub przez odniesienie do działania, w tym sprzedaży produktów lub świadczenia usług, nie są zgodne z prawem Unii lub z prawem jakiegokolwiek państwa członkowskiego, które jest zgodne z prawem Unii, niezależnie od konkretnego przedmiotu lub charakteru tego prawa” (art. 3 lit. h AUC). Jeśli informacje te przyjmują postać cyfrową to mogą zostać także objęte zakresem terminu „treści cyfrowe”, który oznacza „dane wytwarzane i dostarczane w postaci cyfrowej” (art. 2 pkt 5 ustawy o prawach konsumenta)²⁰⁸. Jak zauważa E. Macierzyńska-Franaszczyk, treści cyfrowe stanowią kategorię podlegającą bardzo szybkim zmianom technologicznym. Charakterystyka ich przyszłych postaci, czy też form przekazu, jest nieprzewidywalna²⁰⁹. Okoliczność ta skutkuje płynnością zakresów znaczeniowych terminu „treści cyfrowe”. W konsekwencji definicji legalnych terminu „treści cyfrowych” jest kilka, ponieważ termin ten jest odrębnie definiowany na potrzeby aktów legislacyjnych, które nim operują. Zauważa się, że termin „treści cyfrowe” jest wykorzystywany zarówno w dyrektywie 2011/83/UE²¹⁰ (dyrektywa o prawach konsumenta), jak i w dyrektywie 2015/2366 w sprawie usług płatniczych w ramach rynku

²⁰⁸ Ustawa z dnia 30 maja 2014 r. o prawach konsumenta (t.j. Dz.U. z 2020 r., poz. 287 z późn. zm.).

²⁰⁹ E. Macierzyńska-Franaszczyk, *Treści cyfrowe – ujęcie definicyjne w unijnych i krajowych regulacjach prawnych*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny” 2018, nr 6, s. 140.

²¹⁰ Dyrektywa Parlamentu Europejskiego i Rady 2011/83/UE z dnia 25 października 2011 r. w sprawie praw konsumentów, zmieniająca dyrektywę Rady 93/13/EEG i dyrektywę 1999/44/WE Parlamentu Europejskiego i Rady oraz uchylająca dyrektywę Rady 85/577/EEG i dyrektywę 97/7/WE Parlamentu Europejskiego i Rady (Dz.U. UE L Nr 304, s. 64 z późn. zm.).

wewnętrznego²¹¹, a w konsekwencji w ustawie o prawach konsumenta²¹² oraz w ustawie o usługach płatniczych²¹³.

Zgodnie z motywem 19 dyrektywy 2011/83/UE (dyrektywa o prawach konsumenta) treści cyfrowe dostarczone na trwałym nośniku należy traktować jak towary, a ich dostarczenie ma być objęte umową sprzedaży. Dostarczenie treści cyfrowych w sposób inny niż na trwałym nośniku nie może natomiast stanowić przedmiotu umowy sprzedaży ani umowy o świadczenie usług, ma natomiast stanowić przedmiot umowy o dostarczenie treści cyfrowych²¹⁴. Jak zauważa E. Macierzyńska-Franaszczyk, „wyrażone w dyrektywie ujęcie nie tylko różnicuje umowę o dostarczenie treści cyfrowych zarówno od umowy sprzedaży, jak i od umowy o świadczenie usług, lecz także powoduje, że treści cyfrowe w pewnym obszarze obrotu prawnego mogą być postrzegane jak rzeczy, których własność może być przenoszona w drodze umowy sprzedaży”²¹⁵. Podobnie definicja „treści cyfrowych” zawarta w art. 2 pkt 29a ustawy o usługach płatniczych odnosi ten termin zarówno do usług, jak i towarów²¹⁶. W ocenie E. Macierzyńskiej-Franaszczyk zmienność treści cyfrowych sprzyjać będzie dezaktualizacji definicji formułowanych zbyt szczegółowo, kazuistycznie. Mnożenie autonomicznych odrębnych legalnych definicji pojęcia, którego zakres desygnatów dynamicznie i nieprzewidywalnie się zmienia, zmniejszy w rezultacie przejrzystość prawa²¹⁷.

Definicja terminu „nielegalnych treści” w ogóle nie odwołuje się do technologii ich udostępniania lub przechowywania. Charakter nielegalnych treści mogą mieć zatem zarówno treści cyfrowe, jak i inne informacje, o ile „nie są

²¹¹ Dyrektywa 2007/64/WE Parlamentu Europejskiego i Rady z dnia 13 listopada 2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego zmieniająca dyrektywy 97/7/WE, 2002/65/WE, 2005/60/WE i 2006/48/WE i uchylająca dyrektywę 97/5/WE (Dz.U. UE L Nr 319, s. 1 z późn. zm.).

²¹² Ustawa z dnia 30 maja 2014 r. o prawach konsumenta (t.j. Dz.U. z 2020 r., poz. 287 z późn. zm.).

²¹³ Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (t.j. Dz.U. z 2022 r., poz. 2360 z późn. zm.).

²¹⁴ E. Macierzyńska-Franaszczyk, *Treści cyfrowe...*, s. 132–140.

²¹⁵ Tamże, s. 134.

²¹⁶ Zgodnie z definicją zawartą w art. 2 pkt 29 a ustawy o usługach płatniczych „treści cyfrowe to towary lub usługi wytwarzane i dostarczane lub świadczone w formie cyfrowej, które mogą zostać użyte lub z których można skorzystać wyłącznie za pomocą urządzenia technicznego, z wyłączeniem użycia i konsumpcji fizycznych towarów lub usług”.

²¹⁷ E. Macierzyńska-Franaszczyk, *Treści cyfrowe...*, s. 140.

zgodne z prawem Unii lub z prawem jakiegokolwiek państwa członkowskiego, które jest zgodne z prawem Unii” (art. 3 pkt h AUC). Zważywszy jednak, że zadanie polegające na przeciwdziałaniu rozpowszechnianiu i zwalczaniu nielegalnych treści zostało powierzone w AUC i ARC dostawcom usług cyfrowych, zasadne jest założenie, że należy je odnosić, w pierwszej kolejności, do treści cyfrowych.

Termin „treść” łączy się w sposób naturalny z pojęciem „wypowiedź”, które jest często używane w aktach normatywnych²¹⁸. Każda bowiem wypowiedź powinna być wypełniona treścią. O ile pomiędzy terminami „treści cyfrowe” i „nielegalne treści” występuje relacja krzyżowania, o tyle termin „wypowiedź” ma – jak się wydaje – najszerszy zakres znaczeniowy obejmujący zarówno zakresy terminu „nielegalne treści”, jak i „treści cyfrowe”²¹⁹. Jeśli „moderowanie” dotyczy treści, to oznacza zarazem, że „moderuje” wypowiedź. Nadto jeśli przez moderowanie ustawodawca rozumie jakąś formę ograniczenia, to oznaczać musi (*a minori ad maius*), że ograniczenie to dotyczy wypowiedzi, a dokładniej, swobody wypowiedzi.

W świetle AUC usprawiedliwioną ingerencję w wolność wypowiedzi stanowią, w szczególności, takie czynności pośredników²²⁰, jak: wykrywanie, identyfikowanie i zwalczanie nielegalnych treści (motyw 26; art. 3 lit. t; art. 22; ust. 2 pkt 1), w tym wdrażanie środków umożliwiających osiągnięcie tych celów, a zatem usuwanie treści (motyw 54, 87, 26, 22, 145); ograniczanie widoczności (motyw 54); depozycjonowanie (motyw 55); demonetyzacja (art. 3 lit. t), a ponadto dopuszczalne jest też zastosowanie takich metod, jak zamknięcie lub zawieszenie konta użytkownika (motyw 64, 65). Wymienione

²¹⁸ Art. 11 Karty praw podstawowych.

²¹⁹ Termin ten był omawiany w rozdziale II niniejszej pracy.

²²⁰ Wskazane poniżej czynności pośredników internetowych mogą być wykonywane równolegle i mieć różną intensywność w zależności od rodzaju świadczonej usługi. Przykładowo Google informuje, że usługobiorcy posiadający konto na Google – zgodnie z polityką prywatności tego pośrednika – muszą się liczyć z tym, że Administrator Google (nazywany administratorem domeny) może: uzyskiwać dostęp do informacji zapisanych na koncie, np. do poczty e-mail, oraz zachowywać te informacje; wyświetlać statystyki konta, np. informacje o liczbie instalowanych aplikacji; zmienić hasło do konta; zawiesić lub zablokować dostęp do konta; pobrać informacje o koncie, by zapewnić zgodność z obowiązującym prawem, procesem prawnym lub prawomocnym żądaniem instytucji państwowych; ograniczyć możliwość usuwania lub edytowania informacji lub ustawień prywatności, <https://policies.google.com/privacy?hl=pl> (dostęp: 2.09.2023).

powyżej środki, cele i czynności posłużyły ustawodawcy europejskiemu do sformułowania definicji legalnej terminu „moderowanie treści” zawartej w art. 3 lit. t AUC.

Na moderowanie składa się zatem szereg czynności, które mogą być podejmowane przez pośrednika osobno, uzupełniając albo równolegle. Mogą także pozostawać ze sobą w związku przyczynowo-skutkowym i w różnym stopniu oddziaływać na wolność wypowiedzi, wywołując dolegliwości zarówno o różnej intensywności, jak i na różnych płaszczyznach, tj. w sferze praw osobistych i majątkowych. Usunięcie konta lub ograniczenie świadczenia usługi przez pośredników internetowych może bowiem być odczuwalne jako ograniczenie wolności wypowiedzi albo, ze względu na ograniczenie prawa do zarobkowania (demonetyzacja), ingerencja w sferę praw majątkowych. Rezultatem depozycjonowania będzie – co do zasady – ograniczenie widoczności, natomiast zawieszenie konta będzie skutkowało demonetyzacją.

Moderowanie treści obejmuje zatem szereg czynności, które – jak wynika z art. 17 ust. 1 AUC – skutkują „ograniczeniem”. Ustawodawca europejski nie wskazał jednak wartości, wolności ani praw, których dotyczy „ograniczenie” wymienione w tym przepisie. Dowodzenia nie wymaga jednak, że obejmuje ono – obok innych wolności i praw, jak w szczególności ochrona prywatności, a także ochrona danych osobowych – przede wszystkim swobodę wypowiedzi. Jeśli więc ograniczenie dotyczy praw podstawowych gwarantowanych w KPP, takich jak, w szczególności, wolność wypowiedzi, to ograniczenie to powinno pozostawać w zgodzie z warunkami określonymi w art. 52 ust. 1 KPP. Zgodnie z art. 52 ust. 1 Karty praw podstawowych „Wszelkie ograniczenia w korzystaniu z praw i wolności uznanych w Karcie muszą być przewidziane ustawą i szanować istotę tych praw i wolności. Z zastrzeżeniem zasady proporcjonalności, ograniczenia mogą być wprowadzone wyłącznie wtedy, gdy są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób”.

Termin „moderowanie treści” – ze względu na brzmienie zawartej w art. 3 lit. t AUC definicji legalnej, a także rozwinięcie tej definicji w kolejnych przepisach AUC, w szczególności w art. 17, oraz powiązanie jej z terminem „nielegalne treści” zdefiniowanym w art. 3 pkt h AUC – ma znaczenie normatywne i definiuje zakres oraz charakter upoważnień adresowanych do organów publicznych (Komisja Europejska, państwa członkowskie UE) do „ograniczania” wolności

wypowiedzi. Zdefiniowanie terminu „moderowanie treści” w akcie prawnym o randze rozporządzenia PE wypełnia formalną przesłankę dopuszczalności wprowadzania ograniczeń praw i wolności, wskazaną w art. 52 ust. 1 KPP, potwierdzając, że ograniczenie wolności wypowiedzi ma podstawę w ustawie. Ustanowienie dopuszczalności ograniczenia w ustawie nie przesądza jednak o jego prawnej skuteczności, jeśli ustawa nie zawiera wystarczająco precyzyjnego opisu ograniczenia albo nie precyzuje przesłanek jego dopuszczalności.

Wskazane w ustawie ograniczenie musi spełniać wymóg przejrzystości i być na tyle konkretnie wyrażone, że osoby, które mogłyby zostać dotknięte takim ograniczeniem, powinny mieć możliwość jego przewidzenia. Rzecznik Generalny UE, powołując się obficie na judykaty ETS, szczegółowo omówił, w opinii sporządzonej do wyroku TS z dnia 24 listopada 2011 r. (C-70/10)²²¹, na czym zasadza się wskazana w art. 52 ust. 1 KPP przesłanka „ustanowienia ograniczenia w ustawie”. Rzecznik powołał w szczególności wyrok w sprawie Hoechst przeciwko Komisji²²², w którym Trybunał podkreślił, że ingerencja władz publicznych w dziedzinę prywatnej działalności jakiegokolwiek osoby, czy to fizycznej, czy prawnej, musi mieć podstawę prawną i być uzasadniona względami określonymi w prawie. Ten wymóg ochrony, uznany za ogólną zasadę prawa unijnego, jest korelatem zasad legalności i pewności prawa, które wynikają z idei państwa prawa. Trybunał wielokrotnie orzekał, że zasada pewności prawa wymaga, by uregulowania nakładające obciążenia na jednostki²²³, wywierające dla nich negatywne skutki²²⁴, a także nakładające środki ograniczające mające znaczący wpływ na prawa i wolności

²²¹ Wyrok TS w sprawie Scarlet Extended przeciwko SABAM.

²²² Wyrok TS w sprawie Hoechst AG przeciwko Komisji Wspólnot Europejskich.

²²³ Wyroki TS: z dnia 9 lipca 1981 r. w sprawie Gondrand i Garancini, 169/80, pkt 17; z dnia 22 lutego 1989 r. w sprawach połączonych Komisja przeciwko Francji i Wielkiej Brytanii, 92/87 i 93/87, pkt 22; z dnia 13 lutego 1996 r. w sprawie Van Es Douane Agenten, C-143/93, pkt 27; z dnia 17 lipca 1997 r. w sprawie National Farmers' Union i in., C-354/95, pkt 57; z dnia 16 października 1997 r. w sprawie Banque Indosuez i in., C-177/96, pkt 27; z dnia 23 września 2003 r. w sprawie BGL, C-78/01, pkt 71; z dnia 20 listopada 1997 r. w sprawie Wiener SI, C-338/95, pkt 19.

²²⁴ Wyroki: z dnia 7 czerwca 2005 r. w sprawie VEMW i in., C-17/03, pkt 80; z dnia 14 stycznia 2010 r. w sprawie Stadt Papenburg, C-226/08, pkt 45; z dnia 14 września 2010 r. w sprawie Akzo Nobel Chemicals et Akros Chemicals przeciwko Komisji i in., C-550/07 P, pkt 100; z dnia 2 grudnia 2010 r. w sprawie Jakubowska, C-225/09, pkt 42.

określonych osób²²⁵, były na tyle jasne i precyzyjne, by zainteresowane osoby miały możliwość jednoznacznego poznania swoich praw i obowiązków i podjęcia w związku z tym odpowiednich działań²²⁶. Tymczasem konstrukcja modelu ograniczenia wolności wypowiedzi poprzez „moderowanie treści” nie tylko nie zawiera zamkniętego katalogu czynności, ale ponadto wymienione w definicji czynności także wymagałyby – dla spełnienia wymogu wystarczającej precyzji – zdefiniowania.

W AUC wskazano zależności, jakie zachodzą pomiędzy poszczególnymi czynnościami moderowania oraz zasygnalizowano skutki tych czynności. Każda z czynności moderowania wywołuje skutek bezpośrednio albo pośrednio ingerujący w swobodę wypowiedzi, przy czym skutek ten występuje z różną intensywnością i oddziałuje niekiedy też na inne prawa i wolności użytkownika, w tym prawo do prywatności, prawo ochrony danych osobowych, prawa autorskie, a także, w przypadku demonetyzacji, na prawo do uzyskiwania wynagrodzenia oraz prawo do swobody prowadzenia działalności gospodarczej. W motywie 55 przyjęto np., że „ograniczenie widoczności może polegać na depozycjonowaniu w ramach plasowania lub w systemach rekomendacji, a także na ograniczeniu dostępności usługi dla co najmniej jednego odbiorcy usługi lub zablokowaniu widoczności wpisów danego użytkownika dla całej społeczności internetowej poza autorem bez jego wiadomości – tzw. *shadow banning* (motyw 55). W konsekwencji, pomimo że formalnie zakomunikowanym celem jest ograniczenie widoczności, to jednak czynności z tym celem związane takie jak, w szczególności, zablokowanie wpisów albo usunięcie informacji o użytkowniku z systemów rekomendacji faktycznie skutkować mogą także pozbawieniem go wpływów z reklam

²²⁵ Wyrok z dnia 29 kwietnia 2010 r. w sprawie M i in., C-340/08, pkt 65.

²²⁶ Wyroki: z dnia 30 stycznia 1985 r. w sprawie Komisja przeciwko Danii, 143/83, pkt 10; z dnia 21 czerwca 1988 r. w sprawie Komisja przeciwko Włochom, 257/86, pkt 12; z dnia 16 czerwca 1993 r. w sprawie Francja przeciwko Komisji, C-325/91, pkt 26; z dnia 1 października 2009 r. w sprawie Komisja przeciwko Radzie, C-370/07, pkt 39; z dnia 11 listopada 2010 r. w sprawie Grootes, C-152/09, pkt 43; z dnia 22 grudnia 2010 r. w sprawie Gowan Comércio, C-77/09, pkt 47. W odniesieniu do wymogu jasności i szczegółowości przepisów transponujących dyrektywę zob. m.in. wyroki: z dnia 20 października 2005 r. w sprawie Komisja przeciwko Wielkiej Brytanii, C-6/04, pkt 21; z dnia 10 maja 2007 r. w sprawie Komisja przeciwko Austrii, C-508/04, pkt 73; z dnia 3 marca 2011 r. w sprawie Komisja przeciwko Włochom, C-50/09, pkt 46.

(demonetyzacją), a w sferze praw osobistych, w skrajnych wypadkach, pozbawieniem możliwości korzystania ze swobody wypowiedzi.

Moderować to: „kierować, hamować, poskramiać”, a także „łagodzić napięcia, nie dopuszczać do skrajności”²²⁷. Pośrednicy internetowi występują w charakterze moderatora, a zatem osoby, która „łagodzi napięcia i nie dopuszcza do skrajności”²²⁸. W usługach Google „treści naruszające zasady są usuwane przez sztuczną inteligencję Google lub – jeśli potrzebne jest bardziej szczegółowe zbadanie sprawy – oznaczane do dalszego sprawdzenia przez specjalistów i analityków, którzy przeprowadzają ocenę treści, jakiej nie mogłyby wykonać same algorytmy, na przykład dlatego, że w danym przypadku konieczne jest zrozumienie kontekstu”²²⁹. Zatem ewentualne zastosowanie ograniczenia pozostawione do decyzji sztucznej inteligencji może budzić wątpliwości co do zgodności ograniczenia z przesłankami wskazanymi w art. 52 ust. 1 KPP.

Nie istnieje katalog zobiektywizowanych kryteriów, które pozwalałyby na zastosowanie jednolitego mechanizmu przyjmowania i kategoryzowania zgłoszeń²³⁰. Google podaje, że tylko w odniesieniu do usługi YouTube co minutę przesyłanych jest 500 godzin treści²³¹. Przyznaje zarazem, że dziennie usuwa dziesiątki milionów wiadomości ze swoich usług²³² na podstawie zarówno zgłoszeń, jak i decyzji podejmowanych z własnej inicjatywy.

²²⁷ Hasło: *moderować*, [w:] *Uniwersalny słownik języka polskiego*, Warszawa 2003, s. 698.

²²⁸ Hasło: *moderator*, [w:] *Tamże*, s. 697.

²²⁹ *W jaki sposób stosujemy automatyzację do moderowania treści*, Pomoc Google, https://support.google.com/displayvideo/answer/13584894?hl=pl_ALL&ref_topic=3528231 (dostęp: 3.10.2023).

²³⁰ Pośrednicy przyznają to w swoich wewnętrznych dokumentach. Google pisze, że „Szeroki zakres informacji dostępnych online uniemożliwia poświęcenie każdej treści równej uwagi, ludzkiej recenzji i rozważań. Nawet gdyby było to możliwe, rozsądni ludzie mogliby nie zgadzać się co do odpowiednich wyników. Podobnie, żaden system rankingowy nie może być doskonały, ani nie wszyscy zgadzają się co do wartości, dla których powinni optymalizować”, zob. *Information quality and content moderation*, Google YouTube, https://blog.google/documents/83/information_quality_content_moderation_white_paper.pdf (dostęp: 3.10.2023).

²³¹ *W jaki sposób stosujemy automatyzację...*

²³² Google przyznaje: „Egzekwujemy nasze zasady dotyczące treści na dużą skalę i codziennie podejmujemy dziesiątki milionów działań przeciwko treściom, które nie są zgodne z »zasadami ruchu drogowego« dotyczącymi co najmniej jednego z naszych produktów” (tamże, s. 6). „W 2019 r. z YouTube usunięto ponad 30 milionów filmów z powodu naruszenia naszych Wytycznych dla społeczności. W 2019 r. usunęliśmy z naszych

Mechanizm przyjmowania zgłoszeń oraz ich selekcjonowania i doko-
nywania oceny zasadności zgłoszenia nie gwarantuje użytkownikom, że
decyzje dotyczące treści zostaną podjęte w sposób bezstronny i niearbitralny
na podstawie jednolitych, niedyskryminacyjnych, jednakowych kryteriów
w stosunku do wszystkich użytkowników²³³. Pośrednicy nie dają gwarancji
zastosowania takiego mechanizmu, albowiem nigdy taki nie powstał i – real-
nie – wydaje się niemożliwe jego stworzenie. Pośrednicy odsyłają zatem
w swoich regulaminach (warunkach korzystania z usługi) do obowiązują-
cych u nich zasad, używając bardzo często zaimka dzierżawczego, np. „nasze
zasady”²³⁴, „nasze podejście”²³⁵, „w naszej ocenie”, „nasze warunki”, „nasz
regulamin”. Nie jest jednak jasne, co kryje się pod tymi określeniami, więc nie
wiadomo, czy za zaimkiem „nasze” rzeczywiście stoi jakiś kolegialny organ,

systemów ponad 2,7 miliarda złotych reklam i podjęliśmy działania przeciwko prawie
1 milionowi złotych kont reklamodawców. Po stronie wydawców zamknęliśmy ponad
1,2 miliona kont i usunęliśmy reklamy z ponad 21 milionów stron internetowych, które
należą do naszej sieci wydawców, ponieważ naruszają nasze zasady. Zasady Google Play
zabraniają wielu rodzajów zwodniczych zachowań i treści wprowadzających w błąd,
zwłaszcza jeśli dotyczą one rozpowszechniania aplikacji związanych z medycyną lub zdro-
wieniem osobistym. Jeśli okaże się, że programiści naruszają te zasady, ich aplikacje mogą
zostać usunięte ze Sklepu Google Play. W 2019 roku Google Play zatrzymał ponad
790 000 aplikacji naruszających zasady, zanim zostały opublikowane w Sklepie Play.
W 2019 roku Mapy Google wykryły i usunęły ponad 75 milionów opinii naruszających
zasady i 4 miliony fałszywych profili firmowych, a także usunęły ponad 580 000 opinii
i 258 000 wizytówek firm, które zostały nam bezpośrednio zgłoszone jako naruszające
nasze zasady. Sprawdziliśmy też i usunęliśmy ponad 10 milionów zdjęć i 3 miliony filmów,
które naruszały naszą politykę treści w Mapach Google, a także wyłączyliśmy ponad
475 000 kont użytkowników, które uznano za naruszające zasady” (tamże, s. 7).

²³³ Google wyjaśnia, że przyjmując zgłoszenia, posługuje się formularzami, ale także
innymi kanałami: „Przekazując żądanie usunięcia treści, czy to za pomocą naszych oficjal-
nych formularzy internetowych, czy nieformalnie innymi kanałami (np. za pośrednictwem
zespołu ds. polityki publicznej), osoba zgłaszająca określa powód zgłoszenia”, zob. *Żądania
usunięcia treści składane przez władze państwowe*, Google Raport przejrzystości, <https://transparencyreport.google.com/government-removals/overview> (dostęp: 3.10.2023).

²³⁴ *Wspólna praca nad opracowywaniem zasad*, Google Centrum przejrzystości,
<https://transparency.google.com/our-approach/our-policy-process/> (dostęp: 3.10.2023).
Facebook w swoim regulaminie pisze: „Standardy społeczności: Są to nasze zasady
zapobiegające publikowaniu niebezpiecznych treści”, zob. *Demonetyzacja strony i trybu
profesjonalnego – informacje*, Meta Centrum pomocy dla firm, <https://www.facebook.com/business/help/2339387956318180?id=2520940424820218> (dostęp: 3.10.2023).

²³⁵ *Wspólna praca nad opracowywaniem zasad. Nasze podejście*, Google Centrum
przejrzystości, <https://transparency.google.com/our-approach/our-policy-process/> (dostęp:
3.10.2023).

a jeśli tak, to kto wchodzi w jego skład i jak ten skład został wybrany. Kogo w istocie reprezentuje pośrednik, sugerując, że jego działanie nie jest arbitralne? Jeśli moderator podejmuje decyzje o zastosowaniu określonej formy ograniczenia wolności, to nie jest jasne, jakimi przesłankami się kierował²³⁶. W przypadku zarówno jawnych, jak i niejawnych metod ingerowania w swobodę wypowiedzi dostawcy usług cyfrowych stosują własne wzorce oceny (tzw. nasze zasady). Dostawcy używają w swoich „zasadach”, „regulaminach” i „standardach społeczności” zbieżnych terminów, w szczególności takich jak „mowa nienawiści”, „przemoc”, „nakłanianie do przemocy”, jednakże nie zawsze są one wypełniane taką samą treścią²³⁷. Zbiorczo są one określane jako „nielegalne treści”. Obowiązki skierowane do dostawców usług cyfrowych w AUC mają na celu „przeciwdziałanie rozpowszechnianiu nielegalnych treści w internecie oraz zagrożeniom społecznym, jakie może stwarzać rozpowszechnianie dezinformacji lub innych treści” (motyw 9 AUC).

Google np. pisze, że „Nasze zasady powstają w wyniku skrupulatnych badań, konsultacji z ekspertami, a tam gdzie to niezbędne, również z uwzględnieniem przepisów prawa. W miarę jak zmienia się otaczający nas świat, ewoluują, dzięki czemu zapobiegamy nadużyciom, a jednocześnie pomagamy firmom i twórcom rozwijać się i docierać do nowych odbiorców”²³⁸. Google potwierdza w ten sposób, że respektuje prawo, ale tylko „tam gdzie to niezbędne”, korzysta z pomocy ekspertów, ale nie jest jasne, w jakim celu, w jakim zakresie ani w jaki sposób dokonuje ich doboru. Google potwierdza ponadto, że zasadą jest brak zasad, ponieważ Google zmienia je nieustannie „w miarę jak zmienia się otaczający nas świat”. Oznacza to, że nie istnieje stały katalog zasad,

²³⁶ Google pisze, że „starannie” analizuje zgłoszenia, nie podając żadnego modelu staranności ani stosowanych kryteriów i nie wskazując, jakie kompetencje mają osoby, które dokonują „starannej analizy”: „Gdy otrzymujemy skargi dotyczące treści na naszych platformach, starannie analizujemy te zgłoszenia, aby dopilnować, że zostaną poprawnie skategoryzowane”, zob. *Żądania usunięcia treści...*

²³⁷ Przykładowo w ujęciu proponowanym przez Google nakłanianie do przemocy jest identyfikowane jako „Zachęcanie do szkodliwych lub niebezpiecznych zachowań: treści, które przedstawiają szczególnie szkodliwe lub niebezpieczne zachowania lub zachęcają użytkowników, aby zaangażować się w te zachowania” (*Information quality...*, s. 10). Nadal nie jest jasne, jak należy rozumieć termin „szczególnie szkodliwe treści”.

²³⁸ *Wspólna praca nad opracowywaniem zasad. Jak tworzymy zasady*, Google Centrum przejrzystości, <https://transparency.google/our-approach/our-policy-process/> (dostęp: 3.10.2023).

a nadto zmiany dokonywane w katalogu następują permanentnie według jednostronnie ustalanych przez Google kryteriów, w wybranym zakresie i terminie. W konsekwencji nie jest wykluczone, że czynności użytkowników, które dziś są dopuszczalne, następnego dnia zostaną uznane przez Google za nielegalne. Google powoływać się w tej ocenie będzie mógł zarówno na swoje zasady, jak i na przepisy prawa. Okoliczność ta dowodzi, że Google, a także pozostali pośrednicy, uznają za równoważne przepisy prawa i postanowienia ich własnych regulaminów. Stanowisko to jest rezultatem dokonywanej przez pośredników interpretacji postanowień zawartych w AUC. Uprawniają one pośredników do dokonywania swobodnego wyboru podstawy podejmowanych czynności poprzez wskazanie, czy ma ona źródło w akcie normatywnym, czy w postanowieniach umownych (warunkach korzystania z usług). W efekcie od woli pośredników zależy to, kiedy i na które postanowienia zawarte w rozporządzeniach AUC i ARC będą się powoływać.

Google pisze, że „Inaczej podchodzimy do zasad dotyczących usług, gdy umożliwiamy publiczne udostępnianie treści, a inaczej, gdy chcemy w większym stopniu chronić prywatność”²³⁹. Nie wyjaśnia jednak według jakich parametrów kategoryzuje treści jako „prywatne”, a kiedy uznaje je za „publiczne”. Nie ujawnia także ani treści zasad, którymi się kieruje, ani różnic, jakie – zgodnie z założeniami Google – istnieją pomiędzy tymi dwoma podejściami. Google uzależnia treść i stosowanie zasad od funkcji usługi, jaką realizuje. W szczególności, jak wskazano: „Możemy inaczej podchodzić do zasad w przypadku funkcji, które porządkują treści lub podpowiadają je użytkownikom”. Nie jest jednak jasne, kiedy Google daje prymat funkcji porządkowania ponad funkcję doradzania. Nie przesądza bowiem o tym rodzaj usługi. Przykładowo, w przypadku usługi wyszukiwarki internetowej użytkownik jest profilowany, a zatem w „podpowiadaniach” uzyskuje wyselekcjonowaną przez Google, spersonalizowaną kolejkę wyników wyszukiwania. Nie jest zatem jasne, czy w takim wypadku Google stosowało „funkcję porządkowania”, czy „funkcję podpowiadania”.

Moderowanie treści może następować z wykorzystaniem zarówno jawnych, jak i niejawnych metod działania. W przypadku jawnych metod pośrednik

²³⁹ Wspólna praca nad opracowywaniem zasad. Dlaczego zasady obowiązujące w poszczególnych usługach są różne, Google Centrum przejrzystości, <https://transparency.google/our-approach/our-policy-process/> (dostęp: 3.10.2023).

powiadamia użytkownika o zastosowanym wobec niego ograniczeniu, spełniając w ten sposób obowiązek z art. 17 ust. 1 AUC. Zgodnie z tym przepisem dostawcy usług cyfrowych mają obowiązek uzasadnienia „ograniczeń nałożonych ze względu na fakt, iż informacje przekazane przez odbiorcę usługi stanowią nielegalne treści lub są niezgodne z warunkami korzystania z usług dostawcy” wówczas, gdy ograniczenie to polega co najmniej na jednej z następujących czynności:

- a) ograniczenia w zakresie widoczności określonych informacji przekazywanych przez dostawcę usługi, w tym usuwanie treści, uniemożliwianie dostępu do treści lub depozycjonowanie treści;
- b) zawieszenie, zakończenie lub inne ograniczenie płatności pieniężnych;
- c) zawieszenie lub zakończenie świadczenia usługi w całości lub w części;
- d) zawieszenie lub zamknięcie konta odbiorcy usługi. Wszystkie powyżej wskazane czynności mieszczą się w pojęciu „moderowanie treści” (art. 3 lit. t AUC).

Uzasadnienie decyzji o ograniczeniu zastosowanym przez dostawcę usługi powinno zawierać co najmniej następujące informacje:

- a) wskazanie, czy decyzja obejmuje usunięcie informacji, uniemożliwienie dostępu do nich, depozycjonowanie lub ograniczenie widoczności informacji lub zawieszenie lub zakończenie płatności pieniężnych odnoszących się do takich informacji albo nakłada inne środki, o których mowa w ust. 1, w odniesieniu do informacji, oraz, w stosownych przypadkach, zakres terytorialny decyzji i okres jej obowiązywania;
- b) fakty i okoliczności, na podstawie których podjęto decyzję, w tym w stosownych przypadkach informację, czy decyzję podjęto na podstawie zgłoszenia dokonanego zgodnie z art. 16, czy na podstawie dobrowolnych czynności sprawdzających prowadzonych z własnej inicjatywy oraz, gdy jest absolutnie niezbędne, tożsamość zgłaszającego;
- c) w stosownych przypadkach informacje na temat wykorzystania zautomatyzowanych środków podczas podejmowania decyzji, w tym informację, czy decyzję podjęto w odniesieniu do treści wykrytych lub zidentyfikowanych z wykorzystaniem zautomatyzowanych środków;
- d) jeżeli decyzja dotyczy potencjalnie nielegalnych treści, wskazanie podstawy prawnej, na której opiera się decyzja, oraz wyjaśnienia dotyczące

powodów, dla których na tej podstawie uznaje się dane informacje za nielegalne treści;

- e) jeżeli decyzja opiera się na zarzucanej niezgodności informacji z warunkami korzystania z usług dostawcy usługi hostingu, wskazanie podstawy umownej, na której opiera się decyzja, oraz wyjaśnienia dotyczące powodów, dla których uznaje się dane informacje za niezgodne z tą podstawą;
- f) jasne i przyjazne dla użytkownika informacje na temat przysługujących odbiorcy usługi możliwości odwołania się od decyzji, w szczególności w stosownych przypadkach za pośrednictwem wewnętrznych mechanizmów rozpatrywania skarg, pozasądowego rozstrzygania sporów i sądowych środków odwoławczych (art. 17 ust. 2 AUC).

Moment podjęcia przez dostawcę usług decyzji o wprowadzeniu ograniczenia i sporządzenie jej uzasadnienia rozpoczyna jawny etap działania dostawcy, którego celem jest usunięcie nielegalnych treści i zapobieżenie ich rozpowszechnieniu w przyszłości. Zgodnie z art. 17 ust. 2 AUC uzasadnienie decyzji o wprowadzonym przez dostawcę ograniczeniu powinno zostać doręczone użytkownikowi usługi najpóźniej w dniu nałożenia ograniczenia, bez względu na powód i sposób jego nałożenia. Dostawca ma także obowiązek poinformowania „bez zbędnej zwłoki” o swojej decyzji osobę, która zgłosiła naruszenie na podstawie obowiązujących u dostawcy mechanizmów zgłaszania im obecności w ich usłudze określonych informacji, które dana osoba lub dany podmiot uważają za nielegalne treści (art. 16 ust. 5 w zw. z art. 16 ust. 1 AUC). Natomiast wszystkie wcześniej podejmowane przez dostawcę czynności, tj. przed nałożeniem ograniczenia, nie muszą mieć charakteru jawnego. Przed nałożeniem ograniczenia dostawca nie ma zatem obowiązku powiadamiania podmiotu, wobec którego podjął czynności sprawdzające, że takie czynności są wobec niego prowadzone niezależnie od tego, czy dostawca podjął je z własnej inicjatywy, czy też na podstawie zgłoszenia.

Posługiwanie się przez dostawców niejawnymi metodami moderowania jest rezultatem braku obowiązku powiadamiania odbiorców o podejmowanych wobec nich czynnościach sprawdzających. Jedną z niejawnych metod ograniczania wolności wypowiedzi jest zmniejszenie widoczności treści, a także ukrywanie treści przed innymi użytkownikami bez wiedzy użytkownika, który umieścił dane treści w internecie. Metoda ta jest nazywana

„shadow banning” (blokowanie w cieniu). Shadow banning polega na ograniczeniu widoczności czyichś postów (wiadomości lub zdjęć w mediach społecznościowych), zwykle bez wiedzy osoby, która je opublikowała²⁴⁰, i oznacza dosłownie „ukrytą blokadę” – blokadę w tle (ang. *shadow*, czyli cień). Shadowban nie jest prosty do wykrycia. Polega na ukrywaniu przed innymi użytkownikami umieszczanych postów, co wpływa na ich widoczność albo całkowicie jej pozbawia²⁴¹.

Moderowanie treści ze względu na zakres i sposób zdefiniowania tego pojęcia w treści art. 3 lit. t AUC legalizuje wszelkie podejmowane przez dostawców usług cyfrowych czynności, o ile ich celem jest „w szczególności, wykrywanie, identyfikowanie i zwalczanie nielegalnych treści lub informacji niezgodnych z warunkami korzystania z usług”. W świetle przyjętej w tym przepisie definicji o legalności „moderowania” przesądzać będą dwie przesłanki, tj. po pierwsze, uprawdopodobnienie przez dostawcę, że treści, które zostały poddane procesowi moderowania, mają charakter nielegalny oraz, po drugie, wykazanie, że celem zastosowanych przez dostawcę środków było ich wykrycie, identyfikowanie i zwalczanie. Ciężące na dostawcach usług obowiązki związane z moderowaniem treści wymagają wykazania przejrzystości na etapie podejmowania decyzji o zastosowanych ograniczeniach oraz ich rozliczalności. W motywie 49 wskazano, że „aby zapewnić odpowiedni poziom przejrzystości i rozliczalności, dostawcy usług pośrednich mają obowiązek podawania co roku do wiadomości publicznej sprawozdanie w formacie nadającym się do odczytu maszynowego, zgodnie ze zharmonizowanymi wymogami zawartymi w AUC, dotyczące moderowania treści, w którym brali udział, w tym środków wprowadzonych w rezultacie stosowania i egzekwowania warunków korzystania z ich usług” (motyw 49). Aby zapewnić przejrzystość i umożliwić kontrolę decyzji dostawców platform internetowych

²⁴⁰ Hasło: *shadowbanning*, [w:] *Cambridge Dictionary*, <https://dictionary.cambridge.org/pl/dictionary/english/shadowbanning> (dostęp: 10.10.2023).

²⁴¹ Jak wskazuje się w poradnikach dla osób korzystających np. z Instagrama: „Instagram w pewnym momencie może zacząć ukrywać Twoje posty bez informowania o tym fakcie. Ban polega na ograniczaniu wyświetlenia postów i komentarzy dla kont, które Cię nie obserwują. Blokuje więc możliwość uzyskiwania nowych obserwujących i docierania do osób, które mogłyby być zainteresowane Twoim contentem”, zob. *Shadowban – co to jest i jak się przed nim chronić?*, 10.07.2021, Foto-filtry.pl, <https://foto-filtry.pl/shadowban-co-to-jest-i-jak-sie-przed-nim-chronic/> (dostęp: 30.09.2023).

dotyczących moderowania treści oraz monitorowanie rozpowszechniania nielegalnych treści w internecie, Komisja powinna prowadzić i publikować bazę danych zawierającą decyzje dostawców platform internetowych wraz z uzasadnieniami, w przypadku gdy usuwają oni informacje lub w inny sposób ograniczają ich dostępność lub dostęp do nich (motyw 66).

Podsumowując, stwierdzić należy, że każda czynność podejmowana przez dostawców usług cyfrowych, która ingeruje w sferę wolności wypowiedzi użytkowników internetu jest, co do zasady, dopuszczalna. W akcie o usługach cyfrowych ustanowiono na rzecz pośredników internetowych domniemanie prawne wzruszalne, upoważniając ich do ingerowania w wolność wypowiedzi użytkowników bez ograniczeń ani co do formy i środków, ani co do zakresu tych ingerencji. Nie ulega wątpliwości, że na dostawcach usług ciąży także pewne obowiązki, przede wszystkim sprawozdawcze oraz w zakresie zachowania przejrzystości, co jednak nie uchyla przyznanych im w AUC uprawnień i upoważnień do udzielania i odbierania użytkownikom możliwości wypowiadania się za pośrednictwem środka komunikowania, jakim jest internet.

B. Monitorowanie treści

Aktywność użytkowników internetu, w szczególności w sferze korzystania przez nich z wolności wypowiedzi, podlega wielokrotnemu monitorowaniu, przy czym podmiotem monitorującym jest zawsze dostawca usług pośrednictwa internetowego. Tylko bowiem na rzecz pośredników internetowych ustawodawca europejski ustanowił upoważnienia do podejmowania czynności, które, ze względu na ich cel i zakres, obejmują monitorowanie i filtrowanie treści umieszczanych przez odbiorców usług. Monitorowanie i filtrowanie treści umieszczanych przez użytkownika, w szczególności w celach wykrywczych, odbywa się – co do zasady – niejawnie, a zatem bez wiedzy użytkownika odnośnie do podejmowanych wobec niego czynności i stosowanych przez dostawcę metod.

Formalnie jawność jest zachowana w odniesieniu do czynności „śledzenia użytkowników” wówczas, gdy termin „śledzenie” zostanie zawężony do gromadzenia cookies²⁴² i wykorzystywania innych technologii²⁴³ wskazywanych

²⁴² Istnieją różne rodzaje cookies, które wyróżnia się ze względu na funkcje, jakie pełnią. Najczęściej wskazuje się na cookies: 1) niezbędne do korzystania z usługi – uwierzytelniające pliki cookies wykorzystywane do usług wymagających uwierzytelniania w ramach serwisu, służące do zapewnienia bezpieczeństwa; 2) analityczne, „wydajnościowe” pliki cookies – umożliwiające zbieranie informacji o sposobie korzystania ze stron internetowych; 3) statystyczne – „funkcjonalne” pliki cookies, m.in. umożliwiające „zapamiętanie” wybranych przez użytkownika ustawień i personalizację interfejsu użytkownika. Poza własnymi plikami cookies, na stronie internetowej mogą być wykorzystywane tzw. ciasteczka stron trzecich (ang. *third party cookies*), np. cookies Google. Cookies identyfikują dane urządzenia i przeglądarki używane do przeglądania stron internetowych – pozwalają np. dowiedzieć się, czy dane urządzenie odwiedzało już stronę. Cookies zazwyczaj zawierają nazwę strony internetowej, z której pochodzą, czas przechowywania ich na urządzeniu końcowym, a także, w zależności od stosowanych technologii mogą być przetwarzane np.: 1) dane urządzenia: typ/model urządzenia, unikalne identyfikatory urządzeń, adres MAC, adres IP, system operacyjny, wersja systemu operacyjnego i ustawienia urządzenia, ustawiony język, rozdzielczość ekranu, wersja i rodzaj przeglądarki internetowej; 2) dzień/zdarzenia: czas korzystania z serwisu, dane wyszukiwania oraz wszelkie informacje przechowywane w plikach cookies, które jednoznacznie identyfikują przeglądarkę lub konto użytkownika, np. ostatnia wizyta na stronie, długość wizyty na stronie, rodzaj odwiedzanych stron oraz podstron, adres odwiedzanej strony (URL), wersja przeglądarki internetowej oraz rodzaj, ustawiony język w przeglądarce; 3) dane dotyczące lokalizacji: adres IP, dane o lokalizacji uzyskane za pomocą różnych technologii pozycjonowania (długość i szerokość geograficzna, ISP – np. Play/Orange, inne podane przez użytkownika dane lokalizacyjne), takich jak GPS, punkty dostępu Wi-Fi lub inne czujniki, które mogą dostarczać dane w pobliżu urządzenia (po wyrażeniu zgody na lokalizację); 4) inne dane: źródło wejścia pod UTM, linki, w które kliknął użytkownik, liczba kliknięć i widoków dynamicznej zawartości strony (Informacje zebrane w szczególności z *Polityki prywatności Google*, <https://policies.google.com/technologies/cookies?hl=pl>, a ponadto *Polityki cookies centrumwroclaw.pl*, <https://centrumwroclaw.pl/assets/download/pliki-cookie.pdf> oraz *Plików cookie* strony Unii Europejskiej, https://european-union.europa.eu/cookies_pl). Google definiuje pliki cookies, opisując tę technologię jako przyjazną i pomocną dla użytkownika, a w konsekwencji nieoddziałującą w żaden negatywny sposób na zakres praw i wolności użytkownika: „Cookies to niewielkie pliki tekstowe wysyłane do przeglądarki przez witrynę, którą w danym momencie odwiedzasz. Pozwalają jej zapamiętać informacje na temat Twojej wizyty. Dzięki temu przy kolejnych odwiedzinach witryna jest łatwiejsza w obsłudze i lepiej dostosowana do Twoich preferencji. Do tych celów mogą być używane także inne technologie, między innymi unikalne identyfikatory pozwalające zidentyfikować przeglądarkę, aplikację, urządzenie, piksele lub pamięć lokalną”; zob. *Jak Google korzysta z plików cookie*, Google Prywatność i warunki, <https://policies.google.com/technologies/cookies?hl=pl> (dostęp: 7.10.2023).

²⁴³ Zwraca uwagę, że „cookies to jedna z wielu używanych przez Google technologii. Nie wszystkie zostały wskazane w Polityce prywatności, a w konsekwencji nie zostały one

przez dostawców usług w regulaminach prywatności²⁴⁴. Jawność formalna została zagwarantowana użytkownikom internetu w Ogólnym rozporządzeniu o ochronie danych osobowych (RODO)²⁴⁵ i wypływa z faktu, że dostawcy usług cyfrowych przetwarzający dane osobowe mają status administratorów danych osobowych (ADO), a w konsekwencji ciąży na nich obowiązek wskazany w art. 13 RODO dotyczący poinformowania każdego usługobiorcy o fakcie przetwarzania jego danych (obowiązek informacyjny)²⁴⁶. Formalnie zatem odbiorcy usług cyfrowych mają informacje o fakcie przetwarzania „cookies” pozwalających na śledzenie ich aktywności w internecie²⁴⁷.

Stosowania technologii cookies oraz innych technologii opisywanych przez dostawców usług cyfrowych w politykach prywatności nie należy utożsamiać z terminem „monitorowanie”, którym ustawodawca europejski wielokrotnie operuje w AUC²⁴⁸, ani terminem „filtrowanie”, którym posługiwał się europejski Trybunał Sprawiedliwości²⁴⁹. Śledzenie, o którym mowa w politykach prywatności, polega na przetwarzaniu danych osobowych użytkowników

opisane i nie jest dla użytkownika jasne, w jaki sposób Google ich używa ani nie jest jasne, jakie informacje są przez Google gromadzone z użyciem tych technologii”; zob. *Polityka prywatności*, <https://policies.google.com/privacy?hl=pl> (dostęp 7.10.2023).

²⁴⁴ Obowiązek poinformowania podmiotów danych osobowych o przetwarzaniu ich danych został nałożony na administratorów danych osobowych (ADO) w art. 13 RODO. Jeśli dane użytkowników internetu są gromadzone za pośrednictwem technologii cookies, to na administratorze wykorzystującym tę technologię ciąży obowiązek informacyjny z art. 13 RODO. Obowiązek ten ADO mogą spełnić albo poprzez indywidualne zawiadomianie odbiorców usług o zakresie, celu i terminie przetwarzania danych osobowych odrębnie w odniesieniu do każdej usługi, albo informując – jednocześnie – wszystkich usługobiorców poprzez umieszczenie na stronie internetowej tzw. Polityki prywatności.

²⁴⁵ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. UE L Nr 119, s. 1 z późn. zm.).

²⁴⁶ Zob. przepis nr 336.

²⁴⁷ Google np. w swojej *Polityce prywatności* informuje, że „Do zbierania i przechowywania informacji używamy różnych technologii, w tym plików cookie, tagów pikselowych, pamięci lokalnej, na przykład pamięci przeglądarki lub pamięci podręcznej aplikacji, baz danych i dzienników serwera”; zob. *Polityka prywatności*, <https://policies.google.com/privacy?hl=pl> (dostęp: 10.10.2023).

²⁴⁸ Motywy 30, 34, 66, 103, 108, art. 8 AUC.

²⁴⁹ Wyrok TS w sprawie SABAM przeciwko Netlog.

internetu, podczas gdy monitorowanie i filtrowanie dotyczy umieszczanych przez użytkowników treści (contentu, zawartości).

O ile wykładnia terminu „filtrowanie” dokonywana na gruncie dyrektywy o handlu elektronicznym (2000/31) doprowadziła sędziów Trybunału Sprawiedliwości UE do wniosku, że zastosowanie przez dostawców usług hostingu systemów filtrujących zagraża realizacji praw podstawowych, w szczególności prawa do otrzymywania i przekazywania informacji²⁵⁰, o tyle „śledzenie” przy zastosowaniu technologii cookies oraz innych technologii wykorzystywanych do przetwarzania danych osobowych stanowi praktykę, która nie narusza swobody wypowiedzi użytkowników.

Jak wynika z zakresów znaczeniowych terminów „monitorowanie”, „filtrowanie” i „śledzenie”, czynności te – co do zasady – są podejmowane w określonym celu, w szczególności w celu ustalenia albo sprawdzenia czyjś stanu lub zachowania. Monitorowanie oznacza „stałą obserwację i kontrolę jakichś procesów lub zjawisk”, a także „stały nadzór nad jakimś obiektem chronionym”²⁵¹. Monitorować to „obserwować i kontrolować pracę, przebieg lub stan czegoś za pomocą monitora”²⁵². Termin „monitoring” oznacza natomiast „systematyczne śledzenie i analizę ilościowych i jakościowych zmian pewnych

²⁵⁰ W sprawie C-360/10 Trybunał odpowiadał m.in. na pytanie: czy nakaz, który nakładałby na podmiot świadczący usługi hostingowe obowiązek wprowadzenia systemu filtrowania, wymagałby od niego prowadzenia z tego tytułu aktywnego nadzoru nad wszystkimi danymi każdego z użytkowników jego usług celem zapobieżenia wszelkim przyszłym naruszeniom praw własności intelektualnej? Odpowiedź Trybunału była pozytywna, a w konsekwencji stwierdzono, że „system filtrowania mógłby naruszać także prawa podstawowe użytkowników usług tego usługodawcy, a mianowicie ich prawo do ochrony danych osobowych oraz wolność otrzymywania i przekazywania informacji, chronione przez art. 8 i 11 Karty praw podstawowych Unii Europejskiej. Nakaz pociągałby za sobą, po pierwsze, konieczność identyfikacji, systematycznej analizy i przetwarzania informacji dotyczących profili tworzonych w sieci społecznościowej przez użytkowników tej sieci, przy czym informacje dotyczące tych profili stanowią chronione dane osobowe, jako że pozwalają co do zasady na identyfikację tych użytkowników. Po drugie, istnieje ryzyko, że omawiany nakaz naruszyłby wolność informacji, ponieważ system ten mógłby nie rozróżniać w wystarczającym stopniu treści niezgodnej z prawem i treści zgodnej z prawem, skutkiem czego jego wdrożenie mogłoby doprowadzić do blokady połączeń o treści zgodnej z prawem” (Wyrok TS w sprawie SABAM przeciwko Netlog, sentencja).

²⁵¹ Hasło: *monitorować*, [w:] *Słownik Języka Polskiego PWN*, <https://sjp.pwn.pl/slowniki/monitorowa%C4%87.html> (dostęp: 30.09.2023).

²⁵² Hasło: *monitorować*, [w:] S. Dubisz, *Uniwersalny słownik języka polskiego*, t. 2, Warszawa 2003, s. 706.

wielkości”²⁵³. Wykrywanie zmian w zachowaniu lub stanie kogoś lub czegoś następuje poprzez filtrowanie danych ze względu na przyjęte kryteria. Filtrować to „przepuszczać przez filtr”²⁵⁴, przy czym filtr w informatyce oznacza „rodzaj programu dokonującego selekcji lub prostego przekształcenia danych wejściowych”²⁵⁵.

Terminy „monitorowanie” i „filtrowanie” pozostają ze sobą w związku zarówno znaczeniowym, albowiem ich zakresy częściowo się pokrywają²⁵⁶, jak i przyczynowo-skutkowym, ponieważ filtrowanie jest zazwyczaj czynnością, którą poprzedzono monitoringiem. Monitoring jest stosowany w celu uchwycenia istniejących prawidłowości (podobieństw, powtarzalności stanów, zachowań itd.) oraz ustalenia najbardziej efektywnych kryteriów, które należy zastosować ze względu na cel filtrowania. Zarazem jednak monitorowanie może odbywać się według zdefiniowanych wcześniej kryteriów, co zbliża ten termin znaczeniowo do terminów: śledzenie i filtrowanie.

Monitorowanie, podobnie jak śledzenie, może oznaczać podążanie za kimś: „iść niepostrzeżenie za kimś, obserwować go; także: w tajemnicy zbierać o kimś informacje, zwykle po to, aby wykorzystać je przeciwko niemu”²⁵⁷. Oba terminy mogą oznaczać także: „przyglądać się, przysłuchiwać się z uwagą przebiegowi czegoś, obserwować coś uważnie przez pewien czas”²⁵⁸. Termin „monitorowanie”, ze względu na jego najszerszy zakres znaczeniowy, bywa zamiennie stosowany z pojęciami „śledzenie”, a także „filtrowanie”.

Trybunał badał, w sprawie C-70/10, *Scarlet Extended SA przeciwko Societe belgeique Des Auteurs, Compositeurs et Editeurs SCRL (SABAM)*²⁵⁹, czy filtrowanie może być zakwalifikowane jako ograniczenie praw i wolności w rozumieniu art. 52 ust. 1 Karty praw podstawowych, interpretowanego w świetle art. 8 ust. 2 i art. 10 ust. 2 EKPC²⁶⁰. Gdyby bowiem wspomniany środek

²⁵³ Hasło: *monitoring*, [w:] tamże, s. 706.

²⁵⁴ Hasło: *filtrować*, [w:] S. Dubisz, *Uniwersalny słownik języka polskiego*, t. 1, Warszawa 2003, s. 907.

²⁵⁵ Hasło: *filtrować*, [w:] tamże, s. 907.

²⁵⁶ Oba pojęcia obejmują bowiem czynności wykonywane na „danych wejściowych”.

²⁵⁷ Hasło: *śledzić*, [w:] S. Dubisz, *Uniwersalny słownik języka polskiego*, t. 3, Warszawa 2003, s. 1573.

²⁵⁸ Tamże, s. 1573.

²⁵⁹ Wyrok TS w sprawie *Scarlet Extended* przeciwko SABAM.

²⁶⁰ Trybunał rozważał, czy na dostawcę usługi dostępu do internetu, którego klienci naruszają prawa własności intelektualnej twórców treści umieszczanych w internecie,

należało zakwalifikować jako takie ograniczenie, konieczne stałoby się ustalenie, czy spełnia on poszczególne wymogi określone w tych postanowieniach²⁶¹.

należy nałożyć ogólny obowiązek filtrowania (monitorowania) i nadzoru nad umieszczanymi treściami. Stronami postępowania są SABAM (organizacja reprezentująca autorów, kompozytorów i wydawców utworów muzycznych i zarządzająca ich prawami w zakresie udzielania zezwoleń na wykorzystywanie przez podmioty trzecie ich chronionych utworów) oraz Scarlet Extended SA, dostawca usługi dostępu do internetu (ISP) dla swoich klientów, nieoferujący jednak innych usług, takich jak pobieranie lub wymiana plików. W 2004 r. SABAM zauważyła, że internauci korzystający z usług Scarlet pobierają z internetu, bez zezwolenia i bez uiszczania opłat, utwory zapisane w jej katalogu za pomocą sieci peer-to-peer, i wystąpiła przeciwko Scarlet do sądu krajowego, podnosząc, że Scarlet jako ISP znajduje się w najlepszej pozycji, aby podjąć środki w celu doprowadzenia do zaprzestania naruszeń prawa autorskiego dokonywanych przez jej klientów. Organizacja SABAM zażądała w szczególności nałożenia na Scarlet, pod groźbą okresowej kary pieniężnej, obowiązku doprowadzenia do zaprzestania tychże naruszeń poprzez uniemożliwienie lub zablokowanie wszelkich form wysyłania lub otrzymywania przez jej klientów za pośrednictwem programów peer-to-peer plików zawierających utwory muzyczne, które zostały przesłane bez zezwolenia podmiotów uprawnionych z tytułu praw autorskich. Orzeczeniem z dnia 26 listopada 2004 r. sąd krajowy stwierdził istnienie zgłoszonych przez SABAM naruszeń prawa autorskiego. Jednak przed wydaniem orzeczenia w przedmiocie wniosku o nakazanie zaprzestania naruszeń wyznaczył biegłego w celu zbadania, czy rozwiązania zaproponowane przez SABAM mogą być zrealizowane pod względem technicznym, czy możliwe jest filtrowanie wyłącznie bezprawnej wymiany plików elektronicznych i czy istnieją inne środki, za pomocą których można byłoby kontrolować używanie programów peer-to-peer oraz określać koszty rozpatrywanych środków. Zdaniem eksperta – pomimo istnienia licznych trudności technicznych – wprowadzenie filtrowania i blokady bezprawnej wymiany plików elektronicznych nie jest całkowicie wykluczone. W orzeczeniu z dnia 29 czerwca 2007 r. sąd w Brukseli orzekł, że Scarlet ma doprowadzić, pod groźbą okresowej kary pieniężnej, do zaprzestania naruszeń praw autorskich. Pytania prejudycjalne zadane w niniejszej sprawie miały na celu ustalenie, czy pozostające w związku dyrektywy 2000/31, 2001/29, 2004/48 (dyrektywa 2004/48/WE Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie egzekwowania praw własności intelektualnej) (Dz.U. UE L Nr 157, s. 45), dyrektywa 95/46 (dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. WE L Nr 281, s. 31) i 2002/58 (dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)) (Dz.U. WE L Nr 201, s. 37), interpretowane w świetle wymogów wynikających z ochrony mających zastosowanie praw podstawowych, należy rozumieć w ten sposób, że stoją one na przeszkodzie skierowanemu do ISP lub do podmiotu świadczącego usługi hostingowe, nakazowi wdrożenia systemu filtrowania (zob. M. Kręcis, *Glosa do wyroku TS z dnia 24 listopada 2011 r., C-70/10 oraz do wyroku TS z dnia 16 lutego 2012 r., C-360/10*, LEX/el. 2014).

²⁶¹ Wyrok TS w sprawie Scarlet Extended przeciwko SABAM.

Trybunał Sprawiedliwości zauważył, że filtrowanie oznacza „prowadzenia aktywnego nadzoru nad wszystkimi danymi każdego z klientów celem zapobieżenia wszelkim przyszłym naruszeniom [...]”, a w konsekwencji wymaga „przeprowadzania systematycznej analizy wszelkich treści oraz gromadzenie i identyfikację adresów IP użytkowników, od których pochodzą przesłane w sieci nielegalne treści, przy czym adresy te stanowią chronione dane osobowe, jako że pozwalają na precyzyjną identyfikację tych użytkowników”²⁶². Przeprowadzanie systematycznej analizy adresów IP nazwano w tym samym orzeczeniu „monitorowaniem”²⁶³.

W rozpoznawanej przez Trybunał sprawie dostawca internetu Scarlet Extended SA, od którego żądano wdrożenia systemu filtrowania treści w celu zapobieżenia naruszeniom praw autorskich w przyszłości oraz usunięcia dostępu do nielegalnych treści, wskazał, że „mechanizm blokowania wymagający kontroli wszystkich połączeń elektronicznych obsługiwanych za jej pośrednictwem, stanowi z samej jego natury „ograniczenie” w rozumieniu art. 10 EKPC wolności komunikowania się zagwarantowanej także w art. 11 ust. 1 Karty, niezależnie od zasad technicznych, zgodnie z którymi konkretnie przeprowadza się kontrolę połączeń, zakresu i dokładności dokonywanej kontroli oraz skuteczności i wiarygodności kontroli rzeczywiście przeprowadzanej”²⁶⁴. Ponadto wskazywano na nikłą możliwość stworzenia jednolitych zasad filtrowania. W rzeczywistości „niemożliwe jest bowiem opisanie sposobu konkretnego funkcjonowania, modus operandi, systemu filtrowania i mechanizmu blokowania, do wprowadzenia których zobowiązywałby środek, o którego zastosowanie wniesiono. Zakres wymaganego filtrowania, czyli zarówno osoby, które miałyby być kontrolowane, połączenia podlegające kontroli i intensywność kontroli, jaką należałoby przeprowadzać, jest jednocześnie bardzo ogólny i w części nieokreślony. W konsekwencji nie można określić a priori ani jego konkretnego wpływu na wymianę danych,

²⁶² Monitorowanie zachowania użytkowników internetu oraz w konsekwencji gromadzenie ich adresów IP klóci się z prawem do poszanowania ich życia prywatnego i korespondencji (zob. Wyrok TS w sprawie Scarlet Extended przeciwko SABAM, sentencja).

²⁶³ Pojęcia „monitorowanie” użył Europejski Inspektor Ochrony Danych Osobowych, który wskazała, że „monitorowanie zachowania użytkowników Internetu oraz w konsekwencji gromadzenie ich adresów IP klóci się z prawem do poszanowania ich życia prywatnego i korespondencji” (Wyrok TS w sprawie Scarlet Extended przeciwko SABAM, pkt 76).

²⁶⁴ Tamże, pkt 85.

ani jego ogólnego kosztu ekonomicznego, w szczególności kosztu instalacji i utrzymania”²⁶⁵. Zasygnalizowano ponadto, że nałożenie na Scarlet obowiązku filtrowania stanowiłoby *de facto* przeniesienie odpowiedzialności za walkę z piractwem internetowym na prywatny podmiot (pkt 54 wyroku).

Trybunał podzielił większość wątpliwości zgłoszonych przez Scarlett SA i wskazał, że nakaz „ustanowienia systemu filtrowania pociągałby za sobą konieczność przeprowadzania systematycznej analizy wszelkich treści oraz gromadzenie i identyfikację adresów IP użytkowników, od których pochodzą przesłane w sieci nielegalne treści, przy czym adresy te stanowią chronione dane osobowe, jako że pozwalają na precyzyjną identyfikację tych użytkowników” (pkt 51). Po drugie, istnieje ryzyko, że omawiany nakaz naruszyłby wolność informacji, ponieważ system ten mógłby nie rozróżniać w wystarczającym stopniu niezgodnej z prawem treści i zgodnej z prawem treści, skutkiem czego jego wdrożenie mogłoby doprowadzić do blokady połączeń o treści zgodnej z prawem. W konsekwencji Trybunał uznał, że wydając nakaz zobowiązujący pośredników internetowych do wdrożenia spornego systemu filtrowania, sąd krajowy nie spełniłby wymogu zapewnienia odpowiedniej równowagi między z jednej strony prawem własności intelektualnej, a z drugiej strony wolnością prowadzenia działalności gospodarczej, prawem do ochrony danych osobowych oraz wolnością otrzymywania i przekazywania informacji (pkt 52).

Wskazane powyżej stanowisko Trybunału pozostaje aktualne także na gruncie rozporządzeń cyfrowych w zakresie, w jakim sformułowano w wyroku zasadę, zgodnie z którą pośredników internetowych nie można obejmować ogólnym obowiązkiem (nakazem) monitorowania treści. Zgodnie z art. 8 AUC „Na dostawców usług pośrednich nie nakłada się ogólnego obowiązku monitorowania informacji, które dostawcy ci przekazują lub przechowują, ani aktywnego ustalania faktów lub okoliczności wskazujących na nielegalną działalność”. Zarazem jednak ustawodawca europejski zmodyfikował swoje stanowisko w ten sposób, że uznał monitorowanie (filtrowanie) za dozwoloną praktykę i nie zabronił jej stosowania, a wobec tego – jak należy wnioskować – stwierdził, że monitorowanie (filtrowanie, śledzenie) nie narusza wolności wypowiedzi w stopniu nieproporcjonalnym. W takim zakresie,

²⁶⁵ Tamże, pkt 52.

w jakim ustawodawca europejski uznaje monitorowanie za praktykę, która nie zakłóca korzystania z wolności wypowiedzi, stanowisko to różni się od wcześniej zajmowanego i potwierdzonego spójną linią orzeczniczą zarówno ETPC, jak i ETS.

Brzmienie art. 7 AUC dowodzi, że monitorowanie jest praktyką legalną, a nadto, praktyka ta nie stoi w sprzeczności z zasadą neutralności i nie pozbawia pośredników internetowych możliwości powoływania się na zawarte w art. 4–6 AUC kontratypy. Zgodnie z art. 7 AUC (klauszula dobrego samarytanina):

Dostawców usług pośrednich nie można uznać za nieuprawnionych do skorzystania z wyłączeń odpowiedzialności, o których mowa w art. 4, 5 i 6, tylko z tego powodu, że w dobrej wierze i z należytą starannością prowadzą z własnej inicjatywy dobrowolne czynności sprawdzające lub podejmują inne środki mające na celu wykrycie, identyfikację i usunięcie nielegalnych treści lub uniemożliwienie do nich dostępu lub podejmują niezbędne środki, aby spełnić wymogi prawa Unii i prawa krajowego zgodnego z prawem Unii, w tym wymogi określone w niniejszym rozporządzeniu.

W art. 7 AUC zawarte zostało domniemanie zgodności z prawem działania pośredników, którzy „w dobrej wierze i z należytą starannością prowadzą z własnej inicjatywy dobrowolne czynności sprawdzające lub podejmują inne środki mające na celu wykrycie, identyfikację i usunięcie nielegalnych treści lub uniemożliwienie do nich dostępu lub podejmują niezbędne środki, aby spełnić wymogi prawa Unii i prawa krajowego zgodnego z prawem Unii, w tym wymogi określone w niniejszym rozporządzeniu”. Podejmowanie „czynności sprawdzających” może obejmować monitorowanie, śledzenie i filtrowanie. Czynności sprawdzające mogą być zarówno rezultatem ustaleń z wcześniej prowadzonego monitoringu, jak i podstawą do zlecenia monitoringu. Monitorowanie aktywności użytkowników internetu może więc stanowić środek podjęty w następstwie uzyskanego przez pośrednika na podstawie art. 16 AUC zgłoszenia, ale też może być metodą wykrywczą stosowaną przez pośredników w ramach „dobrowolnych czynności sprawdzających” (art. 7 AUC). Wyrażenie: „podejmowanie środków” użyte w art. 7 AUC obejmuje – co do zasady – każdą czynność, w tym także monitorowanie, o ile czynność

ta miała na „celu wykrycie, identyfikację i usunięcie nielegalnych treści lub uniemożliwienie do nich dostępu”.

Zawarte w art. 8 AUC zabronienie nakładania na pośredników internetowych ogólnego obowiązku monitorowania interpretowane w łączności z art. 7, zawierającym domniemanie zgodności z prawem działania pośredników, którzy „w dobrej wierze i z należytą starannością prowadzą z własnej inicjatywy dobrowolne czynności sprawdzające”, potwierdza, że monitorowanie nie jest nakazane, ale – jak należy interpretować te przepisy – stanowi dobrą praktykę pośredników, a w konsekwencji jej stosowanie zapewnia, że pośrednik dochowuje wymogów należytej staranności wymaganej ze względu na treść obowiązków wymienionych w III rozdziale AUC. Ze względu na odesłanie do „dobrowolnych czynności sprawdzających”, zawarte w art. 7 AUC oraz zalegalizowanie w tym przepisie dopuszczalności stosowania przez pośredników także „innych środków mających na celu wykrycie, identyfikację i usunięcie nielegalnych treści”, zasadne wydaje się stanowisko, zgodnie z którym art. 7 AUC stanowi podstawę legalizującą czynności monitorowania treści.

Monitorowanie aktywności użytkowników internetu może być także prowadzone z powołaniem na inne podstawy prawne legalizujące te czynności. Chcąc usprawiedliwić ingerencję w sferę praw i wolności użytkownika, pośrednicy mogą zatem także wskazywać na postanowienia zawarte w rozdziale IIII AUC normującym obowiązek dochowania należytej staranności, a w konsekwencji uzasadniać, że wykonywanie czynności monitorowania następuje w celu dochowania wymaganego poziomu staranności. Ponadto nie jest wykluczone, że monitorowanie stanowi praktykę przewidzianą przez pośrednika w obowiązującym u niego regulaminie, co w efekcie pozwala pośrednikom internetowym powoływać się na klauzule umowne (warunki korzystania z usług) jako podstawę ingerencji w wolność wypowiedzi odbiorców usług.

Aktywność odbiorców usług może być monitorowana z powodu chęci uwolnienia się pośrednika od odpowiedzialności (chodzi także o uniknięcie przez pośrednika kary finansowej, którą Komisja Europejska może nałożyć na podstawie art. 74 lub art. 76 AUC²⁶⁶) poprzez wykazanie, że przy

²⁶⁶ Komisja może w drodze decyzji nałożyć na danego dostawcę bardzo dużej platformy internetowej lub bardzo dużej wyszukiwarki internetowej grzywny, których wysokość nie może przekraczać 6% jego łącznego światowego rocznego obrotu uzyskanego w poprzednim roku obrotowym, jeżeli Komisja stwierdzi, że dostawca ten umyślnie lub

zwalczaniu nielegalnych treści działań z należytą starannością, oraz z powodu ustanowienia przez pośredników internetowych na własne potrzeby i w celu realizacji własnych interesów regulaminów korzystania z usług określających w szczególności zasady monitorowania (filtrowania).

Obowiązki i zadania nałożone na pośredników internetowych zostały opisane w rozdziale IIII AUC zatytułowanym: *Obowiązki w zakresie należytej staranności na potrzeby przejrzystego i bezpiecznego środowiska internetowego*. Tytuł rozdziału wskazuje, że wymienione w nim obowiązki konstruują wymagany od pośredników standard starannego działania. Pogrupowano je w 6 sekcji, systematyzując w ten sposób, że w pierwszej sekcji wskazane zostały obowiązki adresowane do najszerzej grupy adresatów, tj. wszystkich pośredników internetowych niezależnie od rodzaju świadczonej usługi, jej zakresu oraz niezależnie od potencjału i wpływu pośrednika na wewnętrzny rynek usług. Kolejne sekcje zawierają obowiązki adresowane do coraz węższej grupy pośredników wyodrębnianej albo ze względu na rodzaj usługi (platformy internetowe), albo na zakres wpływu pośrednika i jego potencjał (bardzo duże platformy internetowe i bardzo duże wyszukiwarki internetowe)²⁶⁷.

w wyniku zaniebdania: a) narusza odpowiednie przepisy niniejszego rozporządzenia; b) nie zastosował się do decyzji zarządzającej środki tymczasowe, wydanej na podstawie art. 70; lub nie wykonał zobowiązania, które uznano za wiążące w drodze decyzji na podstawie art. 71 (art. 74 ust. 1 AUC). Komisja może także przyjąć decyzję o nałożeniu odpowiednio na danego dostawcę bardzo dużej platformy internetowej lub bardzo dużej wyszukiwarki internetowej lub inną osobę, o której mowa w art. 67 ust. 1, okresowych kar pieniężnych, których dzienna wysokość nie może przekraczać 5% średniego dziennego dochodu lub światowego rocznego obrotu uzyskanego w poprzednim roku obrotowym, i które są naliczane od daty ustalonej w decyzji, w celu zmuszenia takich podmiotów do: a) dostarczenia prawidłowych i kompletnych informacji w odpowiedzi na decyzję, w której zażądano udzielenia informacji zgodnie z art. 67; b) poddania się kontroli zarządzanej decyzją Komisji przyjętą na podstawie art. 69; c) zastosowania się do decyzji zarządzającej środki tymczasowe, wydanej na podstawie art. 70 ust. 1; d) wykonania zobowiązań, które uczyniono prawnie wiążącymi w drodze decyzji wydanej na podstawie art. 71 ust. 1; e) zastosowania się do decyzji wydanej na podstawie art. 73 ust. 1, w tym, w stosownych przypadkach, do zawartych w niej wymogów dotyczących planu działania, o którym mowa w art. 75 (art. 76 ust. 1 AUC).

²⁶⁷ Kolejne sekcje zawarte w rozdziale III AUC zostały zatytułowane: 1) Obowiązki mające zastosowanie do wszystkich dostawców usług pośrednich; 2) Dodatkowe przepisy mające zastosowanie do dostawców usług hostingu, w tym platform internetowych; 3) Dodatkowe przepisy mające zastosowanie do platform internetowych; 4) Dodatkowe przepisy dotyczące dostawców platform internetowych umożliwiających konsumentom zawieranie z przedsiębiorcami umów zawieranych na odległość; 5) Dodatkowe obowiązki

Adresowane do pośredników przepisy mają mieszany, uprawniający-zobowiązujący charakter. O ile nakładają na pośredników ogólny obowiązek starannego działania, o tyle poszczególne, zawarte w rozdziale III AUC, przepisy nie tyle nakładają na pośredników obowiązki, co raczej – jak się wydaje – kreują na ich rzecz upoważnienia do działania, legalizując ingerencję w prawa i wolności odbiorców usług, w tym w wolność wypowiedzi.

Monitorowanie, na co wskazuje literalna wykładnia art. 8 AUC, może być wykonywane nie tylko w odniesieniu do treści udostępnianych przez użytkowników internetu, ale także w odniesieniu do ich aktywności podejmowanej poza internetem, w tym niezwiązanej bezpośrednio z umieszczanymi treściami²⁶⁸. Monitorowanie odbywa się zazwyczaj po uprzednim poinformowaniu użytkownika, jednakże zazwyczaj informowanie to jest nieefektywne w tym znaczeniu, że użytkownicy pomimo formalnie przekazanej im informacji o stosowanych wobec nich praktykach nie mają świadomości ich skutków i zwykle nie wiedzą, na czym one polegają²⁶⁹. Pośrednicy

spoczywające na dostawcach bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych w zakresie zarządzania ryzykiem systemowym; 6) Inne przepisy dotyczące obowiązków w zakresie należytej staranności.

²⁶⁸ Organizacja Panoptikon przeanalizowała, w jakich obszarach aktywności użytkowników pośrednicy internetowi śledzą przekazywane przez nich treści. Zwrócono uwagę, że dostawcy usług cyfrowych, w tym także dostawcy treści cyfrowych, monitorują aktywność użytkowników, która nie tylko nie jest powiązana ze świadczoną przez dostawców usługą, ale także wówczas, gdy śledzenie dotyczy danych wrażliwych. Wskazano np., że Facebook automatycznie uruchamia mikrofon co jakiś czas, aby wykryć, jakie programy użytkownik ogląda w telewizji i czy np. wycisza telewizor na czas przerwy reklamowej; Facebook wykorzystuje także system, który na podstawie zdjęć i ich opisów oraz wspólnych numerów IP i identyfikatorów urządzeń pomaga ustalić, z kim użytkownicy dzielą gospodarstwo domowe; Offline Trajectories – technologia, która ma przewidywać przyszłe lokalizacje użytkowników. Google Arts & Culture, Art Selfie natomiast, pomimo że podaje jako cel: użytkownik robi sobie selfie, a sztuczna inteligencja Google'a porównuje zdjęcie do dzieł sztuki, to zasadniczym celem zbierania i monitorowania aktywności użytkowników jest trenowanie sztucznej inteligencji; zob. K. Szymielewicz, K. Iwańska, *Śledzenie i profilowanie sieci*, Fundacja Panoptikon 2019, s. 10–11, https://panoptikon.org/sites/default/files/publikacje/panoptikon_raport_o sledzeniu_final.pdf (dostęp: 30.09.2023).

²⁶⁹ W raporcie opracowanym przez Panoptikon wskazano, że przeciętny użytkownik smartfona korzysta aktywnie z około 27 aplikacji miesięcznie. Tylko nieliczni inwestują czas i uwagę w zapoznanie się z ich regulaminami i politykami prywatności. Badanie przeprowadzone przez naukowców z Carnegie Mellon University wykazało, że przeciętna polityka prywatności liczy aż 2518 słów, a jej przeczytanie zajmuje ok. 10 minut. Autorzy raportu *Appfail Report* wskazują, że polityki prywatności najpopularniejszych aplikacji

internetowi, a także pozostali dostawcy usług społeczeństwa informacyjnego, uzyskują zgodę użytkowników na ich śledzenie i monitorowanie, wykorzystując do uzyskania akceptacji użytkownika „wredne praktyki” (ang. *dark patterns*). Stanowią one:

elementy interfejsów w aplikacjach i serwisach internetowych zaprojektowane tak, by skłonić użytkownika do wybrania opcji najkorzystniejszej dla firmy zarabiającej na komercjalizacji danych. Kolory, rozmieszczenie przycisków i sposób wyświetlania komunikatów mają doprowadzić do tego, że użytkownik (niekoniecznie świadomie) „zgodzi się” na głęboką ingerencję w prywatność (np. ciągle śledzenie lokalizacji czy dopuszczenie skryptów śledzących obsługiwanych przez podmioty trzecie)²⁷⁰.

Zarazem w praktyce nad raz rozpowszechnionymi na giełdzie danymi nie ma jakiegokolwiek kontroli – ani ze strony firmy, która wysłała dane na giełdę, ani tym bardziej ze strony samego użytkownika²⁷¹.

Stosowane przez pośredników internetowych praktyki polegające na gromadzeniu danych o użytkownikach i monitorowaniu ich aktywności służą przede wszystkim osiągnięciu przez pośredników celów komercyjnych. Zasady i zakres monitorowania w ramach – jak założono w art. 7 AUC – „dobrowolnych czynności sprawdzających” pośrednicy ustalili w obowiązujących u nich regulaminach i politykach. Nie jest zasadniczym celem monitorowania realizowanego przez pośredników na podstawie obowiązujących u nich regulaminów zwalczanie nielegalnych treści. Cel ten może być realizowany równolegle, tj. przy wykorzystaniu wiedzy pozyskanej przez pośredników w związku z monitorowaniem. Niewątpliwie pośrednicy internetowi byli mocno zainteresowani zalegalizowaniem stosowanych u nich praktyk

są nie tylko długie, lecz także często nieczytelne i niezrozumiałe dla potencjalnego użytkownika; zob. tamże.

²⁷⁰ Najczęściej stosowane *dark patterns* to: 1) niekorzystne dla użytkowników ustawienia domyślne; 2) wydłużona ścieżka zmiany ustawień dla tych, którzy chcą zadbać o swoją prywatność; 3) wyskakujące okienka z ustawieniami prywatności, w których kluczowe informacje zostały pominięte lub przedstawione w mylący sposób; 4) grożenie utratą ważnych funkcjonalności lub usunięciem konta, jeśli użytkownik nie zgodzi się na przekazanie dodatkowych danych; 5) interpretowanie nierzadko przypadkowych akcji (np. nieznacznego ruchu myszką) na korzyść aplikacji/serwisu (tamże, s. 7–8).

²⁷¹ Tamże, s. 21.

polegających na śledzeniu, monitorowaniu i filtrowaniu, co jest faktem notoryjnym. Na gruncie rozporządzeń cyfrowych praktyki te, zgodnie z oczekiwaniami pośredników, zostały zalegalizowane.

Zawarte w art. 7 i 8 AUC postanowienia są obopólnie korzystne. Korzyść pośredników polega na tym, że formalnie potwierdzono legalność stosowanych przez nich praktyk polegających na filtrowaniu, monitorowaniu i śledzeniu użytkowników, także w celach komercyjnych, a ponadto udzielono pośrednikom swobody w zakresie regulowania powyższych praktyk w treści ustalanych przez pośredników, *de facto* jednostronnie (w formie wzorca umownego), wewnętrznych regulaminów i polityk. Ustawodawca europejski co prawda dostrzegł zagrożenie płynące z zastosowanej konstrukcji regulacyjnej, która przenosi na pośredników część zadań ze sfery publicznej, jak w szczególności zwalczanie nielegalnych treści, oraz wyposaża ich w upoważnienia do działania w tym zakresie, a nadto potwierdza równoważność przyjmowanych przez pośredników wewnętrznych regulaminów z treścią obowiązków wynikających z aktów ustawodawczych, jednakże stanął zarazem na stanowisku, że ze względu na ochronę wartości, jaką stanowi swoboda działalności gospodarczej, ingerencja w treść „warunków korzystania z usług” byłaby niedopuszczalna²⁷².

O ile zatem pośrednicy internetowi stali się adresatami obowiązków ustanowionych w celu „zapewnienia przejrzystości, ochrony odbiorców usługi oraz unikania nieuczciwych lub arbitralnych wyników” (motyw 40 AUC) oraz realizacji bardziej jeszcze ogólnego celu, tj. „zapewnienia bezpiecznego, przewidywalnego i godnego zaufania środowiska internetowego oraz dla umożliwienia obywatelom Unii i innym osobom korzystania z przysługujących im

²⁷² W motywie 45 AUC wskazano, że „choć zasadniczo należy przestrzegać swobody umów przysługującej dostawcom usług pośrednich, należy ustanowić pewne zasady dotyczące treści, stosowania i egzekwowania warunków korzystania z usług tych dostawców w celu zapewnienia przejrzystości, ochrony odbiorców usługi oraz unikania nieuczciwych lub arbitralnych wyników. Dostawcy usług pośrednich w warunkach korzystania z ich usług powinni wyraźnie podawać i aktualizować informacje o powodach, dla których mogą ograniczyć świadczenie swoich usług. Warunki te powinny w szczególności zawierać informacje na temat wszelkich polityk, procedur, środków i narzędzi wykorzystywanych do celów moderowania treści, w tym algorytmicznego podejmowania decyzji i weryfikacji przez człowieka, a także na temat regulaminu wewnętrznego systemu rozpatrywania skarg. Powinny one również zawierać łatwo dostępne informacje na temat prawa do zakończenia korzystania z usług [...]”.

praw podstawowych zagwarantowanych w Karcie praw podstawowych Unii Europejskiej, których przestrzeganie ma zapewnić” (motyw 3 AUC), o tyle określone w AUC i ARC ramy prowadzonej przez nich działalności nie naruszają ich interesów. Przeciwnie, przyjęte w ARC i AUC rozwiązania sprzyjają rozwojowi ich potencjału, co potwierdzono w treści wniosku KE do PE o przyjęcie rozporządzenia o rynkach cyfrowych (ARC). We wniosku wskazano, że:

celem niniejszego wniosku jest zatem umożliwienie platformom wykorzystania ich pełnego potencjału dzięki rozwiązaniu na szczeblu UE problemu najpoważniejszych przypadków nieuczciwych praktyk i słabej kontestowalności, aby zarówno użytkownicy końcowi, jak i użytkownicy biznesowi mogli czerpać w pełni korzyści wynikające z gospodarki platform oraz gospodarki cyfrowej w ujęciu ogólnym, w kontestowalnym i uczciwym środowisku²⁷³.

Korzyść prawodawcy europejskiego wynikająca z przyjętej w AUC i ARC konstrukcji prawnej legitymizującej filtrowanie, śledzenie i monitorowanie w internecie polega na usystematyzowaniu – na płaszczyźnie ekonomicznej – reguł gry rynkowej na jednolitym rynku wewnętrznym usług cyfrowych, natomiast – na płaszczyźnie politycznej – na uzyskaniu realnego wpływu na charakter i zakres rozpowszechnianych w internecie treści, a w konsekwencji możliwość kształtowania postaw i opinii, w szczególności poprzez definiowanie terminu „nielegalne treści” oraz zarządzanie intensywnością ich zwalczania.

Powyżej wskazane spostrzeżenia potwierdzają, że na płaszczyźnie regulacji normatywnych nastąpiła zmiana paradygmatu wolności wypowiedzi oraz, w rezultacie, zmiana jego standardu. Ustawodawca europejski legitymizując praktyki pośredników internetowych dotyczące filtrowania, monitorowania i śledzenia, legalizuje ingerencję w prawa podstawowe użytkowników internetu, a w szczególności w prawo do prywatności (art. 7 KPP i art. 8 EKPC), prawo do ochrony danych osobowych (art. 8 KPP) oraz wolność wypowiedzi. (art. 11 KPP i art. 10 EKPC).

²⁷³ Wniosek z dnia 15 grudnia 2020 r. rozporządzenie Parlamentu Europejskiego i Rady w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym (akt o rynkach cyfrowych), pkt I, 1 <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020PC0842>.

Zastosowane w AUC i ARC konstrukcje prawne, które za pomocą domniemań prawnych (art. 7 AUC), odesłań do aktów nienormatywnych takich jak regulaminy i polityki obowiązujące u pośredników internetowych oraz poprzez zmianę kontratypu polegającą na zastąpieniu obowiązku zachowania neutralności (art. 4 6 AUC) obowiązkiem należytej staranności (rozdział III AUC art. 11–32 AUC), modyfikują model ochrony wolności wypowiedzi i rangę tej wolności w hierarchii wartości prawnie chronionych. Jeśli zatem ustawodawca formalnie nie zakwestionował wagi i znaczenia wolności wypowiedzi jako wartości prawnie chronionej ani rangi tej wolności, to jednak poszerzył katalog przesłanek legalizujących ingerencję w wolność wypowiedzi, zaliczając do nich potrzebę zwalczania nielegalnych treści, a nadto upoważnił podmioty prywatne do stosowania środków ochrony prewencyjnej takich jak w szczególności śledzenie, filtrowanie i monitorowanie treści. Zmiana paradygmatu ochrony wolności wypowiedzi polega – w ogólnym ujęciu – na zastąpieniu ujęcia wolnościowego²⁷⁴, ujmującego wolność wypowiedzi jako jedno z podstawowych praw człowieka, którego realizacja nie wymaga udzielenia upoważnienia ze strony państwa, koncepcją prawnopozytywną, która zakłada, że państwo posiada obowiązki pozytywne w odniesieniu do wolności wypowiedzi, a w konsekwencji, że zakres wolności wypowiedzi podlega regulowaniu przez państwo.

²⁷⁴ K. Wojtyczek zauważa, że w przypadku praw wolnościowych do prawodawcy należy przede wszystkim określenie sfery zachowań jednostki poddanej pod ochronę konstytucyjną. Posługuje się on w tym przypadku formułą typu: „Każdemu zapewnia się wolność wyrażania swoich poglądów” (art. 54 Konstytucji RP). Obowiązek ciążyący na organach państwowych oraz innych podmiotach zostaje w tym przypadku określony w sposób dorozumiany. Jest to po pierwsze zakaz przeszkadzania jednostce w podejmowaniu lub niepodjęmowaniu zachowań mieszczących się w danej sferze [...]. Po drugie, jest to nakaz ustanowienia ustawy, która skonkretyzuje ogólny zakaz ingerencji w stosunku do innych jednostek oraz zapewni jednostce odpowiednie środki prawne na wypadek bezprawnej ingerencji ze strony państwa oraz innych podmiotów; zob. K. Wojtyczek, *Granice ingerencji ustawodawczej w sferę praw człowieka w Konstytucji RP*, Kraków 1999, s. 49–50.

C. Systemy rekomendacji

„System rekomendacji” oznacza w pełni lub częściowo zautomatyzowany system wykorzystywany przez platformę internetową w celu sugerowania odbiorcom usługi w jej interfejsie internetowym konkretnych informacji i ich szeregowanie, w tym na skutek wyszukiwania dokonanego przez odbiorcę usługi lub w inny sposób determinującego względną kolejność lub eksponowanie pokazywanych informacji (art. 3 lit. s AUC). Rezultatem stosowanych systemów rekomendacji jest wyświetlanie użytkownikom informacji we „względnej kolejności” (art. 27 ust. 3 AUC), a zatem w kolejności odmiennej dla każdego z odbiorców usługi w zależności od wytworzonego przez dostawcę usługi „profilu” odbiorcy²⁷⁵. Profilowanie stanowi dozwoloną technikę przetwarzania danych osobowych wykorzystywaną przez dostawców usług cyfrowych²⁷⁶ posiadających status administratorów danych osobowych

²⁷⁵ Google np. zbiera co najmniej następujące dane: wyszukiwane hasła, oglądane filmy, wyświetlenia reklam i treści oraz interakcja z nimi, informacje związane z głosem i dźwiękiem, zakupy, osoby, z którymi się kontaktujesz lub którym udostępniasz materiały, aktywność w witrynach i aplikacjach innych firm, które korzystają z naszych usług; historię przeglądania w Chrome synchronizowaną z kontem Google, a także dane z dziennika połączeń telefonicznych i wiadomości, numer telefonu, numer osoby dzwoniącej, numer rozmówcy, do którego dzwonisz, numery przekierowania, adresy e-mail nadawcy i odbiorcy, daty i godziny połączeń i wiadomości, czasy trwania rozmów, ustawienia przesyłania oraz liczbę i typy połączeń i wiadomości oraz informacje z GPS i inne dane z czujników urządzenia wyposażonego w GPS, adres IP, aktywność w usługach Google, np. wyszukiwania i miejsca oznaczone jako dom lub praca, informacji o rzeczach w pobliżu urządzenia, np. punktów dostępu do sieci Wi-Fi, stacji bazowych sieci komórkowych i urządzeń z włączoną obsługą Bluetooth; zob. *Polityka prywatności Google*, <https://policies.google.com/privacy?hl=pl> (dostęp: 2.09.2023).

²⁷⁶ D. Bieńkowski zauważa, że pierwszą metodą zbierania informacji o użytkowniku jest profilowanie aktywne, inaczej jawne (ang. *explicit profile*). Sposób ten opiera się na informacjach uzyskanych bezpośrednio od użytkownika, które są następnie przechowywane w jego profilu i wykorzystywane przez mechanizmy rekomendacji. Przykładem takiego wydobywania wiedzy jest ankietowanie, gdzie użytkujący serwis udziela odpowiedzi na pytania, które są przetwarzane tak, aby można było je zapisać w pewnym wektorze cech użytkownika. Obecnie taki sposób nie spotyka się z uznaniem internautów, gdyż uważany jest za irytujący, przez co ankiety są niechętnie wypełniane. Najczęściej stosowane jest obecnie profilowanie pasywne, inaczej domniemane (ang. *implicit profile*). W podejściu pasywnym zbieraniem informacji zajmuje się system, który obserwuje działania i weryfikuje wzorce zachowań użytkownika, a następnie udoskonala i aktualizuje jego profil. Serwisy korzystające z takiego podejścia nie bazują na opinii użytkownika ani nie oczekują udzielania odpowiedzi na zadawane pytania czy samodzielnego

(ADO). Status ADO został zdefiniowany w ogólnym rozporządzeniu o ochronie danych osobowych (RODO²⁷⁷). Zgodnie z art. 4 pkt 7 RODO administratorem może być „każda osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych”. Pośrednicy internetowi mają status ADO. Ciążą zatem na nich obowiązki wskazane w RODO. Zastosowany w RODO mechanizm legalizowania przetwarzania danych osobowych (art. 6 ust. 1 RODO) pozwolił ADO, w szczególności korzystającym z systemów zautomatyzowanego przetwarzania danych osobowych, a zatem także pośrednikom internetowym, na przetwarzanie danych użytkowników internetu (odbiorców usług) bez uzyskiwania ich zgody. Zgoda podmiotu danych osobowych jest jedną z sześciu równoważnych przesłanek wskazanych w art. 6 ust. 1 RODO legalizujących przetwarzanie danych osobowych. Dopuszczalne jest zatem przetwarzanie danych użytkowników internetu także wówczas, gdy „przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią” (art. 6 ust. 1 lit. f RODO), a także wtedy, gdy „przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy” (art. 6 ust. 1 lit. b RODO)²⁷⁸. ADO, który czerpie upoważnienie do przetwarzania danych osobowych, powołując jako podstawę

dostarczania informacji. Skupiają się na analizie czasu, który jest poświęcany na czytanie o danym produkcie oraz na analizie cech przedmiotów, które są najczęściej oglądane; zob. D. Bienkowski, *Mechanizmy zaawansowanych rekomendacji w systemach portali internetowych*, *Praca inżynierska*, Politechnika Warszawska 2012, s. 16, <https://repo.pw.edu.pl/docstore/download/WUT307327/Praca+inzynierska+-+Daniel+Bienkowski.pdf> (dostęp: 10.10.2023).

²⁷⁷ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. UE L Nr 119, s. 1 z późn. zm.).

²⁷⁸ Przykładowo Google przetwarza dane osobowe, w tym profiluje użytkowników, co do zasady, z powołaniem na przesłankę z art. 6 ust. 1 lit. b i f. Google powołuje się na art. 6 ust. 1 lit. b, kiedy wskazuje, że „Przetwarzamy niektóre dane, aby dostarczyć Ci usługę zgodnie z umową. Gdy na przykład kupujesz dodatkowe miejsce na Dysku Google, musimy przetwarzać informacje o Twojej formie płatności”; zob. *Polityka prywatności Google*, <https://policies.google.com/privacy?hl=pl#europeanrequirements> (dostęp: 2.09.2023).

jedną ze wskazanych w art. 6 ust. 1 RODO okoliczności, może powierzyć²⁷⁹ innym podmiotom (tzw. zaufane podmioty; zaufani partnerzy) dalsze przetwarzanie danych osobowych zgodnie ze wskazanym przez ADO celem²⁸⁰.

Profilowanie różni się od pozostałych operacji przetwarzania danych osobowych celem ich przetwarzania. Profilowanie²⁸¹ służy stworzeniu sylwetki użytkownika (podmiotu danych) będącego odbiorcą usługi dostarczanej przez dostawców usług cyfrowych, w szczególności pośredników internetowych, przy czym przy tworzeniu sylwetki (profilu) uwzględnione zostają tylko te cechy, zachowania i preferencje użytkownika, które są istotne z punktu widzenia interesu usługodawcy²⁸². Profil stanowi zatem jakiś wycinek wiedzy

²⁷⁹ Możliwość powierzenia przez ADO innemu podmiotowi danych osobowych w celu dalszego ich przetwarzania zgodnie ze wskazanym przez ADO celem wynika wprost z art. 28 RODO. Przetwarzanie danych następuje na podstawie pisemnego powierzenia danych innemu podmiotowi, w tym tzw. zaufanemu partnerowi. Zgodnie z art. 28 ust. 3 RODO Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiąże podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

²⁸⁰ Google przyznaje, że powierza dane osobowe milionom firm i organizacji, które Google zalicza do tzw. zaufanych partnerów. Google przyznaje, że we współpracy z Google reklamy wyświetla ponad 2 mln witryn, a podmioty posiadające tytuł prawny do tych witryn Google traktuje jako zaufanych partnerów. Kolejne miliony podmiotów, to współpracujących z Google programiści i firmy zapewniające bezpieczeństwo usług; zob. *Kim są partnerzy Google?*, <https://policies.google.com/privacy/google-partners?hl=pl> (dostęp: 2.09.2023). Google nie udostępnia jednak listy „zaufanych partnerów” („zaufanych firm”).

²⁸¹ Zgodnie z art. 4 pkt 4 RODO profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

²⁸² Do tworzenia profilu wykorzystywane mogą być także dane wrażliwe, co szczególnie ingeruje w prawa i wolności odbiorcy. Ryzyko naruszenia praw lub wolności osób, o różnym prawdopodobieństwie i wadze, może wynikać z przetwarzania danych osobowych mogącego prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, w szczególności: jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi; jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i czynów zabronionych lub związanych z tym środków bezpieczeństwa; jeżeli oceniane

o użytkowniku i jego preferencjach (profil zakupowy, profil społeczny, profil sprzedażowy²⁸³). Pośrednicy internetowi wykorzystują tę wiedzę do budowania systemu rekomendacji²⁸⁴. Termin „rekomendacja” jest w AUC stosowany zamiennie z terminem „sugerowanie”. W art. 27 ust. 2 AUC zatytułowanym: *Przejrzystość systemu rekomendacji* zobowiązano pośredników do wyjaśniania użytkownikom „dlaczego niektóre informacje są sugerowane użytkownikom”, przy czym „wyjaśnienie” powinno zawierać wskazanie co najmniej: 1) kryteriów, które są najistotniejsze przy określaniu informacji sugerowanych odbiorcy usługi, a także 2) powodów względnego znaczenia tych parametrów. „System rekomendacji” oznacza w pełni lub częściowo zautomatyzowany system wykorzystywany przez platformę internetową w celu sugerowania odbiorcom usługi w jej interfejsie internetowym konkretnych informacji i ich szeregowanie, w tym na skutek wyszukiwania dokonanego przez odbiorcę usługi lub w inny sposób determinującego względną kolejność lub eksponowanie pokazanych informacji (art. 3 pkt s AUC).

Zważywszy, że wolność wypowiedzi jest realizowana nie tylko na płaszczyźnie przekazywania (dostarczania) informacji, ale także na płaszczyźnie uzyskiwania dostępu do informacji, należy wskazać, że stosowane przez pośredników internetowych systemy rekomendacji istotnie ingerują w prawo użytkowników do otrzymywania neutralnej, jednakowej, nie-dyskryminującej i tożsamej pod względem jakościowym oraz ilościowym informacji. Stosowanie systemów rekomendacji powoduje, że ze względu

są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się lub jeżeli przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci; jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą (motyw 75 RODO).

²⁸³ Tworzenie profilu klienta stało się jednym z narzędzi biznesowych. Podmioty zajmujące się marketingiem internetowym oferują pomoc w tworzeniu profili klientów dla branży sieciowej. Wskazuje się na możliwość stworzenia, na podstawie danych dotyczących preferencji i zachowań w internecie, nawet 10 tys. profili behawioralnych klientów; zob. *Buduj profile odbiorców wykorzystując dane behawioralne*, DMSales, <https://dmsales.com/budowanie-profilu-odbiorcow/> (dostęp: 10.10.2023).

²⁸⁴ D. Bieńkowski wskazuje, że systemy rekomendacji projektowane są tak, aby mierzyć się z problemem wyszukania przedmiotów o jak największej wartości funkcji przydatności każdemu z użytkowników w jak najkrótszym czasie; zob. D. Bieńkowski, *Mechanizmy...*, s. 18.

na osobiste cechy lub preferencje użytkowników uzyskują oni dostęp do odmiennych zasobów (pakietów) informacji. W środowisku cyfrowym termin „wypowiedź”, podobnie jak poza internetem, może być rozumiany bardzo szeroko. Obejmuje on nie tylko treści werbalne, lecz także wszelkie inne reakcje będące nośnikami treści, w szczególności znaki, gesty, dźwięki i symbole²⁸⁵. Wypracowana na gruncie ETPC koncepcja szerokiej interpretacji terminu „wypowiedź” nadal zachowuje aktualność, także w internecie. Jeśli zatem za wypowiedź przyjąć zachowanie się użytkownika w internecie, w szczególności rodzaj, częstotliwość odwiedzanych stron internetowych oraz długość sesji oraz publiczne reakcje (oznaczanie, polubienia, emotikony) na cudze wypowiedzi, to działanie pośredników polegające na przetwarzaniu tych reakcji, a także sugerowaniu i zachęcaniu użytkownika do zachowań znajdujących odzwierciedlenie w rozpowszechnianych przez niego treściach, stanowi ingerencję w sferę korzystania przez niego z wolności wypowiedzi.

Stosowanie systemów rekomendacji²⁸⁶, ze względu na zakres pozyskiwanych przez pośredników internetowych danych o użytkowniku oraz ich przetwarzanie w celu wywołania po stronie użytkownika zasugerowanego mu zachowania, nie tylko ingeruje w prywatność użytkownika, ale – dodatkowo – ogranicza swobodę otrzymywania informacji, a w konsekwencji ingeruje w prawo do samostanowienia. Przekazywanie spersonalizowanych informacji odpowiadających profilowi użytkownika oznacza ograniczenie, spowolnienie albo blokowanie dostępu do informacji, do których użytkownik, co nie jest wykluczone, uzyskałby szybciej dostęp, gdyby informacje nie były personalizowane. O ile bowiem – czemu nie można zaprzeczyć – posiadanie profilu pozwala na szybszy dostęp do informacji, to jednak w innym wypadku,

²⁸⁵ Szczegółowa analiza tego terminu została przeprowadzona w rozdziale I niniejszej pracy.

²⁸⁶ Opiswane są co najmniej 3 podejścia do tworzenia systemów rekomendacji. Pierwszą techniką rekomendacyjną jest filtrowanie z analizą zawartości (ang. *content-based filtering*), które sugeruje produkty na podstawie podobieństwa ich cech z profilem użytkownika. Uwzględniając jego upodobania, filtrowanie z analizą zawartości wyszukuje pozycje podobne, bazując na analizowaniu atrybutów specyficznych dla danego systemu. Drugim podejściem stosowanym w systemach rekomendacyjnych jest tzw. wspólna filtracja (ang. *collaborative filtering*). Opiera się ona na założeniu, że jeżeli dwóch użytkowników lubi podobne produkty lub ma podobne preferencje, to z dużym prawdopodobieństwem będą podobnie zachowywać się w odniesieniu do innych rzeczy. Trzecia technika przyjmuje podejście mieszane (Zob. D. Bieńkowski, *Mechanizmy...*, s. 20.

w szczególności wówczas, gdy użytkownik wychodzi poza ramy przewidywalnego zachowania, przypisany mu przez pośrednika profil stanowić będzie przeszkodę w pozyskiwaniu dostępu do informacji. Posiadanie określonych cech i preferencji może bowiem zarówno faworyzować użytkownika w dostępie do informacji, jak i – w odniesieniu do innych informacji – ze względu na te same cechy i preferencje użytkownika dostęp do informacji może być spowolniony lub ograniczony.

W AUC zawarto wyjaśnienie, że system rekomendacji jest podstawową częścią działalności platformy internetowej. Jest to sposób szeregowania i prezentowania informacji na jej interfejsie internetowym, aby – jak w skazano w motywie 70 – ułatwić i zoptymalizować dostęp do informacji odbiorcom usługi. Odbywa się to np. poprzez algorytmiczne sugerowanie, plasowanie i szeregowanie informacji, wyróżnianie za pomocą tekstu lub innych przedstawień graficznych lub w inny sposób selekcjonowanie informacji przekazywanych przez odbiorców. W AUC potwierdzono, że takie systemy rekomendacji mogą mieć znaczący wpływ na zdolność odbiorców do wyszukiwania informacji i interakcji z nimi w internecie (motyw 70). Ustawodawca europejski kładzie jednak akcent na pozytywne skutki wykorzystania systemu rekomendacji, wskazując, że służą „ułatwieniu odbiorcom usługi wyszukiwania odpowiednich informacji i przyczynienia się do poprawy doświadczeń użytkowników” (motyw 70). Co prawda zauważono także, że systemy rekomendacji „odgrywają również ważną rolę w akcentowaniu pewnych wiadomości, wirusowym rozpowszechnianiu informacji i stymulowaniu zachowań w internecie” (motyw 70), jednakże nie przesądziło to o potrzebie wprowadzenia regulacji ograniczających stosowanie systemów rekomendacji.

Atrakcyjność systemów rekomendacji tkwi w stymulowaniu zachowań użytkowników, którzy przez system zachęt, w szczególności realizowanych poprzez oferowanie użytkownikom informacji we „względnej kolejności” (art. 27 ust. 3 AUC), podejmują działania dogodne dla „operatora systemu rekomendacji”. Wydaje się, że stopień spersonalizowania informacji wykorzystywanych w systemach rekomendacji nie zawsze jest taki sam. Wysoki stopień spersonalizowania oznacza zarazem zawężanie wyników wyszukiwania i ograniczenie ich ze względu na osobiste cechy i preferencje użytkownika. Użytkownik nie uzyskuje zatem informacji w takim zakresie i odpowiadającej tej jakości, jaka byłaby udziałem tzw. przeciętnego odbiorcy.

Z jednej strony mogą to być wysoce specjalistyczne informacje, z drugiej jednak strony, użytkownik może zostać pozbawiony dostępu do informacji, które uzyskują inni (niesprofilowani) użytkownicy.

Systemy rekomendacji stosują mechanizm różnicowania dostępu do informacji ze względu na przyjęte w tym systemie kryteria, które – co do zasady – nie są znane użytkownikowi²⁸⁷. Zatem nawet jeśli ustawodawca europejski nakazuje pośrednikom internetowym stosującym systemy rekomendacji ujawniać „w swoich warunkach korzystania z usług” „kryteria, które są najistotniejsze przy określaniu informacji sugerowanych odbiorcy usługi” oraz „powodów względnego znaczenia tych parametrów” (art. 27 ust. 2 lit. a i b AUC), to nadal użytkownik nie wie, jaką cechą relevantną wyróżnił się jego profil w stosunku do profili pozostałych użytkowników przy dokonywanym przez pośrednika doborze spersonalizowanego dla niego pakietu informacji. Użytkownik wie zatem, że został „wyróżniony” ze względu na posiadanie pewnej cechy, a nadto wie także, że inni użytkownicy również zostali „wyróżnieni”, jednakże żaden z nich nie ma wiedzy odnośnie do sposobu, w jakim doszło do zróżnicowania ich pozycji w dostępie do informacji.

Stosowane przez pośredników internetowych systemy rekomendacji prowadzą do różnicowania grup użytkowników (profilowania) oraz indywidualizowania (personalizowania) użytkowników ze względu na posiadane cechy i preferencje w zakresie przyznawanych im uprawnień i szeregowania w dostępie do informacji. Stworzony przez dostawców usług cyfrowych profil użytkownika przesądza o zasadach i zakresie udzielania „sprofilowanemu” użytkownikowi dostępu do świadczonych przez pośredników usług, w szczególności poprzez szeregowanie i klasyfikowanie przekazywanych mu informacji według znanego pośrednikowi, lecz nieznanemu użytkownikowi internetu, klucza²⁸⁸.

²⁸⁷ Każdy Administrator danych osobowych ma – co prawda – obowiązek, wynikający z art. 13 RODO, poinformować osobę, której dane przetwarza, o zakresie zebranych danych, a także celu ich przetwarzania i przewidywanym okresie, jednakże nie oznacza to faktycznie, że użytkownik posiada wiedzę, jak wygląda – w świetle algorytmicznej analizy ADO – jaki jest jego profil, w szczególności profil zakupowy, polityczny, społeczny itd.

²⁸⁸ W regulaminie Facebooka, który wszedł w życie 23 sierpnia 2023 r., w szczególności wskazano, że personalizowanie użytkowników skutkujące wyświetlaniem mu określonych informacji jest wynikiem oceny dokonywanej przez Facebook. Arbitralność i uznaniowość Facebooka ujawniają się w treści regulaminu poprzez wielokrotne

Zważywszy, że rozwiązania oparte na profilowaniu mają charakter systemowy, a nadto zostały potwierdzone (zalegalizowane) w rozporządzeniu PE zakładającym pełną harmonizację i bezpośrednio stosowanym we wszystkich państwach członkowskich UE, zasadne jest dokonanie ich oceny na gruncie art. 21 Karty praw podstawowych i art. 10 TFUE, konstytuujących zasadę równego traktowania (niedyskryminacji). Zgodnie z art. 10 TFUE przy określaniu i realizacji swoich polityk i działań Unia dąży do zwalczania wszelkiej dyskryminacji ze względu na płeć, rasę lub pochodzenie etniczne, religię lub światopogląd, niepełnosprawność, wiek lub orientację seksualną. Zakaz dyskryminacji wyartykułowany w art. 21 Karty praw podstawowych²⁸⁹ także zawiera zakaz wszelkiej dyskryminacji, w szczególności „ze względu na płeć, rasę, kolor skóry, pochodzenie etniczne lub społeczne, cechy genetyczne, język, religię lub przekonania, poglądy polityczne lub wszelkie inne poglądy, przynależność do mniejszości narodowej, majątek, urodzenie, niepełnosprawność, wiek lub orientację seksualną”.

Dokonując wykładni pojęcia „dyskryminacja” na gruncie art. 21 KPP, A. Wróbel zauważa, że „Istotnym elementem definicji dyskryminacji jest niedozwolone kryterium różnicujące lub niedozwolona podstawa (*prohibited ground*) nierównego traktowania. Jest to najogólniej rzecz ujmując, pewna cecha, właściwość lub charakterystyka osoby, ze względu na które wyodrębnia się daną jednostkę spośród innych osób i ze względu na tę cechę traktuje się

użycie takich wyrażeń jak, w szczególności: „naszym zdaniem”, a także „jeżeli uznamy”. Jeśli zdaniem Facebooka (zdaniem firmy META) użytkownik ma pewne cechy albo prezentuje zachowania nadające się do skatalogowania jako „profil użytkownika”, są mu dostarczane informacje w wybranej przez Meta kolejności i zakresie. W regulaminie postanowiono np., że: „Regulamin stanowi umowę pomiędzy użytkownikiem a Meta Platforms Ireland Limited. [...] Korzystając z naszych Produktów, użytkownik wyraża zgodę na wyświetlanie mu reklam, które naszym zdaniem mogą być istotne dla niego i jego zainteresowań. Wykorzystujemy dane osobowe użytkownika, aby określić, które spersonalizowane reklamy mu pokazać”; zob. Regulamin, https://www.facebook.com/legal/terms_preview_DSA (dostęp: 25.09.2023). W innym miejscu Regulaminu wskazano: „Jeżeli uznamy, że zawartość jest sprzeczna z naszymi regulaminami i zasadami, podejmujemy w związku z nią działania [...]”; zob. *W jaki sposób stosujemy nasze zasady dotyczące treści*, <https://transparency.fb.com/pl-pl/enforcement/taking-action/applying-content-policies/> (dostęp: 25.09.2023).

²⁸⁹ Karta praw podstawowych.

tę osobę inaczej, z reguły mniej korzystnie, niż osoby, które nie mają tej cechy, właściwości lub charakterystyki”²⁹⁰.

Mechanizm systemów rekomendacji stosowanych przez pośredników internetowych opiera się na wyróżnieniu użytkownika ze względu na cechy lub preferencje, a następnie sklasyfikowaniu go do kategorii podmiotów, których „profile” tworzy pośrednik, by – jak będzie wskazywał – „ułatwić” użytkownikowi dostęp do informacji, ale także – czego pośrednicy nie akcentują – stymulować zachowania użytkownika poprzez zachęcanie go do zachowań zgodnych z interesem pośrednika.

System rekomendacji stosowany przez pośredników internetowych działa, co dodatkowo zwraca uwagę, na zasadach zbliżonych do warunkowego dostępu²⁹¹, przy czym spełnienie przez użytkownika „warunku” uzyskania dostępu pozostaje poza sferą decyzyjną użytkownika. W miejsce użytkownika decyzje te podejmuje za niego pośrednik internetowy na podstawie uprzednio przeprowadzonej oceny zachowania się użytkownika (przesłanki behawioralne) i jego cech osobistych. Oznacza to, że dostęp do informacji o wysokim poziomie referencyjności jest warunkowany nie tylko sprawnością i precyzją sformułowanego przez użytkownika zapytania, ale przede wszystkim wypadkową cech tworzących profil użytkownika, a niekiedy także wykazaniem przez użytkownika posiadania uprawnień dostępu do informacji, w szczególności poprzez zaakceptowanie warunków wskazanych w systemie rejestracji, obligatoryjnym logowaniu lub przy uiszczeniu mikropłatności. W konsekwencji dostęp do informacji staje się możliwy tylko

²⁹⁰ A. Wróbel, *Komentarz do art. 21 KPP*, [w:] *Karta Praw Podstawowych...*, pkt 16.

²⁹¹ Dostęp warunkowy w sektorze nowych technologii jest rozumiany jako „zapewnianie przez nadawców i operatorów stosujących odpowiednie środki techniczne, możliwości odbioru przesyłanych usług tylko uprawnionym do tego osobom (zob. Grupa problemowa do spraw techniki i sprzętu Międzyresortowego Zespołu ds. Telewizji i Radiofonii Cyfrowej, *Dostęp warunkowy dla polskiej naziemnej telewizji cyfrowej*, Warszawa 2009, s. 20). W dyrektywie 98/84/WE z dnia 20 listopada 1998 r. w sprawie prawnej ochrony usług opartych lub polegających na warunkowym dostępie (Dz.U. WE L Nr 320) pojęcie „dostępu warunkowego jest rozumiane jako wszelkie środki i/lub urządzenia techniczne, przy pomocy których dostęp do usług chronionych w zrozumiałej formie jest uwarunkowany wcześniejszym indywidualnym upoważnieniem (art. 2 pkt b). W ustawie z dnia 5 lipca 2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym (t.j. Dz.U. z 2015 r., poz. 1341) warunkowy dostęp oznacza „wszelkie środki oraz przedsięwzięcia techniczne, warunkujące korzystanie z usług chronionych przez indywidualnego usługobiorcę”.

dla zalogowanych użytkowników, co oznacza zazwyczaj potwierdzenie przyjęcia warunków świadczenia usługi zawartych w regulaminach host providerów, a także udzielenie koniecznych zezwoleń lub dalej idących zgód na bardziej intensywne, precyzyjne i ingerujące w sferę praw osobistych użytkownika profilowanie. Systemy rekomendacji, pomimo że do wyświetlania informacji wykorzystują wiele mechanizmów profilowania i personalizowania treści, to jednak każdy z wykorzystywanych mechanizmów opiera się na kryterium behawioralnym, tj. związanym z cechami osobistymi użytkownika internetu i sposobem jego aktywności w sieci²⁹².

Ustawodawca europejski dostrzegając zagrożenie wynikające z możliwości wielokrotnego monitorowania użytkowników, wskazuje, że „dostawcy usług pośrednich w warunkach korzystania z ich usług powinni wyraźnie podawać i aktualizować informacje o powodach, dla których mogą ograniczyć świadczenie swoich usług. Warunki te powinny w szczególności zawierać informacje na temat wszelkich polityk, procedur, środków i narzędzi wykorzystywanych do celów moderowania treści, w tym algorytmicznego podejmowania decyzji i weryfikacji przez człowieka, a także na temat regulaminu wewnętrznego systemu rozpatrywania skarg. Powinny one również zawierać łatwo dostępne informacje na temat prawa do zakończenia korzystania z usługi” (motyw 45 AUC).

Różnicowanie w dostępie do informacji ma wymiar systemowy, a zatem nie jest praktyką jednorazową, przypadkową lub incydentalną. Działalność pośredników internetowych stosujących systemy rekomendacji, polegających na filtrowaniu i doborze tylko niektórych informacji i opinii przy

²⁹² Jak zauważa D. Bieńkowski, „Wzorzec »najpierw najlepszy« (ang. *best first*) jest obecnie najbardziej popularnym wzorcem wykorzystywanym w mechanizmach rekomendacji. Jego zadaniem jest sugerowanie produktów czy wyników zapytania nie w kolejności, w jakiej zostały odszukane, a przedstawienie ich od najbardziej trafnego dla użytkownika. Kolejnym wzorcem, z którego mogą korzystać mechanizmy rekomendacji, jest nawigacja fasetowa (ang. *faceted navigation*), uważana za jedną z największych innowacji w dziedzinie wyszukiwania i rekomendacji. Kolejnym mechanizmem jest personalizacja oparta na profilowaniu. Obserwowanie operacji wykonywanych przez użytkownika może dostarczyć niezbędnych informacji o jego upodobaniach i rutynowych czynnościach, które mogą być podstawą zaawansowanej personalizacji. Stworzenie na takiej podstawie profilu użytkującego serwis, pozwoli algorytmom dostosować wygląd i zaprezentować treści zgodnie z indywidualnymi preferencjami, potrzebami i zainteresowaniami (zob. D. Bieńkowski, *Mechanizmy...*, s. 12–15).

jednoczesnym opóźnianiu, ograniczaniu albo blokowaniu dostępu do innych informacji, niepoparte świadomie wyrażoną przez użytkownika zgodą na takie działanie, stanowi przejaw dyskryminacji na płaszczyźnie wolności wypowiedzi.

Zalegalizowanie przez ustawodawcę europejskiego działań systemowych, a zatem realizowanych w sposób zaplanowany, celowy, świadomy, a nadto kontrolowany przez podmioty prywatne, w szczególności bardzo duże platformy internetowe i bardzo duże wyszukiwarki internetowe, może rodzić także wątpliwości odnośnie do ich dopuszczalności ze względu na przesłankę proporcjonalności ingerencji w wolność wypowiedzi. Skoro bowiem ingerencji dokonują podmioty prywatne działające – co do zasady – w ramach wolności gospodarczej, pozostające poza kontrolą państw członkowskich, korzystając zarazem z obszernego katalogu upoważnień wynikających zarówno z AUC, jak i ustanowionych przez nich regulaminów korzystania z usług, a nadto ingerencja ta może przybierać nawet najbardziej dotkliwą dla użytkowników formę, tj. usuwania treści (art. 17 ust. 1 lit. a AUC), a także zawieszenia świadczenia usługi (art. 23 ust. 1 AUC), to istnieje poważne ryzyko zachwiania prawidłowego balansu pomiędzy ochroną wolności wypowiedzi a przeciwdziałaniem naruszeniu innej chronionej wartości, zwłaszcza wówczas, gdy identyfikowanie tej wartości oraz ustalenie ryzyka jej naruszenia odbywa się poza kontrolą wyspecjalizowanych organów i zostało w całości powierzone pośrednikom internetowym.

V. Odwrócony standard wolności wypowiedzi

1. Prejudycjalne przesłanki ochrony – aspekty materialnoprawne

A. Ochrona praw autorskich

Zasady ochrony praw autorskich w internecie reguluje dyrektywa 2019/790¹. Dostawcy usług cyfrowych zostali określani – zgodnie z art. 2 pkt 6 dyrektywy DSM – jako „dostawcy usług udostępniania treści online”. Dostawca usług udostępniania treści online oznacza dostawcę usług społeczeństwa informacyjnego, którego głównym lub jednym z głównych celów jest przechowywanie i udzielanie publicznego dostępu do dużej liczby chronionych prawem autorskim utworów lub innych przedmiotów objętych ochroną zamieszczanych przez użytkowników tych usług, które są przez niego organizowane i promowane w celach zarobkowych. W dyrektywie zastrzeżono jednocześnie, że dostawców usług takich jak nienastawione na zysk encyklopedie internetowe, nienastawione na zysk repozytoria naukowe i edukacyjne, platformy tworzenia otwartego oprogramowania i platformy wymiany otwartego oprogramowania, dostawców usług łączności elektronicznej zdefiniowanych w dyrektywie (UE) 2018/1972, internetowych platform handlowych oraz usług w chmurze dla przedsiębiorstw i usług w chmurze obliczeniowej, które umożliwiają użytkownikom zamieszczanie treści na własny użytek, nie uznaje się za dostawców usług udostępniania treści online w rozumieniu dyrektywy (art. 2 pkt 6 dyrektywy DSM).

¹ Dyrektywa DSM.

Niezależnie od wskazanych wyżej wyłączeń podmiotowych, określone w dyrektywie DSM zasady odpowiedzialności stosowane do „dostawców usług udostępniania treści online” zostały uregulowane odmiennie niż ma to miejsce – w ogólności – do dostawców usług cyfrowych. Ustawodawca europejski ustanawia bowiem trzy reżimy odpowiedzialności. O ile ogólne zasady ponoszenia odpowiedzialności przez dostawców usług cyfrowych reguluje dyrektywa 2000/31, w szczególności jej art. 12–14², o tyle odmiennie kształtują się zasady odpowiedzialności podmiotów świadczących usługi pośrednie, a także inne są zasady odpowiedzialności dostawców usług udostępniania treści online.

Należy podkreślić, że termin „dostawca usługi cyfrowej” zdefiniowany w art. 4 pkt 6 dyrektywy NIS³ jest najbardziej pojemny i obejmuje zarówno dostawców usług społeczeństwa informacyjnego (art. 1 lit. b dyrektywy w sprawie usług społeczeństwa informacyjnego)⁴, jak też usług pośrednich w rozumieniu art. 3 lit. g rozporządzenia w sprawie usług cyfrowych⁵, przy czym – zgodnie z tym przepisem – usługi pośrednie stanowią pewien rodzaj (część) usług społeczeństwa informacyjnego.

Działalność „dostawców usług udostępniania treści online” stanowi, zgodnie z art. 2 pkt 6 dyrektywy DSM⁶, usługę społeczeństwa informacyjnego. Zarazem w zakresie, w jakim polega ona na „przechowywaniu chronionych prawem autorskim utworów” mieści się – co do zasady – w definicji terminu „usługa pośrednia” (art. 3 lit. g rozporządzenia w sprawie usług cyfrowych). Niemniej ustawodawca europejski postanowił, że w odniesieniu do dostawców usług cyfrowych, jeśli przedmiotem ich działalności jest przechowywanie

² Dyrektywa o handlu elektronicznym.

³ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. UE L Nr 194/1), <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32016L1148#d1e697-1-1> (dostęp: 10.10.2023).

⁴ Dyrektywa 2015/1535.

⁵ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych) (Dz.U. UE L Nr 277/1), <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32022R2065#d1e1573-1-1> (dostęp: 10.10.2023) – dalej: rozporządzenie w sprawie usług cyfrowych (o usługach cyfrowych).

⁶ Dyrektywa DSM.

lub udzielanie dostępu do przedmiotów praw autorskich lub praw pokrewnych, do ustalenia zasad ponoszenia odpowiedzialności zastosowanie znajdują przepisy dyrektywy DSM. Wskazane tam zasady odmiennie ustalają zakres i sposób ponoszenia odpowiedzialności za naruszenia prawa działalności dostawców usług cyfrowych, niż zostało to określone w dyrektywie 2000/31 w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego⁷, a zarazem odmiennie, niż wynika to z treści rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych (akt o usługach cyfrowych). Odmiennie zasady odpowiedzialności wskazane dla dostawców udostępniania treści online oznacza *de facto* wkroczenie w sferę wolności wypowiedzi tych podmiotów poprzez ograniczenie sfery swobody wypowiedzi ze względu na potrzebę ochrony praw wyłącznych twórców oraz podmiotów uprawnionych z innych tytułów niż autorstwo dzieła. Dostawcy usług udostępniania treści online ponoszą odpowiedzialność za czynności publicznego udostępniania lub podawania do publicznej wiadomości utworów na zasadach określonych w dyrektywie DSM (motyw 65 dyrektywy DSM). Przesłanka ochrony praw twórców stanowi zatem jeden z elementów konstrukcyjnych współczesnego standardu wolności wypowiedzi.

Korzystanie z przedmiotów własności intelektualnej przez inne osoby niż sam twórca zawsze rodziło niepokój o zakres zgodnego z prawem (dozwolonego) użytku utworów, w szczególności wówczas, gdy pozostawało to w związku ze swobodą wypowiedzi realizowaną przez podmiot korzystający z utworu. Zmiana postaci utworu z analogowej (tradycyjnej) na cyfrową oraz możliwość wprowadzenia utworu do publicznie dostępnego systemu teleinformatycznego problem ten pogłębiła. Konflikt między realizacją wolności wypowiedzi a korzystaniem z przedmiotów praw autorskich i praw pokrewnych ustawodawca unijny rozstrzyga w postanowieniach dyrektywy 2019/790, pozostawiając zarazem w mocy postanowienia dyrektywy 2001/29⁸ w zakresie, w jakim zapewnia ona ochronę środków technologicznych.

⁷ Dyrektywa o handlu elektronicznym.

⁸ Dyrektywa 2001/29/WE Parlamentu Europejskiego i Rady z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym (Dz.U. UE L Nr 167, s. 10 z późn. zm.).

Celem wprowadzania wyjątków i ograniczeń w zakresie korzystania z wolności wypowiedzi w internecie, rozumianej także jako wolność świadczenia usług polegających na przechowywaniu i udostępnianiu treści własnych i cudzych, jest – jak wskazano w motywie 6 w dyrektywy DSM – osiągnięcie sprawiedliwej równowagi między prawami i interesami twórców i innych podmiotów uprawnionych z jednej strony, a prawami i interesami użytkowników z drugiej strony. O ile zadaniem dyrektywy 2001/29 była ochrona środków technologicznych (art. 6) w celu zagwarantowania uprawnionym podmiotom realizacji praw wyłącznych:

1. do zwielokrotniania utworu (art. 2),
2. do decydowania o publicznym udostępnieniu utworu (art. 3) oraz
3. do rozpowszechniania utworu (art. 4) poprzez wyczerpujące wyliczenie wyjątków i ograniczeń dla realizacji tych praw (motyw 32),

o tyle cel dyrektywy DSM stanowi „modernizacja niektórych aspektów unijnych ram prawa autorskiego w celu uwzględnienia postępu technologicznego i nowych kanałów rozpowszechniania treści chronionych w ramach rynku wewnętrznego” (motyw 83).

„Modernizacja” dotychczasowych regulacji prawnoautorskich nastąpiła przede wszystkim poprzez wyczerpujące wyliczenie szczególnych przypadków, w których, bez uszczerbku dla praw podmiotów uprawnionych, dozwolone jest eksploatowanie utworów, w tym także mechanizmów udzielania licencji zbiorowych oraz wyodrębnienia szczególnych celów, które usprawiedliwiają dalej idącą ingerencję w prawa autorskie. *Ratio legis* przyjęcia dyrektywy DSM było – jak wynika z zawartych w niej motywów – uzupełnienie istniejących już regulacji (motyw 4 dyrektywy DSM)⁹.

⁹ W motywie 4 wskazano, że dyrektywa DSM opiera się na zasadach określonych w dyrektywach obowiązujących obecnie w tej dziedzinie i stanowi ich uzupełnienie, tj.: dyrektywa 96/9/WE Parlamentu Europejskiego i Rady z dnia 11 marca 1996 r. w sprawie ochrony prawnej baz danych (Dz.U. L Nr 77, s. 20), dyrektywa o handlu elektronicznym, dyrektywa 2001/29/WE Parlamentu Europejskiego i Rady z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym (Dz.U. L Nr 167, s. 10), dyrektywa 2006/115/WE Parlamentu Europejskiego i Rady z dnia 12 grudnia 2006 r. w sprawie prawa najmu i użyczenia oraz niektórych praw pokrewnych prawu autorskiemu w zakresie własności intelektualnej (Dz.U. L Nr 376, s. 28), dyrektywa Parlamentu Europejskiego i Rady 2009/24/WE z dnia 23 kwietnia 2009 r. w sprawie ochrony prawnej programów komputerowych (Dz.U. L Nr 111, s. 16), dyrektywa Parlamentu Europejskiego i Rady 2012/28/UE z dnia 25 października

Pojęcie standardu wolności wypowiedzi stanowi konstrukcję prawną, na którą składa się zestaw powiązanych ze sobą uprawnień i obowiązków przyjmujących postać praw pozytywnych i negatywnych. W ujęciu pozytywnym standard wolności wypowiedzi oznacza zatem przestrzeń dozwolonej aktywności polegającej na udostępnianiu, przechowywaniu, przetwarzaniu i pozyskiwaniu treści w każdej formie nadającej się do przenoszenia informacji. W ujęciu negatywnym standard wolności wypowiedzi obejmuje obowiązek niedziałania, powstrzymania się przed działaniem albo jego zaniechania, jeśli działanie pozostawało w kolizji z prawem podmiotowym innej osoby. Potrzeba ochrony praw autorskich i pokrewnych modyfikuje standard wolności wypowiedzi, uzależniając ocenę zgodności z prawem korzystania z wolności wypowiedzi od ustalenia ich autorstwa, przy czym bez znaczenia dla ustalenia legalnego albo nielegalnego sposobu korzystania z wolności wypowiedzi jest treść i forma, lecz ważny jest jej prawnoautorski status, tj. ustalenie, czy wypowiedź jest utworem, a w konsekwencji, czy istnieją prawne ograniczenia w jej eksploatacji przez inne osoby.

Zważywszy na okoliczność, że elementem wypowiedzi może być wypowiedź cudza, a także jej fragment, w szczególności wówczas, gdy ma charakter twórczy, niezależnie od tego, czy przyjmuje postać werbalną, dźwiękową, czy wizualną (albo inną, jednakże zawsze „ustaloną” w rozumieniu art. 1 ust. 1 pr. aut.¹⁰), konieczne jest takie uregulowanie stosunków społecznych, które nie tylko umożliwi zidentyfikowanie i przypisanie autorstwa (oznaczenie) wypowiedzi i jej fragmentów, ale także pozwoli na eksploatowanie wypowiedzi zgodnie z zamysłem i celami jej twórcy. Eksploatowanie cudzej twórczości

2012 r. w sprawie niektórych dozwolonych sposobów korzystania z utworów osieroconych (Dz.U. L Nr 299, s. 5), dyrektywa Parlamentu Europejskiego i Rady 2014/26/UE z dnia 26 lutego 2014 r. w sprawie zbiorowego zarządzania prawami autorskimi i prawami pokrewnymi oraz udzielania licencji wieloterytorialnych dotyczących praw do utworów muzycznych do korzystania online na rynku wewnętrznym (Dz.U. L Nr 84, s. 72).

¹⁰ Zgodnie z art. 1 ust. 1 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz.U. z 2022 r., poz. 2509) przedmiotem prawa autorskiego jest każdy przejaw działalności twórczej o indywidualnym charakterze, ustalony w jakiejkolwiek postaci, niezależnie od wartości, przeznaczenia i sposobu wyrażenia (utwór). W orzecznictwie wskazuje się, że „przejaw działalności twórczej” oznacza, iż sama myśl ludzka, choćby nawet oryginalna, nie wystarcza, by stała się przedmiotem ochrony prawnej, lecz musi być uzewnętrzniona w postaci ustalającej jej treść i formę (Wyrok NSA z dnia 11 lipca 2018 r., II FSK 1845/16, LEX nr 2528581).

stanowi niewątpliwie przejaw realizacji wolności wypowiedzi zarówno twórcy, jak i podmiotu, który korzysta z cudzego utworu, w tym także w ramach własnej działalności twórczej (twórczość równoległa, prowadzenie własnego rodzaju twórczości) oraz wówczas, gdy zapoznaje się z cudzą twórczością, przechowuje ją, przetwarza, a także, kiedy udostępnia ją innym osobom, w tym w ramach dostarczania usług udostępniania treści online.

Termin „eksploatacja utworu” rozumiany jako konglomerat czynności podejmowanych w imieniu własnym przez podmioty o różnym statusie i w różnych celach ujawnia złożoność standardu wolności wypowiedzi jako konstruktu terminologicznego, który nie ma jednorodnego, zamkniętego katalogu desygnatów. Nie istnieje bowiem standard wolności wypowiedzi jednakowy dla wszystkich, a nadto dookreślanie (precyzowanie) zakresu tego pojęcia może prowadzić do zakwestionowania samego pojęcia standardu. Innego standardu wolności wypowiedzi może zatem oczekiwać twórca, który ma interes prawnych w szerokiej ochronie wypowiedzi, co służy utrzymaniu lub poszerzeniu jego monopolu autorskiego. Inny interes ma użytkownik końcowy. Użytkownik końcowy oznacza osobę fizyczną lub prawną, która korzysta z podstawowych usług platformowych w charakterze innym niż użytkownik biznesowy (art. 2 pkt 20 AUC¹¹). Inny interes prawny ma natomiast użytkownik biznesowy, który w celach związanych z prowadzoną działalnością gospodarczą eksploatuje cudze utwory. „Użytkownik biznesowy” oznacza osobę fizyczną lub prawną działającą w celach handlowych lub zawodowych, która korzysta z podstawowych usług platformowych do celów związanych z dostarczaniem towarów użytkownikom końcowym lub świadczeniem usług na rzecz użytkowników końcowych lub w toku dostarczania towarów takim użytkownikom lub świadczenia usług na ich rzecz (art. 2 pkt 21 aktu o rynkach cyfrowych).

Realizacja celów zawartych w dyrektywie DSM i innych aktach prawnych poprzedzających jej przyjęcie, rozumianych jako równoważenie interesów podmiotów uprawnionych z praw wyłącznych z prawami i interesami pozostałych uczestników rynku usług cyfrowych, następuje poprzez system

¹¹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828 (akt o rynkach cyfrowych) (Dz.U. UE L Nr 265, s. 1).

wyłączeń i ograniczeń, którym ustawodawca europejski obejmuje dostawców usług cyfrowych, wyróżniając w tej grupie szczególne kategorie podmiotów, tj. organizacje badawcze (art. 2 pkt 1 dyrektywy DSM¹²), instytucje dziedzictwa kulturowego (art. 2 pkt 3 dyrektywy DSM¹³), a także dostawców publikacji prasowych (art. 2 pkt 4 dyrektywy DSM) oraz „dostawców usług udostępniania treści online” (art. 2 pkt 6 dyrektywa DSM). W odniesieniu do każdej z wymienionych powyżej grup zastosowanie znajduje odmienny system ograniczeń i wyłączeń.

Przez system ograniczeń i wyłączeń należy rozumieć zestaw narzędzi i środków prawnych wskazanych w dyrektywach autorskich, które służą zawężeniu zakresu korzystania z praw wyłącznych przez uprawnione podmioty, a w konsekwencji służą poszerzeniu przestrzeni dozwolonej eksploracji utworów przez podmioty wskazane w tym systemie. Stworzenie wyczerpującego systemu ograniczeń i wyłączeń miało nastąpić w dyrektywie 2001/29/WE¹⁴. System ten uległ jednak doprecyzowaniu i poszerzeniu w dyrektywie DSM poprzez objęcie nim organizacji badawczych i instytucji dziedzictwa narodowego, a także publikacji prasowych oraz działalności służącej zilustrowaniu w ramach nauczania lub badań naukowych, o ile wskazane jest źródło, łącznie z imieniem i nazwiskiem twórcy, chyba że okaże się to niemożliwe, i w stopniu uzasadnionym przez niekomercyjny cel, który ma być osiągnięty (art. 5 ust. 3 lit. a dyrektywy 2001/29).

W odniesieniu do organizacji badawczych i instytucji dziedzictwa narodowego zauważono, że stają one wobec problemu niepewności prawa odnośnie do tego, w jakim zakresie mogą one dokonywać analizy treści w drodze eksploracji tekstów i danych. W niektórych przypadkach eksploracja tekstów i danych może obejmować czynności chronione prawem autorskim

¹² „Organizacja badawcza” oznacza uczelnię, łącznie z należącymi do niej bibliotekami, instytut badawczy lub inny podmiot, którego głównym celem jest prowadzenie badań naukowych lub działalności edukacyjnej obejmującej także – nienastawione na zysk – prowadzenie badań naukowych (art. 2 pkt 1 dyrektywy DSM).

¹³ „Instytucja dziedzictwa kulturowego” oznacza ogólnodostępną bibliotekę lub muzeum, archiwum lub instytucję dziedzictwa filmowego lub instytucję dziedzictwa dźwiękowego.

¹⁴ W motywie 32 dyrektywy 2001/29 *explicite* wskazano, że „Niniejsza dyrektywa zawiera wyczerpujące wyliczenie wyjątków i ograniczeń dla prawa do zwielokrotniania i prawa do publicznego udostępniania utworu”.

lub prawem do bazy danych (motyw 8 dyrektywy DSM). W konsekwencji przyjęto, że instytucje te i organizacje mogą powoływać się na wyjątek od wyłącznego prawa do zwielokrotniania oraz od prawa do ochrony przed pobieraniem danych z bazy danych (motyw 11 dyrektywy DSM). Za instytucje dziedzictwa kulturowego powinno się uważać ogólnodostępne biblioteki i muzea, niezależnie od rodzaju utworów lub innych przedmiotów objętych ochroną znajdujących się w ich stałych zbiorach, a także archiwa oraz instytucje dziedzictwa filmowego lub dźwiękowego. Za dopuszczalne, a zatem objęte wyjątkiem egzekwowania praw wyłącznych, przyjęto, że biblioteki i muzea, niezależnie od rodzaju utworów lub innych przedmiotów objętych ochroną znajdujących się w ich stałych zbiorach, jak też archiwa oraz instytucje dziedzictwa filmowego lub dźwiękowego mogą tworzyć i przechowywać kopie utworów pozostających w ich zasobach.

Szczegółne zasady eksploracji, w tym publicznego udostępniania utworów, przyznano wydawcom prasy, a mianowicie prawo do zwielokrotniania, publicznego udostępniania utworów i podawania do publicznej wiadomości artykułów na aktualne tematy gospodarcze, polityczne lub religijne oraz utworów nadawanych lub innych przedmiotów objętych ochroną tego samego rodzaju, chyba że korzystanie z nich zostało zastrzeżone i o ile zostanie wskazane źródło (art. 5 ust. 3 lit c dyrektywy 2001/29). Ponadto uznano organizacyjny i finansowy wkład, jaki wydawcy wnoszą w produkcję publikacji prasowych. Za konieczne uznano stworzenie zachęt dla wydawców prasy, aby zapewnić stabilność branży wydawniczej, a tym samym zwiększyć dostępność rzetelnych informacji (motyw 55 dyrektywy DSM). Wydawcom zagwarantowano zatem nie tylko szersze ramy korzystania z przedmiotów praw autorskich i pokrewnych, z wyłączeniem jednak prawa do linkowania (motyw 57 dyrektywy DSM), ale także zapewniono ochronę publikacji prasowych¹⁵

¹⁵ Przez „publikację prasową” ustawodawca europejski rozumie zbiór złożony głównie z utworów literackich o charakterze dziennikarskim, mogący jednakże obejmować także inne utwory lub inne przedmioty objęte ochroną, który: a) stanowi odrębną całość w ramach periodycznej lub regularnie aktualizowanej pod jednym tytułem publikacji, takiej jak gazeta lub czasopismo o tematyce ogólnej lub specjalistycznej; b) ma na celu dostarczenie opinii społecznej informacji dotyczących aktualnych wiadomości lub innej tematyki; oraz c) jest publikowany w dowolnym medium z inicjatywy dostawcy usług, na jego odpowiedzialność i pod jego kontrolą (art. 2 pkt 4 dyrektywy DSM). Zastrzeżono zarazem, że publikacje periodyczne publikowane do celów naukowych lub akademickich,

wytwarzanych przez dziennikarzy i rozpowszechnianych na stronach internetowych wydawcy. Ochrona ta obejmuje zwielokrotnianie i podawanie do publicznej wiadomości publikacji prasowych (art. 15 ust. 2 dyrektywy DSM w zw. z art. 2 i art. 3 ust. 2 dyrektywy 2001/29). Tym samym ustawodawca europejski tworzy odmienne standardy wolności wypowiedzi dla dostawców usług, których – ze względu na przyjętą definicję – należy kwalifikować do wskazanych powyżej grup podmiotów.

Mechanizm wyłączeń i ograniczeń nie znajduje zastosowania do „dostawców usług udostępniania treści online”. Jak wyjaśniono w wytycznych do art. 17 dyrektywy DSM¹⁶, aby wchodzić w zakres definicji dostawcy usług udostępniania treści online oraz w zakres systemu określonego art. 17, dostawca usług musi łącznie spełniać wszystkie wymogi zawarte w definicji, tj. po pierwsze, być dostawcą usług społeczeństwa informacyjnego w rozumieniu art. 1 ust. 1 lit. b) dyrektywy 2015/1535; po drugie, mieć za główny lub jeden z głównych celów w kwestii utworów lub innych przedmiotów chronionych prawem autorskim:

- a) przechowywanie i udzielanie publicznego dostępu do nich;
- b) dysponowanie ich dużą liczbą;
- c) zarządzanie utworami zamieszczanymi przez użytkowników,
- d) organizowanie i promowanie ich w celach zarobkowych¹⁷.

„Główny cel” lub „jeden z głównych celów” usługi społeczeństwa informacyjnego należy rozumieć jako główną lub dominującą funkcję (lub jedną z głównych funkcji) lub rolę dostawcy usług¹⁸.

Definicja usługi udostępniania treści online zawarta w dyrektywie DSM, jak wynika z motywu 62 dyrektywy, powinna być interpretowana w ten sposób, by obejmować nią wyłącznie usługi online, które odgrywają ważną rolę na rynku treści online, konkurując z innymi usługami online dotyczącymi

takie jak czasopisma naukowe, nie są publikacjami prasowymi do celów niniejszej dyrektywy (tamże).

¹⁶ Komunikat Komisji do Parlamentu Europejskiego i Rady EMPTy z dnia 4 czerwca 2021 r.: Wytyczne dotyczące art. 17 dyrektywy 2019/790 w sprawie prawa autorskiego na jednolitym rynku cyfrowym, <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52021DC0288> (dostęp 15.10.2023) – dalej: Wytyczne do art. 17 dyrektywy DSM.

¹⁷ Tamże, pkt III.

¹⁸ Tamże.

treści, takimi jak internetowe usługi audio i wideo dla tych samych odbiorców. Usługami „udostępniania treści online” są takie usługi, których głównym lub jednym z głównych celów jest przechowywanie i umożliwianie użytkownikom zamieszczania i udostępniania dużej ilości treści chronionych prawem autorskim w celach zarobkowych. Usługi te obejmują zatem działalność, której głównym celem jest umożliwianie użytkownikom zamieszczania i udostępniania dużej ilości treści chronionych prawem autorskim w celach zarobkowych. Ocena tego, czy dostawca usług udostępniania treści online przechowuje i udziela dostępu do dużej ilości treści chronionych prawem autorskim, powinna być dokonywana indywidualnie dla każdego przypadku i powinna uwzględniać połączenie elementów, takich jak odbiorcy usługi oraz liczba plików zawierających treści chronione prawem autorskim zamieszczanych przez użytkowników usługi (motyw 63).

Grupa „dostawców usług udostępniania treści online”, której aktywność w internecie polega na dokonywaniu czynności „publicznego udostępniania”¹⁹ lub „podawania do publicznej wiadomości utworu” nie tylko nie została objęta mechanizmem wyłączeń i ograniczeń, ale nie znajdują do niej zastosowania reguły wyłączenia odpowiedzialności odnoszące się do usług społeczeństwa informacyjnego wskazane w art. 12–14 dyrektywy o handlu elektronicznym (art. 17 ust. 3 oraz motyw 65 dyrektywy DSM).

Na gruncie dyrektywy DSM przyjęto, że ocena braku bezprawności działania dostawców tych usług powinna odwoływać się do wzorca starannego działania²⁰, wprowadzając zarazem szczególne zasady ponoszenia odpowiedzialności²¹. Ustawodawca europejski używa określenia „wszelkich starań” jakich podjąć się powinni dostawcy, by – ewentualnie – uwolnić się od odpowiedzialności za naruszenia praw autorskich wówczas, gdy udostępniają

¹⁹ Przez publiczne udostępnienie.

²⁰ Obowiązek starannego działania wymaga od dłużnika dołożenia wszelkich starań w celu osiągnięcia rezultatu, bez konieczności jego osiągnięcia. Zobacz podobnie wyroki TS: z dnia 4 czerwca 2009 r. w sprawie Komisja przeciwko Grecji, C-250/07, pkt 68; a także w sprawie UPC Telekabel Wien, pkt 53.

²¹ Opinia Rzecznika Generalnego Henrika Saugmandsgaarda Øe przedstawiona w dniu 15 lipca 2021 r. w sprawie Rzeczpospolita Polska przeciwko Parlamentowi Europejskiemu, Radzie Unii Europejskiej, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=244201&pageIndex=0&doclang=PL&mode=req&dir=&occ=first&part=1&cid=670286> (dostęp: 22.11.2023) – dalej: Opinia Rzecznika Generalnego w sprawie RP przeciwko PE i Radzie.

lub podają do publicznej wiadomości na swoich stronach internetowych cudze utwory. Ocena zaistnienia sprawstwa czynu określanego jako „publiczne udostępnienie” albo „podanie do publicznej wiadomości” stanowiła jedno z kluczowych zagadnień prawnych wymagających interpretacji *in casu* przez Trybunał Sprawiedliwości UE. E. Laskowska-Litak wskazuje, że od 1995 r. Trybunał Sprawiedliwości rozpatrzył blisko 100 pytań prejudycjalnych z zakresu samego tylko prawa autorskiego, przy czym ponad połowa z nich została złożona po 2014 r., a przeważająca większość zapytań kierowanych do TS odnotowana została w odniesieniu do problematyki publicznego udostępnienia utworu²². Trybunał wprowadził skomplikowany i kazuistyczny system ustalania, czy relewantne zachowanie stanowi akt publicznego udostępniania utworu. Dokonując wykładni terminu „publiczne udostępnianie”, TSUE uwzględnia co najmniej trzy kryteria weryfikacji. Po pierwsze TSUE ustala, czy w ogóle doszło do aktu udostępnienia utworu. Po drugie ocenia, czy zachowaniu można przypisać kwalifikację publicznego, a więc czy stanowi ono przeciwieństwo zachowania „prywatnego”. Po trzecie analizuje, czy publiczność, do której skierowane było udostępnienie, jest „nowa”, tj. czy jest to publiczność niezakładana przez twórcę w momencie dokonywania pierwotnego udostępnienia²³.

Okoliczność publicznego udostępnienia utworu, jeśli odbywa się w celach zarobkowych, a nadto obejmuje „dużą ilość treści”, ocenianą z perspektywy liczby potencjalnych jej odbiorców oraz liczby plików zawierających chronione utwory, kwalifikuje dostawcę usługi do grupy usługodawców udostępniających treści online. Biorąc pod uwagę fakt, że dostawcy usług udostępniania treści online udzielają dostępu do treści, których sami nie zamieszczają, lecz które są zamieszczane przez ich użytkowników, do celów dyrektywy DSM przewidziany został odrębny mechanizm odpowiedzialności. Zasadą jest uzyskiwanie przez tych dostawców zezwolenia uprawnionego podmiotu na publiczne udostępnienie treści (motyw 64).

W przypadkach, gdy nie udzielono zezwolenia, znajduje zastosowanie zasada starannego działania jako podstawa dokonywania oceny zgodności

²² E. Laskowska-Litak, *Technicyzacja a unifikacja prawa autorskiego*, „Europejski Przegląd Sądowy” 2023, nr 3, s. 41.

²³ Tamże, s. 42–43.

z prawem świadczenia usług dostarczania treści online. W dyrektywie wskazano, że jeżeli dostawcom usług nie udzielono zezwolenia, powinni oni dołożyć wszelkich starań zgodnie z wysokimi standardami staranności zawodowej w sektorze, aby zapobiegać dostępności w swoich serwisach nieobjętych zezwoleniem utworów i innych przedmiotów objętych ochroną zidentyfikowanych przez odpowiednie podmioty uprawnione (motyw 66). Przy dokonywaniu oceny, czy dostawca usług udostępniania treści online dołożył wszelkich starań zgodnie z wysokimi standardami staranności zawodowej w sektorze, należy wziąć pod uwagę to, czy dostawca usług podjął wszystkie kroki, jakie podjąłby staranny podmiot dla osiągnięcia celu dotyczącego zapobiegania dostępności nieobjętych zezwoleniem utworów lub innych przedmiotów objętych ochroną na swojej stronie internetowej, przy uwzględnieniu najlepszych praktyk stosowanych w sektorze i skuteczności podjętych kroków w świetle wszystkich istotnych czynników i rozwoju sytuacji oraz zasady proporcjonalności (motyw 66). Zarazem wskazano, że dostawcy usług udostępniania treści online powinni ponosić odpowiedzialność w związku z konkretnymi utworami i innymi przedmiotami objętymi ochroną, w odniesieniu do których otrzymali odpowiednie i niezbędne informacje od podmiotów uprawnionych, chyba że dostawcy ci wykażą, że dołożyli wszelkich starań zgodnie z wysokimi standardami staranności zawodowej w sektorze (motyw 66).

Konstrukcja wzorca starannego działania wymaganego od dostawcy usługi udostępniania treści online musi uwzględniać przesłanki wskazane w art. 17 dyrektywy DSM. Zgodnie z art. 17, jeżeli nie udzielono zezwolenia, dostawcy usług udostępniania treści online ponoszą odpowiedzialność za nieobjęte zezwoleniem czynności publicznego udostępniania, w tym podawania do wiadomości publicznej, chronionych prawem autorskim utworów i innych przedmiotów objętych ochroną, chyba że wykażą, że spełnione zostały łącznie trzy przesłanki wymienione w art. 17 ust. 4 lit. a–c, tj. A) dołożyli wszelkich starań, aby uzyskać zezwolenia, oraz B) dołożyli wszelkich starań – zgodnie z wysokimi standardami staranności zawodowej w sektorze – aby zapewnić brak dostępu do poszczególnych utworów i innych przedmiotów objętych ochroną, w odniesieniu do których podmioty uprawnione przekazały dostawcom usług odpowiednie i niezbędne informacje; oraz w każdym przypadku C) działali niezwłocznie po otrzymaniu odpowiednio uzasadnionego

zastrzeżenia od podmiotów uprawnionych w celu zablokowania dostępu do utworów lub innych przedmiotów objętych ochroną, których dotyczy zastrzeżenie, lub usunięcia ich ze swoich stron internetowych, a także dołożyli wszelkich starań, aby zapobiec ich przyszłemu zamieszczaniu zgodnie z lit. b).

Adresatem zawartych w art. 17 ust. 4 dyrektywy DSM przepisie obowiązków jest nie tylko dostawca usług cyfrowych, lecz także państwo. Obowiązek państwa polega na zalegalizowaniu czynności monitorowania i filtrowania treści przez dostawców usług cyfrowych przed ich udostępnieniem, a także na powstrzymaniu się przez państwo przed stosowaniem sankcji za takie czyny, jeśli ich sprawcami są dostawcy usług udostępniania treści online. Obowiązek dostawców takich usług polega natomiast na prewencyjnej analizie dostarczanych przez użytkowników materiałów pod kątem zgodności tych materiałów z prawem autorskim oraz na blokowaniu materiałów przekazywanych przez użytkowników w celu ich publicznego udostępnienia w sieci w wypadku stwierdzenia, że stwarzają one zagrożenie dla ochrony praw autorskich lub pokrewnych.

Wymienione w art. 17 ust. 4 dyrektywy DSM przesłanki konstruują wzorec wymaganego poziomu staranności, a zarazem stanowią warunki, których wypełnienie przez dostawców usług udostępniania treści online pozwala im na uwolnienie się od odpowiedzialności prawnej. Zawarty w art. 17 dyrektywy DSM model starannego działania nakłada na dostawców usług udostępniania treści obowiązki na dwóch płaszczyznach, tj. w zakresie nadzoru nad ich usługami w celu „zapewnienia braku dostępu” do utworów i innych przedmiotów objętych ochroną wskazanych przez podmioty uprawnione i „zapobiec ich przyszłemu zamieszczaniu”, a także w celu wykrycia i zablokowania lub usunięcia, w sposób proaktywny, wśród ogółu treści, które użytkownicy umieszczają online, te, które naruszają prawa autorskie i pokrewne. W opinii Rzecznika Generalnego art. 17 ust. 4 dyrektywy 2019/790 ustanawia system odpowiedzialności dostawców za niedbalstwo: dostawcy usług udostępniania treści zostaną pociągnięci do odpowiedzialności zgodnie z tym przepisem, gdy nie zwalczali z wystarczającą starannością umieszczania online nielegalnych treści przez użytkowników ich usług. Wspomniany art. 17 – w ocenie Rzecznika – stanowi w tym zakresie rodzaj konstrukcji hybrydowej między odpowiedzialnością bezpośrednią ponoszoną przez osoby, które dopuszczają

się czynów niedozwolonych, a odpowiedzialnością pośrednią (lub wtórną) ponoszoną przez pośredników za działania osób trzecich²⁴.

Odmienne zastosowany w art. 17 mechanizm odpowiedzialności oceniła Rzeczpospolita Polska, widząc w nim zagrożenie dla realizacji wolności wypowiedzi zagwarantowanej w art. 11 Karty praw podstawowych²⁵ i art. 10 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności²⁶. Opisany w art. 17 ust. 4 lit. c wzorzec starannego działania, w zakresie w jakim nakłada na dostawców usług obowiązek, by dołożyli wszelkich starań, aby zapobiec przyszłemu zamieszczaniu utworów i innych przedmiotów objętych ochroną, pozostaje – jak zauważyła to Rzeczpospolita Polska, wszczynając na tym tle spór z Komisją i Parlamentem Europejskim²⁷ – narusza wolność wypowiedzi użytkowników internetu.

Zarzut naruszenia EKPC i KPP został oparty na argumentacji, że w celu zwolnienia się z całkowitej odpowiedzialności za udzielenie publicznego dostępu do utworów chronionych prawem autorskim lub innych przedmiotów objętych ochroną zamieszczanych przez ich użytkowników z naruszeniem prawa autorskiego dostawcy usług udostępniania treści online są zobowiązani na mocy art. 17 ust. 4 lit. b) i art. 17 ust. 4 lit. c) *in fine* dyrektywy 2019/790 do prowadzenia prewencyjnego monitorowania wszystkich treści, które ich użytkownicy chcą umieścić online. W tym celu muszą oni korzystać z narzędzi informatycznych umożliwiających uprzednie automatyczne filtrowanie tych treści. Nakładając takie środki prewencyjnego nadzoru na dostawców usług udostępniania treści online, bez przewidzenia przy tym gwarancji zapewniających poszanowanie prawa do wolności wypowiedzi i informacji, zaskarżone przepisy – jak podnosił rząd polski – stanowią ograniczenie w wykonywaniu tego prawa podstawowego, które nie szanuje ani istoty tego

²⁴ Opinia Rzecznika Generalnego w sprawie RP przeciwko PE i Radzie.

²⁵ Karta praw podstawowych Unii Europejskiej (Dz.U. UE C z 2007 r. Nr 303, s. 1 z późn. zm.).

²⁶ Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz.U. z 1993 r. Nr 61, poz. 284 z późn. zm.).

²⁷ Wyrok TS z dnia 26 kwietnia 2022 r. w sprawie Rzeczpospolita Polska przeciwko Parlamentowi Europejskiemu, Radzie Unii Europejskiej, C-401/19, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=261223&pageIndex=0&doclang=PL&mode=lst&dir=&occ=first&part=1&cid=682678#1> (dostęp: 15.10.2023) – dalej: Wyrok TS w sprawie RP przeciwko PE i Radzie.

prawa, ani zasady proporcjonalności, i którego w konsekwencji nie można uznać za uzasadnione²⁸.

Rzeczpospolita Polska utrzymywała, że nakładając na dostawców usług udostępniania treści online obowiązek dołożenia wszelkich starań, po pierwsze, aby zapewnić brak dostępu do poszczególnych chronionych treści, w odniesieniu do których podmioty uprawnione przekazały odpowiednie i niezbędne informacje, oraz po drugie, aby zapobiec przyszłemu zamieszczaniu chronionych treści, co do których podmioty uprawnione złożyły odpowiednio uzasadnione zastrzeżenia, zaskarżone przepisy *in fine* dyrektywy 2019/790 ograniczają wykonywanie prawa do wolności wypowiedzi i informacji użytkowników tych usług zagwarantowane w art. 11 Karty²⁹. Rzeczpospolita Polska domagała się stwierdzenia nieważności art. 17 ust. 4 lit. b) oraz art. 17 ust. 4 lit. c) *in fine* – to znaczy w części obejmującej sformułowanie: „a także dołożyli wszelkich starań, aby zapobiec ich przyszłemu zamieszczaniu, zgodnie z lit. b)” – dyrektywy 2019/790. Tytułem ewentualnego żądania, na wypadek uznania przez Trybunał, że przepisy, o których mowa powyżej, nie mogą zostać oddzielone od pozostałych przepisów zawartych w art. 17 wspomnianej dyrektywy bez zmiany istoty regulacji zawartej w tym artykule – stwierdzenia nieważności tego art. 17 w całości³⁰.

W zarzutach zawartych w skardze RP skierowanej do TSUE wskazano, że prewencyjna weryfikacja dokonywana przez dostawców usług stanowi szczególnie poważną ingerencję w prawo do wolności wypowiedzi i informacji użytkowników internetu, ponieważ z jednej strony wiąże się z ryzykiem blokowania treści zgodnych z prawem, a z drugiej strony kwestia niezgodności danych treści z prawem, a zatem również ich blokowania, jest rozstrzygana automatycznie przez algorytmy, i to jeszcze przed jakimkolwiek rozpowszechnieniem tych treści³¹.

Z wytycznych KE do art. 17 dyrektywy DSM *explicite* wynika, że katalog metod i środków, jakie mogą stosować dostawcy usług udostępniania treści online w celu wykrywania i zapobieżenia publicznemu udostępnieniu chronionych utworów, jest nieograniczony. Wskazano bowiem, że przy obecnym

²⁸ Tamże, pkt 35.

²⁹ Tamże, pkt 39.

³⁰ Tamże, pkt 12.

³¹ Tamże, pkt 41.

stanie techniki nie istnieje żadna technologia pozwalająca dokonać oceny, czy w świetle standardów wymaganych zgodnie z prawem dana treść, którą użytkownik zamierza zamieścić, narusza je, czy też stanowi zgodny z prawem sposób korzystania. Powszechnie stosowana jest obecnie technologia rozpoznawania treści na podstawie cyfrowego odcisku palca (ang. *fingerprinting*), która wykorzystuje cyfrowy odcisk palca utworu (ang. *fingerprint*), z którym porównywane są treści zamieszczane przez użytkowników na platformie. Stosowane są także inne technologie, które umożliwiają wykrywanie nieobjętych zezwoleniem treści. Obejmują one haszowanie³², znak wodny³³, wykorzystanie metadanych³⁴, wyszukiwanie według słów kluczowych³⁵ lub kombinację różnych technologii. Niektórzy dostawcy usług opracowali własne rozwiązania, natomiast inni korzystają z usług osób trzecich³⁶. Komisja Europejska zaleca, by dostawcom usług udostępniania treści online pozostawić swobodę wyboru technologii lub rozwiązań w celu spełnienia obowiązku z art. 17 ust. 4 lit. b i c dyrektywy DSM³⁷.

Rząd polski zarzucał postanowieniom dyrektywy, że w celu uniknięcia odpowiedzialności platformy internetowe zobowiązane do jej stosowania będą musiały automatycznie weryfikować (filtrować) treści zamieszczane przez użytkowników pod kątem potencjalnych naruszeń prawa autorskiego.

³² Haszowanie to technika polegająca na przekształcaniu pliku w łańcuch liczb zwany „wartością skrótu”. Ta wartość skrótu pozwala zidentyfikować treści zamieszczone przez użytkownika, a tym samym wykryć treści potencjalnie nieobjęte zezwoleniem. Według niektórych opinii wykrywanie przy pomocy tej techniki nieobjętych zezwoleniem treści działa wtedy, gdy zamieszczony plik jest identyczny z utworem, który został „poddany haszowaniu”, podczas gdy w przypadku cyfrowego odcisku palca można nawet rozpoznać różnice.

³³ Znak wodny to rozwiązanie polegające na tym, że oryginalny plik jest „opatrzone znakiem wodnym”, a zatem może być rozpoznany po zamieszczeniu go na serwerze na podstawie tego znaku wodnego, który działa jak podpis.

³⁴ Wykorzystanie metadanych pozwala na śledzenie, czy dany utwór został zamieszczony na podstawie metadanych powiązanych z treścią, takich jak nazwisko autora, tytuł utworu.

³⁵ Wyszukiwanie według słów kluczowych było wymieniane w szczególności jako rozwiązanie dla mniejszych dostawców usług, którzy mogą nie mieć środków na wdrażanie bardziej złożonych i kosztownych technologii. Jest to najprostsza technika polegająca na tym, że w ramach usługi ręcznie przeszukuje się stronę internetową, aby znaleźć tytuł np. danego utworu/wykonawcy w celu wykrycia treści potencjalnie naruszających prawo autorskie.

³⁶ Wytyczne do art. 17 dyrektywy DSM, pkt 2.

³⁷ Tamże, pkt 2.

A to wraz z obowiązkiem wprowadzenia mechanizmów kontroli prewencyjnej nie spełnia wymogu proporcjonalności i tym samym narusza prawo do wolności słowa³⁸. Rzeczpospolita Polska twierdziła ponadto, że prawodawca Unii nie może zrzec się odpowiedzialności za tę ingerencję w prawo zagwarantowane w art. 11 Karty, ponieważ jest ona nieuniknioną, a nawet przewidzianą przez instytucje Unii konsekwencją systemu odpowiedzialności ustanowionego w art. 17 ust. 4 dyrektywy 2019/790³⁹.

Trybunał potwierdził, że przewidziany w art. 17 dyrektywy DSM nowy reżim odpowiedzialności ingeruje w wolność wypowiedzi i informacji przez użytkowników usług udostępniania treści, zagwarantowane w art. 11 KPP oraz w art. 10 Konwencji o ochronie praw człowieka i podstawowych wolności⁴⁰. Nie spowodowało to jednak uwzględnienia skargi i nie doprowadziło do stwierdzenia nieważności art. 17 ust. 4 dyrektywy DSM. Trybunał podkreślił, że ani pozwane instytucje, ani interwenienci nie byli w stanie wskazać na rozprawie przed Trybunałem ewentualnych alternatyw dla takich narzędzi⁴¹. W konsekwencji Trybunał uznał, że dostawcy usług są zmuszeni do prewencyjnego filtrowania i blokowania rozpatrywanych treści⁴². Z tego powodu prawodawca unijny zamiast bezpośrednio przewidzieć obowiązek wprowadzenia takich narzędzi, narzucił je pośrednio, za pomocą przesłanek wyłączenia odpowiedzialności przewidzianych w tych przepisach⁴³.

Oddalając skargę Polski, TSUE zauważył, że art. 17 dyrektywy 2019/790 zawiera pełny system gwarancji, który chroni prawo do wolności wypowiedzi i informacji użytkowników usług udostępniania treści online oraz zachowuje sprawiedliwą równowagę między wchodzącymi w grę prawami i interesami⁴⁴.

³⁸ K. Żaczekiewicz-Zborska, *TSUE: Wolność słowa i prawo do informacji w sieci – zapewnione w dyrektywie*, 26.04.2022, <https://www.prawo.pl/prawo/wolnosc-slowa-i-prawo-do-informacji-w-sieci-zapewnione-w-514835.html> (dostęp: 15.10.2023).

³⁹ Wyrok TS w sprawie RP przeciwko PE i Radzie, pkt 42.

⁴⁰ Tamże, pkt 58. TSUE wskazał, że „Należy zatem stwierdzić, że odrębny system odpowiedzialności wprowadzony w art. 17 ust. 4 dyrektywy 2019/790 w odniesieniu do dostawców usług udostępniania treści online zawiera ograniczenie wykonywania prawa do wolności wypowiedzi i informacji użytkowników tych usług udostępniania, zagwarantowanego w art. 11 Karty”.

⁴¹ K. Gliściński, *Gwarancje...*, s. 28–36.

⁴² Tamże, s. 29.

⁴³ Opinia Rzecznika Generalnego w sprawie RP przeciwko PE i Radzie, cyt. za: K. Gliściński, *Gwarancje...*, s. 29.

⁴⁴ Wyrok TS w sprawie RP przeciwko PE i Radzie, pkt 62.

TSUE podkreślił, że w art. 17 przewidziano szczególny system zezwoleń i odpowiedzialności dotyczący praw autorskich i praw pokrewnych („prawa autorskie”), który ma zastosowanie do niektórych dostawców usług społeczeństwa informacyjnego określonych zgodnie z art. 2 pkt 6 dyrektywy jako dostawcy usług udostępniania treści online. W poprzednich obowiązujących ramach prawnych⁴⁵ nie było jasne, czy ci dostawcy usług ponoszą odpowiedzialność w zakresie praw autorskich za czynności wykonywane przez swoich użytkowników. Artykuł 17 zapewnia pewność prawa co do tego, czy dostawcy usług udostępniania treści online wykonują czynności regulowane prawem autorskim w związku z czynnościami wykonywanymi przez swoich użytkowników, a także zapewnia pewność prawa użytkownikom⁴⁶.

Niezależnie od argumentacji wskazanej przez polski rząd w skardze do TSUE, zauważyć trzeba, że zaproponowany w art. 17 dyrektywy DSM model wyważania praw interesów trzech grup podmiotów, tj. uprawnionych z tytułu praw wyłącznych, dostawców usług udostępniania treści online i użytkowników internetu, zasadza się na stosowaniu środków ochrony prewencyjnej. Konstrukcja tego modelu zawiera domniemanie uchylenia bezprawności działania dostawców usług, którzy stosując środki prewencyjne jak w szczególności monitorowanie treści, filtrowanie, wstrzymywanie publikacji ze względu na podejrzenie naruszenia albo przeświadczenie o tym, że do takiego naruszenia doszło, ingerują w wolność wypowiedzi użytkowników internetu. Wystarczającą przesłanką usprawiedliwiającą ingerencję w wolność wypowiedzi użytkowników internetu – zgodnie z mechanizmem ustalonym w art. 17 dyrektywy DSM – jest rodzaj świadczonej usługi, tj. udostępnianie treści online. Konstrukcja ta przypomina immunitet materialny. Ustawodawca europejski przesądził bowiem, że niedopuszczalne jest postawienie dostawcom usługi udostępniania treści online zarzutu ingerencji w wolność wypowiedzi już tylko z tego powodu, że głównym przedmiotem ich działalności jest udostępnianie, w celach zarobkowych, dużej ilości treści online.

Bezsporne pozostaje zarazem, że zastosowany w art. 17 dyrektywy DSM mechanizm ingeruje w wolność wypowiedzi użytkowników internetu,

⁴⁵ Art. 3 dyrektywy 2001/29/WE i art. 14 dyrektywy 2000/31/WE.

⁴⁶ Wyrok TS w sprawie RP przeciwko PE i Radzie.

co przyznał zarówno Rzecznik Generalny w sporządzonej opinii⁴⁷, a stanowisko to podzieliła Komisja Europejska w wytycznych do art. 17 oraz potwierdził TSUE w wyroku oddalającym skargę Rzeczypospolitej Polskiej. W ocenie Rzecznika Generalnego „prawodawca Unii mógł zgodnie z prawem zastąpić nową równowagą tę, którą wdrożył pierwotnie”⁴⁸. Prawodawca Unii podjął polityczną decyzję na korzyść twórczych sektorów. Uznał on, że wcześniejsza równowaga pomiędzy wchodzącymi w grę prawami i interesami nie jest już zadowalająca i że w celu dalszego zapewnienia podmiotom uprawnionym wysokiego poziomu ochrony należy ustanowić nowy system odpowiedzialności w odniesieniu do niektórych dostawców usług „Web 2.0”, nakładając na nich pewne obowiązki nadzorowania treści umieszczanych online przez użytkowników ich usług. Biorąc pod uwagę szeroki zakres uznania przysługujący prawodawcy, Rzecznik ocenił, że taki wybór nie jest co do zasady nieproporcjonalny.

K. Gliściński wskazuje, że jedno z podstawowych zagadnień, wokół którego toczyło się postępowanie przed Trybunałem, dotyczyło tego, czy ochrona praw podstawowych użytkowników ma być wzięta pod uwagę uprzednio (gwarancje *ex ante*), tj. przed zastosowaniem filtrowania i blokowania (usuwania) treści, czy jedynie następnie (gwarancje *ex post*), tj. dopiero po zablokowaniu (usunięciu) konkretnej treści na skutek skorzystania z gwarancji proceduralnych polegających na składaniu skarg i dochodzeniu roszczeń przewidzianych w art. 17 ust. 9 dyrektywy DSM⁴⁹. W opinii Rzecznika Generalnego obowiązuje przedstawiona przez Parlament, Radę i Komisję wykładnia, zgodnie z którą prawa użytkowników należy brać pod uwagę *ex ante*, a nie tylko *ex post*. Tylko bowiem taka wykładnia zapewnia proporcjonalność ograniczenia w korzystaniu z prawa do wolności wypowiedzi⁵⁰. Pod tym względem prawdą jest, że mechanizm składania skarg i dochodzenia roszczeń, o którym mowa w art. 17 ust. 9 dyrektywy 2019/790, stanowi jednocześnie zasadniczą gwarancję, stanowiąc konieczny składnik każdego systemu filtrowania z uwagi na wynikające z tego działania ryzyko „nadmiernego blokowania”. Jednakże o ile te gwarancje proceduralne są istotne, o tyle nie są one same w sobie wystarczające do zapewnienia „właściwej równowagi” między prawem

⁴⁷ Opinia Rzecznika Generalnego w sprawie RP przeciwko PE i Radzie, pkt 101.

⁴⁸ Tamże, pkt 132.

⁴⁹ K. Gliściński, *Gwarancje...*, s. 28–36.

⁵⁰ Opinia Rzecznika Generalnego w sprawie RP przeciwko PE i Radzie, pkt 177.

autorskim a wolnością wypowiedzi użytkowników⁵¹. W opinii Rzecznika istnienie takich gwarancji proceduralnych nie zwalnia organów władzy publicznej z zadbania o to, aby zminimalizować skutek uboczny środka filtrowania i blokowania. Wszystkie środki filtrowania i blokowania muszą być „ściśle ukierunkowane” w tym znaczeniu, że powinny dotyczyć nielegalnych treści i nie mogą mieć arbitralnego lub nadmiernego wpływu na treści zgodne z prawem⁵². Środki nadzoru, do których stosowania pośrednik jest zobowiązany, nie mogą tworzyć przeszkód w zgodnym z prawem korzystaniu z jego usług⁵³. Trybunał orzekł, że środek blokujący nie może „niepotrzebnie [pozbawiać]” internautów możliwości zgodnego z prawem udostępniania informacji i dostępu do nich⁵⁴. Rzecznik, powołując się na orzecznictwo ETPC, podkreśla, że nie można w społeczeństwie demokratycznym wymagać absolutnej skuteczności – a więc „zerowego ryzyka”⁵⁵ ewentualnego naruszenia praw autorskich, jeżeli skutkowałoby to zablokowaniem znacznej ilości zgodnych z prawem treści⁵⁶. Prewencyjna blokada wszystkich treści zwielokrotniających utwory i inne przedmioty objęte ochroną wskazane przez podmioty uprawnione skutkowałaby tym, że użytkownicy ponosiliby w sposób systematyczny konsekwencje beczynności, ponieważ rozpowszechnianie zgodnych z prawem treści nie mogłoby nastąpić bez – zakońzonego sukcesem – wniesienia przez nich skargi. Gdyby użytkownicy ci musieli systematycznie dochodzić przysługujących im praw w ramach mechanizmu składania skarg, jest wysoce prawdopodobne, że znaczna część z nich zrezygnowałaby z uczynienia tego, w szczególności z uwagi na brak wystarczającej wiedzy, aby ocenić, czy wykorzystanie tych przedmiotów jest zgodne z prawem i czy w związku z tym istnieją podstawy do wniesienia takiej skargi. Prewencyjne „nadmierne blokowanie” każdego zgodnego z prawem wykorzystania i systematyczne przerzucenie na użytkowników ciężaru wykazania tej zgodności z prawem mogłyby w ten sposób doprowadzić, w krótkim lub długim okresie,

⁵¹ Tamże, pkt 180.

⁵² Wyroki TS: w sprawie UPC Telekabel Wien, pkt 56; w sprawie Tobias Mc Fadden przeciwko Sony Music Entertainment Germany GmbH, pkt 93.

⁵³ Wyrok TS w sprawie L'Oréal przeciwko eBay, pkt 131.

⁵⁴ Wyrok TS w sprawie UPC Telekabel Wien, pkt 63.

⁵⁵ Opinia Rzecznika Generalnego w sprawie RP przeciwko PE i Radzie, pkt 184.

⁵⁶ Wyroki ETPC: w sprawie Ahmet Yildirim przeciwko Turcji, § 66; w sprawie Kharitonov przeciwko Rosji, § 45; a także w sprawie Kablis przeciwko Rosji, § 94.

do *chilling effect* w stosunku do wolności wypowiedzi i twórczości, przekładającego się na spadek aktywności tych użytkowników⁵⁷.

Nadto Rzecznik dostrzega, że jakkolwiek usługodawcy będący pośrednikami są z technicznego punktu widzenia dobrze przygotowani do zwalczania obecności pewnych informacji niezgodnych z prawem rozpowszechnianych za pośrednictwem ich usług, to jednak nie można od nich oczekiwać, że dokonają „niezależnej oceny” zgodności z prawem rozpatrywanych informacji. Ci będący pośrednikami usługodawcy zazwyczaj nie posiadają fachowej wiedzy, a przede wszystkim koniecznej niezależności – *a fortiori*, gdy ciąży nad nimi groźba wielkiej odpowiedzialności. Nie można zatem uczynić ich arbitrami zgodności z prawem online, odpowiedzialnymi za rozstrzyganie złożonych kwestii prawnych. W konsekwencji, aby zminimalizować ryzyko „nadmiernego blokowania”, a tym samym zagwarantować poszanowanie prawa do wolności wypowiedzi, usługodawca będący pośrednikiem powinien być zobowiązany jedynie do filtrowania i blokowania informacji, których niezgodność z prawem została wcześniej stwierdzona przez sąd lub, w innym przypadku, informacji, których bezprawny charakter „nasuwa się od razu”, to znaczy w sposób oczywisty, bez, w szczególności, konieczności rozważania ich kontekstu⁵⁸.

Powyższe argumenty przemawiają za zastosowaniem ochrony wolności wypowiedzi użytkowników zgodnie z systemem *ex ante*, a zatem przed zastosowaniem przez dostawców usług udostępniania treści online systemów filtrujących i blokowaniem treści. Zaakceptowanie takiego stanowiska nakłada na krajowego ustawodawcę – jak zauważa K. Gliściński – obowiązek uwzględnienia, w toku implementacji dyrektywy DSM, ustanowienia skonkretyzowanego systemu gwarancji *ex ante*. Oznacza to, że państwa członkowskie powinny zapewnić w swoim ustawodawstwie, aby treści umieszczone zgodnie z prawem nie były blokowane przez dostawców usług udostępniania treści online przed wydaniem rozstrzygnięcia w tym zakresie przez niezależny organ⁵⁹. Nadto wymagana w dyrektywie współpraca między dostawcami usług udostępniania treści internetowych a podmiotami uprawnionymi nie może

⁵⁷ Opinia Rzecznika Generalnego w sprawie RP przeciwko PE i Radzie, pkt 187.

⁵⁸ Tamże, pkt 197 i 198.

⁵⁹ K. Gliściński, *Gwarancje...*, s. 28–36.

prowadzić do uniemożliwiania dostępności utworów lub innych przedmiotów objętych ochroną zamieszczanych przez użytkowników, które nie naruszają prawa autorskiego i praw pokrewnych, w tym również w przypadku, gdy takie utwory lub inne przedmioty objęte ochroną są objęte wyjątkiem lub ograniczeniem. Państwa członkowskie powinny zatem zapewnić, aby użytkownicy internetu mogli opierać się co najmniej na następujących obowiązujących wyjątkach lub ograniczeniach przy zamieszczaniu i udostępnianiu treści: a) cytowanie, krytyka, recenzowanie; b) korzystanie do celów karykatury, parodii lub pastiszu⁶⁰.

Zagwarantowanie skutecznych zabezpieczeń przed nadmiernym blokowaniem treści spoczywa zatem na każdym państwie członkowskim z osobna. Przyjęte rozwiązania powinny gwarantować, by – po pierwsze – prywatne podmioty, jakimi są dostawcy usług, nie decydowały arbitralnie o zgodności bądź niezgodności z prawem treści przekazanych przez użytkowników internetu i – po drugie – państwo powinno zadbać o symetrię (równowagę) w zakresie korzystania z wolności wypowiedzi, która mogłaby zostać zakłócona, gdyby postanowienia dyrektywy DSM zostały wprost inkorporowane do polskiego porządku prawnego bez zawartego w ustawie systemu dodatkowych (nowych) gwarancji wolności wypowiedzi dla użytkowników internetu. W konsekwencji dostawcy usług nie powinni mieć możliwości dowolnego ustalania przez siebie parametrów systemów filtrujących, które będą decydować o tym, jakie treści zostaną rozpowszechnione. Gwarancje te muszą zarazem być konkretne i stanowcze adekwatnie do ryzyka naruszenia praw podstawowych powstałego ze względu na ustalony w art. 17 dyrektywy DSM szczególny mechanizm odpowiedzialności dostawców usług dostarczania treści online⁶¹.

⁶⁰ Opinia Rzecznika Generalnego w sprawie RP przeciwko PE i Radzie.

⁶¹ Szczegółową analizę zakresu i proponowanych w doktrynie sposobów implementacji dyrektywy DSM przeprowadził K. Gliściński (zob. K. Gliściński, *Gwarancje...*). Autor zauważa, że propozycje implementacji dyrektywy DSM (Projekt ustawy o zmianie ustawy o prawie autorskim i prawach pokrewnych oraz niektórych innych ustaw, <https://legislacja.rcl.gov.pl/projekt/12360954/katalog/12887995#12887995> oraz <https://legislacja.rcl.gov.pl/docs//2/12360954/12887989/12887990/dokument588064.pdf> dostęp: 16.08.2023) nie tylko nie przewiduje żadnych gwarancji *ex ante*, lecz także nawet nie dokonuje literalnej implementacji art. 17 ust. 7 dyrektywy DSM. Zgodzić się należy z postulatami K. Gościńskiego odnośnie do sposobu implementacji i jej zakresu, w szczególności potrzeby stworzenia krajowych ram regulacyjnych, które spowodują,

B. Przeciwdziałanie treściom nielegalnym

Celem rozwiązań przyjętych w AUC jest, jak wskazano w art. 1 ust. 1 tego rozporządzenia, stworzenie „bezpiecznego, przewidywalnego i budzącego zaufanie środowiska internetowego”⁶². Nie jest jasne, w jaki sposób PE definiuje pojęcie bezpieczeństwa, a zatem czy na gruncie AUC należy identyfikować to pojęcie z bezpieczeństwem publicznym (brak zagrożenia w ujęciu obiektywnym) czy z bezpieczeństwem indywidualnym (brak zagrożenie w odczuciu jednostki) a nadto czy ujmuje je jako stan proces społeczny, wartość, czy potrzebę. Nie jest zarazem pewne, w jaki sposób należy rozumieć termin „środowisko internetowe”. Na próżno szukać definicji legalnych tych terminów w treści rozporządzeń cyfrowych.

Wykładnia tych pojęć, dokonywana na podstawie treści wniosków KE do PE w sprawie rozporządzeń cyfrowych⁶³, dowodzi, że prawodawca europejski nadaje tym terminom kontekst ogólnospołeczny i niezindywidualizowany⁶⁴. Jednakże w wyjaśnieniach adresowanych do opinii publicznej, publikowanych na stronach internetowych organów UE, prawodawca europejski wyjaśnia, że jego celem było zapewnienie bezpieczeństwa obywateli UE w wymiarze indywidualnym, w tym praw podstawowych, praw konsumentów oraz zagwarantowanie pewności prawa i uczciwej konkurencji dla przedsiębiorców. Wskazano zatem, że „Akt o usługach cyfrowych wraz z aktem o rynkach cyfrowych tworzą pakiet dotyczący usług cyfrowych, który ma zapewnić użytkownikom cyfrowym dostęp do bezpiecznych produktów i chronić prawa podstawowe użytkowników umożliwić wolną i uczciwą konkurencję w sektorach cyfrowych pobudzającą innowacyjność i wzrost”⁶⁵.

że stosowane przez dostawców usług algorytmy będą zaprojektowane tak, aby zapobiegać i minimalizować naruszenia praw podstawowych, takich jak prawo do wolności wypowiedzi, poprzez domyślną ochronę wyjątków i ograniczeń.

⁶² Omówienie Aktu o usługach cyfrowych, Baza aktów prawnych Unii Europejskiej, <https://eur-lex.europa.eu/PL/legal-content/summary/digital-services-act.html> (dostęp: 21.11.2023).

⁶³ Wniosek AUC oraz Wniosek ARC.

⁶⁴ W treści wniosku w sprawie AUC termin „bezpieczeństwo” jest wprost używany z dookreśleniem „publiczne” (Wniosek AUC, s. 17, 36, 38, 46, 74).

⁶⁵ Akt o usługach cyfrowych, <https://www.consilium.europa.eu/pl/policies/digital-services-act/> (dostęp: 21.11.2023). Podobnie na stronach Parlamentu Europejskiego wskazuje się, że „Akt o usługach cyfrowych chroni prawa i interesy wszystkich zainteresowanych

Im bliżej daty, od której AUC zaczną być stosowane we wszystkich Państwach Członkowskich UE⁶⁶, tym bardziej precyzyjnie i jednoznacznie organy UE dokonują wykładni (wykładnia autentyczna) motywów, jakimi kierowano się, uchwalając rozporządzenia cyfrowe. Wskazuje się zatem, że „Akt o usługach cyfrowych jest pierwszą na świecie regulacją cyfrową, która nakłada na firmy cyfrowe w całej UE odpowiedzialność za treści zamieszczane na ich platformach”, a nadto, że ma on na celu „zabezpieczenie unijnego internetowego środowiska informacyjnego”⁶⁷. Oznacza to, że celem i istotą rozporządzeń cyfrowych jest, w pierwszej kolejności, zwalczanie nielegalnych treści oraz przeciwdziałanie nielegalnym treściom (fałszywym informacjom, propagandzie, nawoływaniu do nienawiści, molestowaniu i niegodziwemu traktowaniu dzieci w celach seksualnych), szybkie reagowanie na te treści i umożliwianie użytkownikom ich sygnalizowania, a także stosowanie narzędzi moderowania treści, które obejmują możliwość zaskarżania decyzji o usunięciu treści zamieszczonych przez użytkowników lub o ograniczeniu dostępu do nich⁶⁸.

Realizacja powyższych celów stanowi *per se* ingerencję w wolność wypowiedzi użytkowników internetu. Dopuszczalność ingerencji jest uwarunkowana wykazaniem przesłanki „nielegalności” treści.

Zagrożenie dla realizacji wolności wypowiedzi może stanowić zarówno nadmiernie szeroka definicja „treści nielegalnych”, jak i rodzaj zastosowanych środków ochrony, a także mechanizm ich stosowania i egzekwowania.

stron, w szczególności obywateli UE, poprzez zwalczanie nielegalnych treści online, w tym towarów i usług, głównie przez: 1) oferowanie większej kontroli nad tym, co użytkownicy widzą w internecie, oraz zapewnienie im dokładniejszych informacji o wyświetlanych reklamach, 2) oferowanie możliwości łatwego znakowania nielegalnych treści lub produktów, mowy nienawiści i dezinformacji, 3) zapewnienie platformom środków do współpracy z „zaufanymi podmiotami sygnalizującymi” oraz 4) nałożenie obowiązków w zakresie identyfikowalności przedsiębiorców na internetowych platformach handlowych; zob. Akt o usługach cyfrowych – omówienie, <https://eur-lex.europa.eu/PL/legal-content/summary/digital-services-act.html> (dostęp: 22.11.2023).

⁶⁶ Zgodnie z art. 93 ust. 2 AUC zaczną być stosowane w UE począwszy od 17.02.2024 r.

⁶⁷ Motyw 3 Zalecenie Komisji (UE) 2023/2425 z dnia 20 października 2023 r. w sprawie koordynacji reakcji na incydenty wynikające w szczególności z rozpowszechniania nielegalnych treści, zanim rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 (akt o usługach cyfrowych) zaczną być w pełni stosowane (Dz.U. UE L, s. 2425).

⁶⁸ Akt o usługach cyfrowych, <https://www.consilium.europa.eu/pl/policies/digital-services-act/> (dostęp: 21.11.2023).

Pojęcie nielegalnych treści i jego wykładnia, a przede wszystkim to, jaki podmiot (organ) jest upoważniony do dokonywania wiążącej wykładni tego pojęcia, ma kluczowe znaczenie dla standardu wolności wypowiedzi na jednolitym rynku cyfrowym. O ile na gruncie AUC i ARC przyjęto, że „to, co jest nielegalne poza internetem, jest również nielegalne w internecie”⁶⁹, to jednak sposoby, środki i tryb zwalczania nielegalnych treści w internecie i poza nim są całkowicie odmienne. W efekcie standardy wolności wypowiedzi w internecie i poza nim nie są tożsame. Przeciwnie, w internecie powstaje odwrócony standard, który charakteryzuje się przede wszystkim tym, że przyzwala na prewencyjną ingerencję w wolność wypowiedzi, a nadto istotnie ogranicza zobiektywizowaną ocenę „nielegalności”, zastępując ją oceną uznaniową dokonywaną przez podmioty prywatne (strażników dostępu), a w dodatku modyfikuje przesłanki służące legalnemu weryfikowaniu wypowiedzi i jej kwalifikowania do kategorii legalnych albo nielegalnych. Nielegalne mogą być bowiem wypowiedzi ze względu na ich treść lub formę, co wydaje się oczywiste, jednakże trzeba zwrócić uwagę, że nielegalny może być także proces ich kwalifikowania i oceny. Nie jest zarazem dopuszczalne, by dokonać prawidłowej kwalifikacji wypowiedzi, jeśli zastosowany tryb jest wadliwy. Tryb ten nie powinien być zatem dowolny, a jego stosowanie winno opierać się o zobiektywizowane, jednolite przesłanki.

Jeśli zatem poza internetem standard wolności wypowiedzi był budowany na podstawie przesłanek zawartych w art. 10 EKPC oraz, jak to ma miejsce w przypadku Polski, postanowień Konstytucji normujących granice wprowadzania ograniczeń praw i wolności (art. 31 ust. 3 Konstytucji RP), to przy założeniu, że standardy w internecie i poza internetem są tożsame, należałoby utrzymać zarówno mechanizm, jak i przesłanki dokonywania oceny dopuszczalności ingerencji w wolność wypowiedzi. Chodzi zatem o stosowanie tzw. testu szkodliwości wypracowanego na gruncie art. 10 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności i art. 54 ust. 1 w zw. z art. 31 ust. 3 Konstytucji RP. Mechanizm ten, jak wskazywano we

⁶⁹ Opinia Europejskiego Komitetu Regionów – Akt o usługach cyfrowych i akt o rynkach cyfrowych (Dz.U. UE C z 2021 r. Nr 440, s. 67), https://sip.lex.pl/#/act/69490030/3007948/opinia-europejskiego-komitetu-regionow-akt-o-uslugach-cyfrowych-i-akt-o-rynkach-cyfrowych?keyword=%22akt%20o%20rynkach%20cyfrowych%22&unitId=passage_1042 (dostęp: 19.08.2023) – poprawka 7.

wcześniejszych fragmentach niniejszej pracy, pozwala na usprawiedliwienie ograniczenia wolności wypowiedzi tylko wówczas, gdy – po pierwsze – ograniczenie było przewidziane w ustawie i – po drugie – ograniczenie służy ochronie innej równoważnej wartości i jest uzasadnione istnieniem pilnej społecznie potrzeby udzielenia takiej ochrony oraz – po trzecie – zastosowane środki ingerencji i ich intensywność są proporcjonalne, co oznacza, że nie są nadmierne, nie wywołują efektu mrozącego (ang. *chilling effect*), są bowiem usprawiedliwione ze względu na cel, jakiemu służą. Nadto ocena zasadności i intensywności ingerencji w wolność wypowiedzi jest domeną niezawisłych sądów przy założeniu, że w sferze ochrony praw i wolności status podmiotów pozostających ze sobą w sporze, tj. pokrzywdzonego i naruszydiciela, opiera się na zasadzie równoprawności stron. Zważywszy jednocześnie, że wolność wypowiedzi ma charakter wolności osobistej, ingerencja w to dobro jest objęta domniemaniem bezprawności działania naruszydiciela.

W środowisku cyfrowym, jak wskazuje analiza AUC i ARC, przyjęto odmienne założenia. Uznano zatem – po pierwsze – że istnieje wartość nadrzędna w stosunku do wolności wypowiedzi i jest nią „bezpieczeństwo internetowego środowiska informacyjnego”⁷⁰, po drugie – założono, że ingerencja w wolność wypowiedzi może być nie tylko w pewnych okolicznościach usprawiedliwiona, ale ponadto staje się obowiązkiem ciążącym na podmiotach publicznych, oraz – po trzecie – skoro ingerencja w wolność wypowiedzi staje się obowiązkiem podmiotów publicznych, to domniemywa się, że jest ona zgodna z prawem, po czwarte – wystarczającą przesłanką usprawiedliwiającą ingerencję jest ustalenie ich „nielegalności”, przyjmując jednocześnie, że ocenę tę oprzeć można – jak wskazano w motywie 63 AUC – na ustaleniu, że „dla osoby nieposiadającej wiedzy fachowej jest oczywiste, bez przeprowadzenia jakiegokolwiek merytorycznej analizy, że treści są nielegalne”. Obok zatem kategorii „nielegalnych treści” wyróżniono kategorię „oczywiście nielegalnych treści”, a ustalenie wystąpienia przesłanki „nielegalności” odniesiono do wzorca przeciętnego odbiorcy.

⁷⁰ Motyw 3 Zalecenie Komisji (UE) 2023/2425 z dnia 20 października 2023 r. w sprawie koordynacji reakcji na incydenty wynikające w szczególności z rozpowszechniania nielegalnych treści, zanim rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 (akt o usługach cyfrowych) zacznie być w pełni stosowane (Dz.U. UE L, s. 2425).

Na gruncie AUC uznano zatem *a priori*, że istnieją treści, które są pierwotnie nielegalne, a ustalenie istnienia tej okoliczności nie wymaga posiadania wiedzy fachowej ani zachowania bezstronności, w szczególności nie wymaga się, by oceny tej dokonywał niezawisły sąd. Fakt wykrycia nielegalnej treści powiązany z obowiązkiem podjęcia reakcji, której skutkiem ma być usunięcie lub zablokowanie treści. Zakres ingerencji jest uwarunkowany intensywnością stopnia bezprawności treści, przy czym sama ingerencja sprowadzająca się do blokowania lub usuwania nielegalnych treści stanowi realizację obowiązków nałożonych na podmioty prywatne (pośrednicy internetowi, w tym strażnicy dostępu) i publiczne (państwa członkowskie, Komisja Europejska), a nie, jak na gruncie klasycznego modelu (standardu), efekt czynności służących równoważeniu, pozostających w konflikcie, praw i interesów, na których ochronę powołują się równoprawne podmioty.

Potrzeba zapewnienia bezpieczeństwa „internetowego środowiska informacyjnego” stanowi – w ocenie prawodawcy europejskiego – przesłankę uzasadniającą ingerencję w sferę praw i wolności jednostek, a nadto nakłada na organy publiczne obowiązek działania (obowiązek pozytywny) polegający na stosowaniu skutecznych środków usuwania i przeciwdziałania rozpowszechnieniu nielegalnych treści. Potrzeba zapewnienia bezpieczeństwa „internetowego środowiska informacyjnego” stanowi bowiem, w ujęciu rozwiązań zawartych w pakiecie cyfrowym, wartość nadrzędną, której naruszenie lub zakłócenie, jak się sugeruje, może zostać zakwalifikowane, na gruncie art. 83 ust. 1 TFUE, jako szczególnie poważna przestępczość⁷¹ w wymiarze

⁷¹ Art. 83 ust. 1 TFUE przewiduje kompetencję do harmonizacji prawa karnego materialnego w dziesięciu wymienionych w nim obszarach, w drodze zwykłej procedury ustawodawczej. Określone w prawie UE normy minimalne mają dotyczyć definicji przestępstw i kar, natomiast wymienione obszary są szczególnie poważne i mają odniesienie transgraniczne. Komentowany przepis zezwala Radzie na podjęcie decyzji rozszerzającej listę – podstawą decyzji ma być ocena „rozwoju przestępczości” (A. Grzelak, *Artykuł 3*, [w:] *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz. Tom I (art. 1–89)*, t. 1, D. Miąsik, N. Półtorak, A. Wróbel (red.), Warszawa 2012, art. 83). Wymienione w art. 83 ust. 1 TFUE obszary to: terroryzm, handel ludźmi oraz seksualne wykorzystywanie kobiet i dzieci, nielegalny handel narkotykami, nielegalny handel bronią, pranie pieniędzy, korupcja, fałszowanie środków płatniczych, przestępczość komputerowa i przestępczość zorganizowana. Z akapitu drugiego tego przepisu wynika wprost, że „W zależności od rozwoju przestępczości Rada może przyjąć decyzję określającą inne dziedziny przestępczości spełniające kryteria, o których mowa w niniejszym ustępie. Rada stanowi jednomyślnie po uzyskaniu zgody Parlamentu Europejskiego”. A. Grzelak zauważa, że w art. 83 ust. 2

transgranicznym rodząca potrzebę wspólnego jej zwalczania w całej Unii. W konsekwencji nieingerowanie w treść wypowiedzi stanowić może naruszenia obowiązku działania wymaganego na gruncie pakietu cyfrowego od podmiotów publicznych. *A contrario* działanie, którego skutkiem jest ograniczenie wolności wypowiedzi, jeśli dotyczy treści nielegalnych, stanowi jedynie dowód tego, że organy działały zgodnie z zasadą należytej staranności. Akcent został zatem położony na usuwanie treści, a nie ich ochronę. Deliktem staje się nieusunięcie treści, a nie – jak było dotychczas – ich usuwanie lub blokowanie.

W zaleceniu Komisji z dnia 20 października 2023 r. w sprawie koordynacji reakcji na incydenty wynikające w szczególności z rozpowszechniania nielegalnych treści⁷² wskazano, że „Unia ustanowiła przełomowe przepisy mające na celu zabezpieczenie unijnego internetowego środowiska informacyjnego, które gwarantują swobodny dostęp do informacji, zwłaszcza w czasach konfliktu, ale które również wymagają podejmowania skutecznych reakcji na rozpowszechnianie nielegalnych treści w internecie i zagrożenia dla dyskursu obywatelskiego, wyborów i bezpieczeństwa”. W szczególności wskazano, że pośrednicy internetowi „muszą stosować środki przeciwdziałające ryzyku związanemu z rozpowszechnianiem nielegalnych treści w internecie, a także wprowadzić mechanizm umożliwiający użytkownikom sygnalizowanie nielegalnych treści oraz szybko podejmować działania w odpowiedzi na takie zgłoszenia”⁷³. W motywie 3 zalecenia zauważono zarazem, że rozporządzenie AUC nie przesądza, czy dany rodzaj treści kwalifikuje się jako nielegalne. O niezgodności treści z prawem decydują przepisy prawa krajowego lub, w zharmonizowanych obszarach, przepisy europejskie. W efekcie ocena dopuszczalności ingerencji w wolność wypowiedzi w internecie

TFUE nastąpiło wprowadzenie wyraźnej podstawy prawnej dla harmonizacji prawa karnego w celu zapewnienia skuteczności innym politykom UE. Przyjęcie art. 83 ust. 2 miało otworzyć możliwość harmonizacji znamion typów czynów zabronionych i kar w dziedzinach określonych w ramach innych polityk UE. W rezultacie artykuł 83 ust. 1 i 2 przyznają kompetencję nie tylko do harmonizacji znamion typów czynów zabronionych, lecz także kar. Oznacza to możliwość uregulowania obu kwestii – zwłaszcza w przypadku art. 83 ust. 2 – w jednym akcie prawnym (tamże).

⁷² Zalecenie Komisji (UE) 2023/2425 z dnia 20 października 2023 r. w sprawie koordynacji reakcji na incydenty wynikające w szczególności z rozpowszechniania nielegalnych treści, zanim rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 (akt o usługach cyfrowych) zacznie być w pełni stosowane (Dz.U. UE L, s. 2425).

⁷³ Tamże.

motywowana potrzebą usuwania lub blokowania nielegalnych treści będzie wymagała potwierdzenia ich nielegalnego charakteru na podstawie przepisów prawa europejskiego zabraniających rozpowszechniania treści określonego rodzaju, a także w aktach prawa krajowego państw członkowskich⁷⁴.

Brak przesądzenia w AUC o tym, jakie treści rozpowszechniane w internecie należy kwalifikować jako nielegalne, nie oznacza jednak, że termin „treści nielegalne” nie ma definicji legalnej, ponieważ ustawodawca europejski wskazał w art. 3 lit. h AUC, że termin „nielegalne treści” oznacza „informacje, które same w sobie lub przez odniesienie do działania, w tym sprzedaży produktów lub świadczenia usług, nie są zgodne z prawem Unii lub z prawem jakiegokolwiek państwa członkowskiego, które jest zgodne z prawem Unii, niezależnie od konkretnego przedmiotu lub charakteru tego prawa”. W motywie 12 AUC wyjaśniono, że aby osiągnąć cel zakładający zapewnienie bezpiecznego, przewidywalnego i godnego zaufania środowiska internetowego, do celów niniejszego rozporządzenia pojęcie nielegalnych treści powinno w szerokim zakresie odzwierciedlać istniejące przepisy w środowisku pozainternetowym. W szczególności pojęcie nielegalnych treści należy – jak wskazano w AUC – zdefiniować szeroko, tak by obejmowało informacje dotyczące nielegalnych treści, produktów, usług i działań. Pojęcie to należy rozumieć w szczególności jako odnoszące się do informacji, niezależnie od ich formy, które zgodnie z obowiązującym prawem są albo same w sobie nielegalne, takich jak nielegalne nawoływanie do nienawiści lub treści o charakterze terrorystycznym i niezgodne z prawem treści dyskryminujące, albo które stają się nielegalne na mocy obowiązujących przepisów ze względu na fakt, iż odnoszą się one do nielegalnych działań. Przykładowo może to być udostępnianie obrazów przedstawiających niegodziwe traktowanie dzieci w celach seksualnych, bezprawne udostępnianie prywatnych obrazów bez zgody, cyberstalking, sprzedaż produktów niespełniających wymogów lub podrobionych, sprzedaż towarów lub świadczenie usług z naruszeniem

⁷⁴ Mając powyższe na uwadze, należy przyjąć, że wszystkie regulacje normujące zarówno wprost prawa i obowiązki uczestników rynku cyfrowego, jak i te akty prawne, które są niezbędne do tego, by prawidłowo ustalić zakres pojęcia „nielegalne treści”, są ze sobą powiązane i tworzą „pakiet cyfrowy”. Termin „pakiet cyfrowy” jest używany w niniejszej rozprawie szeroko i obejmuje obok AUC i ARC także te akty prawne, które pozostają z nimi w związku podmiotowym lub przedmiotowym.

prawa ochrony konsumentów, nieuprawnione wykorzystanie materiałów chronionych prawem autorskim, nielegalne oferowanie usług zakwaterowania lub nielegalna sprzedaż żywych zwierząt. Z kolei film wideo naocznego świadka potencjalnego przestępstwa nie powinien być uważany za nielegalną treść tylko dlatego, że przedstawia on czyn zabroniony, w przypadku gdy nagrywanie lub rozpowszechnianie takiego filmu wśród ogółu społeczeństwa nie jest nielegalne na mocy prawa krajowego lub prawa Unii. W tym zakresie nie ma znaczenia, czy nielegalny charakter informacji lub działania wynika z prawa Unii, czy z prawa krajowego, które jest zgodne z prawem Unii, oraz jaki jest dokładny charakter lub przedmiot danego prawa.

Stwierdzenie, czy w odniesieniu do konkretnej wypowiedzi występuje przesłanka „nielegalności”, wymaga ustalenia tego, jakie konkretnie nakazy lub zakazy wyartykułowane w przepisach prawa UE albo prawa wewnętrznego państw członkowskich narusza wypowiedź „podejrzewana” o to, że zawiera nielegalne treści. Obszerność, złożoność oraz wielokierunkowość prawa UE generuje ryzyko, że zarzut „nielegalności” może zostać podniesiony wobec nawet tych treści, które na gruncie krajowych rozwiązań prawnych mieszczą się w granicach prawa⁷⁵. Jak zauważono w motywie 11 zalecenia

⁷⁵ Przykładowo wątpliwości budzić musi podstawa uchylenia przez Parlament Europejski czterem polskim parlamentarzystom, w tym Patrykowi Jakiemu, immunitetu poselskiego w związku z toczącym się – z oskarżenia prywatnego – przed Sądem Rejonowym dla Warszawy Mokotowa postępowaniem, w którym zarzucono parlamentarzystom, że w dniu 17 października 2018 r. w mediach społecznościowych – na portalu Twitter na stronie Prawa i Sprawiedliwości – poprzez polubienie wzięli udział w rozpowszechnieniu opublikowanego spotu wyborczego pod hasłem „Bezpieczny samorząd”. Spot był częścią kampanii wyborczej do samorządów lokalnych prowadzonej przez partię Prawo i Sprawiedliwość, której parlamentarzyści są członkami i z ramienia której kandydowali do PE. Parlamentarzystom zarzucono, że opublikowany spot miał zawierać treści wzywające do nienawiści wobec imigrantów muzułmańskich. W decyzji PE wskazano, że ważący dla podjęcia decyzji o uchyleniu immunitetu był fakt, że czyny zarzucane Patrykowi Jakiemu nie dotyczą opinii lub stanowiska zajętego przez niego w głosowaniu w czasie wykonywania obowiązków posła do Parlamentu Europejskiego w rozumieniu art. 8 Protokołu nr 7 w sprawie przywilejów i immunitetów Unii Europejskiej; mając na uwadze, że w przedmiotowej sprawie wniosek o uchylenie immunitetu dotyczy okoliczności faktycznych związanych z działaniami o charakterze lokalnym prowadzonymi przed uzyskaniem statusu, a w konsekwencji immunitetu posła do PE; zob. Sprawozdanie w sprawie wniosku o uchylenie immunitetu Patryka Jakiego, https://www.europarl.europa.eu/doceo/document/A-9-2023-0345_PL.html (dostęp: 15.10.2023). Postępowanie sądowe stanowiące przyczynę uchylenia immunitetu PE należałoby ocenić w szczególności na gruncie rozwiązań zawartych w świetle treści Wniosku KE z dnia

z 20 października 2023 r., istnieje wiele aktów prawa Unii przewidujących ramy prawne mające zastosowanie do niektórych szczególnych rodzajów nielegalnych treści, które są przedstawiane i rozpowszechniane w internecie, oraz harmonizuje to, co należy uznać za nielegalne w całej Unii. Właśnie mnogość przepisów UE stanowiła dla prawodawcy europejskiego argument na uzasadnienie potrzeby pełnej harmonizacji przepisów służących zwalczaniu nielegalnych treści oraz wyboru rozporządzeń jako najbardziej odpowiedniego instrumentu regulacji. Nadto Komisja Europejska podjęła działania na rzecz poszerzenia zawartego w art. 83 TFUE katalogu europrzestępstw, opowiadając się za tym, by rozpowszechnianie niektórych kategorii „nielegalnych treści”, w szczególności tzw. mowy nienawiści, zostało zaliczone do kategorii poważnych przestępstw o charakterze transgranicznym, co otwierałoby organom UE drogę do definiowania znamion tego przestępstwa oraz ustalania rodzaju i rozmiarów kary⁷⁶.

27 kwietnia 2022 r. Dyrektywa Parlamentu Europejskiego i Rady w sprawie ochrony osób, które angażują się w debatę publiczną, przed ewidentnie bezpodstawnymi lub stanowiącymi nadużycie postępowaniami sądowymi („strategiczne powództwa zmierzające do stłumienia debaty publicznej”; <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52022PC0177> dostęp: 15.10.2023). W projekcie dyrektywy wskazuje się, że ewidentnie bezpodstawne lub stanowiące nadużycie postępowania sądowe zmierzające do stłumienia debaty publicznej (często określane również mianem strategicznych powództw zmierzających do stłumienia debaty publicznej lub „SLAPP”) są zjawiskiem obserwowanym w Unii Europejskiej od niedawna, ale wraz z upływem czasu stają się coraz powszechniejsze. Stanowią one szczególnie szkodliwą formę nękania i zastraszania stosowaną przeciwko osobom działającym na rzecz ochrony interesu publicznego. Celem wniosku jest zapewnienie ochrony osobom, przeciwko którym wytacza się powództwa typu SLAPP, a także zapobieżenie dalszemu szerzeniu się tego zjawiska w UE.

⁷⁶ Komisja Europejska postuluje poszerzenie dziedziny przestępczości wymienionych w art. 83 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) o nową dziedzinę, tj. przestępstwa z nienawiści i mowę nienawiści. Komisja Europejska wnosi, by „nienawiść wobec osób lub grup posiadających (lub postrzeganych jako posiadające) cechy objęte ochroną oraz nawoływanie do nienawiści i przestępstwa z nienawiści uznać za dziedzinę przestępczości w rozumieniu art. 83 ust. 1 TFUE”; zob. Komunikat Komisji do Parlamentu Europejskiego i Rady z dnia 9 grudnia 2021 r., Bardziej inkluzywna i bezpieczna Europa: rozszerzenie wykazu przestępstw UE o nawoływanie do nienawiści i przestępstwa z nienawiści, <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52021DC0777&from=IT> (dostęp: 15.10.2023). Realizacja tego postulatu oznacza poszerzenie katalogu tzw. europrzestępstw o nową dziedzinę, a w konsekwencji umożliwi instytucjom UE wydawanie aktów prawnych ustanawiających normy minimalne odnoszące się do określania znamion typów i kategorii przestępstw z nienawiści i mowy nienawiści, a w efekcie dokonywania kwalifikacji określonych zachowań jako wyczerpujących znamiona przestępstw,

Jak wspomniano w zaleceniu z 20 października 2023 r., do kategorii „nielegalnych treści” należy zaliczyć co najmniej te wypowiedzi, których sankcjonowanie przewidują dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 w sprawie zwalczania terroryzmu⁷⁷, rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym⁷⁸, a także decyzja ramowa Rady 2008/913/WSiSW z dnia 28 listopada 2008 r. w sprawie zwalczania pewnych form i przejawów rasizmu i ksenofobii za pomocą środków prawnokarnych⁷⁹. Stanowisko to jest wyrazem kontynuacji linii wyrażonej przez organy UE w zaleceniu z 2018 r. dotyczącym nielegalnych treści⁸⁰. Na gruncie tego aktu prawnego dokonano także subtelного rozróżnienia pomiędzy kategorią „nielegalnych” i „szkodliwych”

a także ustalania rozmiaru kar, jakie grożą za ich popełnienie i określania środków ochrony służących pokrzywdzonym i ofiarom tych przestępstw. Nadto do kompetencji organów stanowiących UE należałoby przesądzenie o zamkniętym albo otwartym katalogu grup podmiotów, których prawa zostaną poddane ochronie oraz ustalenie przesłanek ochrony. Projektowane działanie należy rozpatrywać nie tylko w kategoriach przeciwdziałania nowym typom przestępstw, w szczególności cyberprzestępstw, ale także analizować je ze względu na prawdopodobne skutki, jakie mogą one wywołać w sferze korzystania przez obywateli państw członkowskich UE z konstytucyjnie gwarantowanych praw i wolności, w tym z wolności wypowiedzi. Projektowane rozwiązania, ze względu na przedmiot i proponowaną metodę regulacji, legitymizują działania organów UE w zakresie, w jakim będą one mogły skutecznie oddziaływać na ustalenie granic swobody wypowiedzi.

⁷⁷ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępująca decyzję ramową Rady 2002/475/WSiSW oraz zmieniająca decyzję Rady 2005/671/WSiSW (Dz.U. L Nr 88, s. 6) – dalej: dyrektywa 2017/541.

⁷⁸ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym (Dz.U. UE L Nr 172, s. 79) – dalej: rozporządzenie w sprawie treści terrorystycznych.

⁷⁹ Decyzja ramowa Rady 2008/913/WSiSW z dnia 28 listopada 2008 r. w sprawie zwalczania pewnych form i przejawów rasizmu i ksenofobii za pomocą środków prawnokarnych (Dz.U. UE L Nr 328, s. 55).

⁸⁰ Zalecenie Komisji (UE) 2018/334 z dnia 1 marca 2018 r. w sprawie działań na rzecz skutecznego zwalczania nielegalnych treści w internecie (Dz.U. UE L Nr 63, s. 50). Przyjęcie przez PE rozporządzeń cyfrowych zostało także poprzedzone konsultacjami dotyczącymi kodeksów samoregulacyjnych prowadzonych przy wsparciu Komisji, przewidujących system dobrowolnych zobowiązań do zapewnienia bezpieczeństwa produktów (ang. *product safety pledge*), Protokół ustaleń w sprawie sprzedaży podrobionych towarów w internecie, kodeks postępowania dotyczący nielegalnego nawoływania do nienawiści w internecie (Wniosek AUC, s. 6).

treści, przy czym zarówno jedno, jak i drugie – w zamyśle KE – są niepożądane i powinny być usuwane z przestrzeni publicznej. „Nielegalne treści” zostały w zaleceniu z 2018 r. zdefiniowane jako „wszelkie informacje, które nie są zgodne z prawem Unii lub z prawem danego państwa członkowskiego” (Rozdział I ust. 4 lit. b).

W decyzji ramowej Rady z 2008 r. zobowiązano państwa członkowskie do kryminalizacji szeregu czynów umyślnych związanych z publicznym nawoływaniem do przemocy lub nienawiści skierowanej przeciwko grupie osób, którą definiuje się według rasy, koloru skóry, wyznawanej religii, pochodzenia albo przynależności narodowej lub etnicznej, lub przeciwko członkowi takiej grupy. Zobowiązano w niej również państwa członkowskie do kryminalizacji czynów umyślnych obejmujących aprobowanie, negowanie lub rażące pomniejszanie zbrodni ludobójstwa, zbrodni przeciwko ludzkości, zbrodni wojennych i zbrodni przeciwko pokojowi, skierowanych przeciwko grupie osób, którą definiuje się według rasy, koloru skóry, wyznawanej religii, pochodzenia albo przynależności narodowej lub etnicznej, lub przeciwko członkowi takiej grupy, jeśli czyny takie mogą podburzać do przemocy lub wzbudzać nienawiść skierowaną przeciwko tej grupie lub jej członkowi.

W dyrektywie 2017/541 zostały określone normy minimalne dotyczące definicji przestępstw i sankcji w dziedzinie przestępstw terrorystycznych. Zdefiniowanie „treści terrorystycznych rozpowszechnianych w internecie” nastąpiło natomiast w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym⁸¹.

Treść o charakterze terrorystycznym w internecie stanowią materiały, które podlegają do popełnienia przestępstwa terrorystycznego, pochwalają akty terrorystyczne, popierają popełnianie takich przestępstw, nakłaniają do popełnienia lub przyczynienia się do przestępstw terrorystycznych, nakłaniają do uczestnictwa w działaniach grupy terrorystycznej, udzielają instruktażu w zakresie wytwarzania szeregu rodzajów broni do celów terrorystycznych lub wyrażają groźbę popełnienia przestępstwa terrorystycznego⁸². W rozporządzeniu w sprawie treści terrorystycznych określono ramy prawne

⁸¹ Rozporządzenie w sprawie treści terrorystycznych.

⁸² Tamże.

umożliwiający państwu członkowskiemu kierowanie do dostawców usług hostingowych nakazów usunięcia tych treści, które zobowiązują ich do usunięcia danych treści w ciągu jednej godziny. Ponadto zobowiązano w nim dostawców usług hostingowych narażonych na treści o charakterze terrorystycznym do wdrożenia szczególnych środków w celu zapobiegania wykorzystywaniu ich usług do niewłaściwych celów. W rozporządzeniu zauważono, że przeciwdziałanie treściom o charakterze terrorystycznym w internecie to element szerszego problemu dotyczącego treści nielegalnych w internecie i wymaga połączenia środków o charakterze prawodawczym, nieprawodawczym i środków dobrowolnych, opartych na współpracy między organami a dostawcami usług hostingowych, w sposób, który w pełni szanuje prawa podstawowe (motyw 3).

Wyczerpujący wykaz poważnych przestępstw, których popełnienie, a także – jak wynika z art. 5 dyrektywy w sprawie terroryzmu – nawoływanie do ich popełnienia powinno być ścigane we wszystkich państwach członkowskich, zawiera art. 3 dyrektywy w sprawie terroryzmu. Katalog ten obejmuje ściganie przestępstw takich jak ataki na życie ludzkie, stanowiących czyny umyślne, które można zakwalifikować jako przestępstwa terrorystyczne wyłącznie w przypadku, gdy zostały popełnione w określonym celu terrorystycznym, mianowicie, aby poważnie zastraszyć ludność, bezprawnie zmusić rząd lub organizację międzynarodową do podjęcia lub zaniechania działania lub aby poważnie zdestabilizować lub zniszczyć podstawowe struktury polityczne, konstytucyjne, gospodarcze lub społeczne danego państwa lub danej organizacji międzynarodowej. Groźby popełnienia takich czynów umyślnych również należy uznawać za przestępstwa terrorystyczne, jeżeli obiektywne przesłanki wskazują, że dopuszczono się ich, kierując się jednym z wymienionych celów terrorystycznych (motyw 9).

Do katalogu poważnych przestępstw⁸³ w myśl art. 5 tej dyrektywy w sprawie terroryzmu należy także „publiczne nawoływanie do popełnienia przestępstwa terroryzmu”. Przestępstwo związane z publicznym nawoływaniem do popełniania czynów będących przestępstwem terrorystycznym obejmuje m.in. pochwalanie i usprawiedliwianie terroryzmu lub rozpowszechnianie w internecie lub poza nim wiadomości lub obrazów, w tym obrazów dotyczących

⁸³ Art. 83 ust. 1 TFUE.

ofiar terroryzmu, w celu zdobycia poparcia dla idei terrorystycznych lub w celu poważnego zastraszania ludności. W myśl motywu 10 dyrektywy taki czyn powinien podlegać karze, jeżeli stwarza niebezpieczeństwo popełnienia aktów terrorystycznych. W każdym konkretnym przypadku przy ocenianiu, czy takie niebezpieczeństwo istnieje, uwzględnić należy szczególne okoliczności sprawy, takie jak autora i adresata wiadomości, a także kontekst, w jakim doszło do popełnienia czynu. To, czy niebezpieczeństwo jest istotne i czy ma ono wiarygodny charakter, należy również brać pod uwagę przy stosowaniu przepisu o publicznym nawoływaniu zgodnie z prawem krajowym (motyw 10).

W dyrektywie zobowiązano państwa członkowskie UE do podejmowania niezbędnych środków w celu zapewnienia, aby karze jako przestępstwo – jeżeli popełniono je umyślnie – podlegało rozpowszechnianie lub innego rodzaju udostępnianie w dowolny sposób, w internecie lub poza nim, przekazu do publicznej wiadomości z zamiarem podżegania do popełnienia przestępstwa terrorystycznego (art. 5 dyrektywy). Wskazano zarazem, że środkiem służącym „zwalczaniu treści internetowych publicznie nawołujących do popełnienia przestępstwa”, który powinien być wykorzystany przez państwa członkowskie, jest usuwanie lub blokowanie treści internetowych, przy czym środki te powinny mieć zastosowanie zarówno do treści znajdujących się na serwerach mieszczących się na terytorium tych państw, jak i poza nim (art. 21 ust. 1 dyrektywy). Jeśli usunięcie lub zablokowanie treści u źródła nie jest wykonalne, państwa członkowskie mogą „podjąć środki w celu zablokowania użytkownikom korzystającym z internetu na ich terytorium dostępu do takich treści” (art. 21 ust. 2 dyrektywy). W motywie 40 dyrektywy zastrzeżono zarazem, że „wyrażanie radykalnych, polemicznych lub kontrowersyjnych poglądów w toku debaty publicznej dotyczącej delikatnych kwestii politycznych wykracza poza zakres zastosowania niniejszej dyrektywy, a w szczególności poza zakres definicji publicznego nawoływania do popełniania przestępstw terrorystycznych”. Zarazem w rozporządzeniu w sprawie treści terrorystycznych przesądzono⁸⁴, że na wypadek, gdyby państwo członkowskie nie podjęło

⁸⁴ W motywie 50 wskazano, że, ponieważ cel niniejszego rozporządzenia, a mianowicie zapewnienie sprawnego funkcjonowania jednolitego rynku cyfrowego poprzez przeciwdziałanie rozpowszechnianiu w internecie treści o charakterze terrorystycznym, nie może zostać osiągnięty w sposób wystarczający przez państwa członkowskie, natomiast ze względu na rozmiary i skutki możliwe jest jego lepsze osiągnięcie na poziomie

skutecznych środków przeciwdziałania popełniania przestępstwa, w szczególności nawoływania do terroryzmu, Unia Europejska może podjąć odpowiednie działania zgodnie z zasadą pomocniczości wyrażoną w art. 5 TFUE.

W motywie 50 rozporządzenia w sprawie treści terrorystycznych wyrażono stanowisko, zgodnie z którym cel rozporządzenia, a mianowicie zapewnienie sprawnego funkcjonowania jednolitego rynku cyfrowego poprzez przeciwdziałanie rozpowszechnianiu w internecie takich treści, nie może zostać osiągnięty w sposób wystarczający przez państwa członkowskie, a zarazem ze względu na rozmiary i skutki możliwe jest jego lepsze osiągnięcie na poziomie Unii, może ona podjąć działania zgodne z zasadą pomocniczości określoną w art. 5 TUE. W tym samym miejscu (motyw 50) stwierdzono, że rozporządzenie w sprawie treści terrorystycznych nie wykracza poza to, co jest konieczne do osiągnięcia celu rozporządzenia, a w konsekwencji jest zgodne z wyrażoną w art. 5 TFUE zasadą proporcjonalności. Podobny mechanizm służący usprawiedliwieniu ingerencji przez podmiot publiczny (Komisja Europejska, państwa członkowskie UE) w swobodę wypowiedzi obywateli został przewidziany w rozporządzeniach cyfrowych. W motywie 155 AUC powołano się na zasadę pomocniczości zawartą w art. 5 TUE, wskazując, że „ponieważ cele niniejszego rozporządzenia, mianowicie przyczynianie się do prawidłowego funkcjonowania rynku wewnętrznego oraz zapewnienie bezpiecznego, przewidywalnego i budzącego zaufanie środowiska internetowego, w którym prawa podstawowe zapisane w Karcie praw podstawowych są odpowiednio chronione, nie mogą zostać osiągnięte w sposób wystarczający przez państwa członkowskie, gdyż działając samodzielnie, nie mogą one osiągnąć niezbędnej harmonizacji i współpracy, natomiast ze względu na zakres terytorialny i podmiotowy możliwe jest ich lepsze osiągnięcie na poziomie Unii, może ona podjąć działania zgodne z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsze rozporządzenie nie wykracza poza to,

Unii, może ona podjąć działania zgodne z zasadą pomocniczości określoną w art. 5 TUE. W tym samym miejscu (motyw 50) wyrażono stanowisko, zgodnie z którym rozporządzenie w sprawie treści terrorystycznych nie wykracza poza to, co jest konieczne do osiągnięcia tego celu, a w konsekwencji jest zgodne z wyrażoną w art. 5 TFUE zasadą proporcjonalności.

co jest konieczne do osiągnięcia tych celów”. Treść tożsamą z powyżej zacytowaną zawiera także motyw 107 ARC.

Powołanie się PE w rozporządzeniach cyfrowych na zasadę pomocniczości i wybór przez PE rozporządzenia jako właściwego instrumentu regulacyjnego w sferze normowania praw i wolności, w tym także ustalania granic wolności wypowiedzi, przenosi *de facto* na podmioty publiczne, w tym przede wszystkim Komisję Europejską, uprawnienia w zakresie kształtowania standardu wolności wypowiedzi w internecie. Zgodnie z zasadą pomocniczości, w dziedzinach, które nie należą do jej wyłącznej kompetencji, Unia podejmuje działania tylko wówczas i tylko w takim zakresie, w jakim cele zamierzonego działania nie mogą zostać osiągnięte w sposób wystarczający przez państwa członkowskie, zarówno na poziomie centralnym, jak i regionalnym oraz lokalnym, i jeśli ze względu na rozmiary lub skutki proponowanego działania możliwe jest lepsze ich osiągnięcie na poziomie Unii (art. 5 ust. 3 TUE). Zgodnie z zasadą proporcjonalności zakres i forma działania Unii nie wykraczają poza to, co jest konieczne do osiągnięcia celów Traktatów (art. 5 ust. 3 TUE).

Jest oczywiste, że wypowiedziane w art. 5 TUE zasady pomocniczości i proporcjonalności nie mogą zastępować wypracowanych na gruncie art. 10 ETPC zasad: proporcjonalności, podstawy ustawowej i usprawiedliwionego celu. Zarówno sposób definiowania, jak i zwalczania nielegalnych treści proponowany w pakiecie cyfrowym, a w konsekwencji sposób ustalania granic dopuszczalnych ograniczeń wolności wypowiedzi, są całkowicie odmienne od przyjętych na gruncie klasycznych rozwiązań wypracowanych w szczególności na gruncie wykładni art. 10 EKPC dokonywanej przez Europejski Trybunał Praw Człowieka. I.C. Kamiński zwraca uwagę, że konstrukcja zastosowana na gruncie pakietu cyfrowego prowadzi do sytuacji, w której:

publiczny (państwowy) podmiot zostanie wyposażony w uprawnienie do eliminowania „złej treści”. To on miałby wiedzieć lepiej, co służy publicznemu dobru i jednostce. Paradygmat „wolnego rynku idei” ustępowałby miejsca paradygmatowi „troskliwego opiekuna”. Można, oczywiście, argumentować, że wypowiadająca się jednostka miałaby do swojej dyspozycji procedury kontrolne i odwoławcze, co powinno eliminować możliwość

i pokusę nadużyć. Nie unieważnia to jednak obaw związanych ze zmianą modelu swobody wypowiedzi”⁸⁵.

Pomysły formułowane wobec dostawców usług pośrednich w unijnym rozporządzeniu AUC autor ten postrzega jako „kontrastujące z konwencyjnym standardem wypracowanym przez Trybunał”⁸⁶.

Przesądzające o konstrukcji nowego, kontraktowego standardu wolności wypowiedzi jest nie tylko zakres pojęcia „nielegalne treści”, ale przede wszystkim to, komu zostało udzielone, na gruncie AUC i ARC, upoważnienie do jego definiowania. Zarówno zatem w ujęciu materialnoprawnym, jak i formalnym (proceduralnym) mieścić się może ryzyko naruszenia swobody wypowiedzi. O ile poza internetem przyjmuje się domniemanie, że wkroczenie w cudzą wolność wypowiedzi ma charakter bezprawny, o tyle w środowisku internetowym mechanizm ten został odwrócony. Oznacza to, że naruszyciel będący podmiotem publicznym (Komisja Europejska, państwa członkowskie) albo prywatnym (pośrednicy internetowi, w tym strażnicy dostępu) może wobec odbiorcy usługi i użytkownika internetu (użytkownika końcowego) korzystać z domniemania zgodności z prawem takiego działania, powołując się na obowiązek dochowania należytej staranności lub klauzulę dobrego samarytanina. Dostawca usługi cyfrowej jest bowiem *ex lege*, co wynika wprost z AUC, upoważniony do monitorowania i filtrowania treści przed ich publicznym udostępnieniem w celu zapobiegania rozpowszechnieniu treści nielegalnych. Działania dostawcy polegające na monitorowaniu, filtrowaniu, ograniczaniu dostępu, blokowaniu lub usuwaniu takich treści dowodzą, w myśl AUC, że dostawca dochowuje wymogu należytej staranności, co – w konsekwencji – pozwala mu na uchylenie się od odpowiedzialności prawnej za ewentualne naruszenia praw i interesów treścią bądź formą rozpowszechnionej wypowiedzi.

Obok aspektów materialnoprawnego i proceduralnego, które kształtują granice wolności wypowiedzi, w środowisku cyfrowym ujawnia się nowy czynnik generujący ryzyko naruszenia wolności wypowiedzi. Jest to czynnik związany z istnieniem w sferze internetowej ryzyka nieadekwatnej reakcji

⁸⁵ I.C. Kamiński, *Falszywe wiadomości...*, s. 90–107.

⁸⁶ Tamże.

ze strony dostawców usług pośrednich (platforma internetowa lub wyszukiwarka internetowa) na treść lub formę wypowiedzi przekazanej przez odbiorcę usługi do publicznego udostępnienia. Pośrednik powołując się na wynikające z AUC lub ARC upoważnienie do monitorowania, filtrowania i moderowania treści oraz obowiązek należytej staranności, może uchylić się od odpowiedzialności za przechowywane i publicznie udostępniane przez niego (na platformie lub w wyszukiwarce) wypowiedzi. Zakres wolności wypowiedzi użytkownika internetu (odbiorcy usługi) zależeć będzie zatem od przyjętego przez pośrednika modelu starannego działania, przy czym realizacja wolności wypowiedzi może pozostawać w kolizji z obowiązkiem starannego działania dostawcy usług cyfrowych.

Konstrukcja zaproponowanego w AUC standardu wolności wypowiedzi zasadza się na domniemaniu zgodności z prawem działania podmiotu publicznego, który dokonuje ustalenia i oceny wypowiedzi pod kątem jej legalności, a następnie – w razie stwierdzenia, że wypowiedź narusza prawo UE – eliminowania ich z obiegu publicznego przy pomocy pośredników internetowych posiadających faktyczne władztwo w zakresie usuwania i blokowania treści. Jeśli więc w środowisku realnym oczekiwane jest przede wszystkim nieingerowanie w cudzą wolność wypowiedzi, to w środowisku cyfrowym ingerencja w wolność wypowiedzi nie tylko zostaje usprawiedliwiona, ale staje się elementem konstrukcyjnym nowego modelu wolności wypowiedzi. Model ten normuje prawa i obowiązki w sposób asymetryczny, nieproporcjonalnie wzmacniając prawa podmiotów publicznych i pośredników internetowych kosztem praw odbiorców usług i pozostałych użytkowników internetu.

Asymetria praw nie ma charakteru przypadkowego. Jest konstrukcją, dzięki której ustawodawca europejski realizuje cele rozporządzeń AUC i ARC. Europejski Komitet Regionów zauważył, że – co prawda – nie ma nic antykonkurencyjnego w budowaniu dobrze prosperującego biznesu, jakim jest wiele platform, jednakże dostrzec należy asymetrię informacji, której dysponentami są strażnicy dostępu i użytkownicy końcowi⁸⁷. Stwierdzenie to nie jest jednak wystarczająco precyzyjne i nie oddaje w pełni różnicy, w jakiej znajdują się użytkownicy internetu oraz pośrednicy internetowi. Nie chodzi

⁸⁷ Opinia Europejskiego Komitetu Regionów – Akt o usługach cyfrowych i akt o rynkach cyfrowych, (Dz.U. UE C z 2021 r. Nr 440, s. 67), poprawka 29.

bowiem jedynie o różnice odnośnie do zakresu wiedzy, w jaką wyposażeni są pośrednicy internetowi i użytkownicy internetu. O wiele istotniejsza jest bowiem asymetria praw i upoważnień, na jakie podmioty te mogą się powoływać we wzajemnych stosunkach. O ile jednak poza internetem istnieje system organów publicznych – przede wszystkim organów wymiaru sprawiedliwości – które rozstrzygają o zgodności albo niezgodności (nielegalności) wypowiedzi z prawem, o tyle w przestrzeni internetowej podmioty prywatne, dzięki upoważnieniu do korzystania z narzędzi filtrujących i monitorujących, mogą podejmować działania ze skutkiem porównywalnym do stosowania środków prawnych.

Europejski Komitet Regionów zauważa, że rozporządzenie AUC określa jedynie formalny proces postępowania z nielegalnymi treściami i że określenie, co stanowi nielegalne treści w rozumieniu rozporządzenia, należy do państw członkowskich⁸⁸. Jednakże przeniesienie na podmioty prywatne kompetencji do ustalania *in casu* zgodności lub niezgodności z prawem wypowiedzi przekazanej przez usługobiorcę w celu jej rozpowszechnienia sytuuje państwa członkowskie w roli drugoplanowej i niesprawczej.

Słusznie konstatuje I.C. Kamiński, widząc w regulacjach zawartych w rozporządzeniach cyfrowych niebezpieczeństwo ograniczenia – w stosunku do obecnie istniejących – granic wolności wypowiedzi. Rozporządzenia cyfrowe zmieniają tradycyjną perspektywę przyjmowaną przez strasburski Trybunał przy ustalaniu tzw. europejskiego standardu wolności wypowiedzi. Jak wskazuje I.C. Kamiński, „ta perspektywa była słusznie zorientowana na wypowiadający się podmiot i na zapewnienie wolności komunikowania informacji oraz opinii. Polityki skierowane przeciwko dezinformacji skupiają się natomiast na odbiorcy przekazu”⁸⁹. W konsekwencji powstaje ryzyko odejścia od koncepcji „wolnego rynku opinii” wywodzonego z modelu amerykańskiego na rzecz centralistycznego zarządzania treścią w internecie, kiedy to upoważnione organy decydować będą o usuwaniu treści. Jak stwierdza I.C. Kamiński, nie ma powodów, by odchodzić od reguły mądrze wyrażonej

⁸⁸ Tamże, pkt 11.

⁸⁹ I.C. Kamiński, *Fałszywe wiadomości...*, s. 90–107.

w amerykańskim orzecznictwie: lekarstwem na „problematyczną wypowiedź” jest – co do zasady – więcej mowy, a nie wymuszana cisza⁹⁰.

Przywołane powyżej obawy I.C. Kamińskiego, które należy w całości podzielić, obnażają fasadowość ogłoszonych przez organy UE celów, jakie miały być osiągnięte dzięki wdrożeniu rozporządzeń cyfrowych. Skutki przyjęcia i zastosowania rozporządzeń, w szczególności w zakresie identyfikowania i zwalczania nielegalnych treści, mogą – z dużym prawdopodobieństwem – prowadzić do rezultatów całkowicie sprzecznych z postulowanymi przez PE i Radę. Wskazać należy, że jako oczekiwany skutek przyjęcia rozporządzeń cyfrowych wskazywano, że AUC „ograniczy ryzyko błędnego lub nieuzasadnionego blokowania wypowiedzi, złagodzi efekt mrozący w odniesieniu do wypowiedzi, będzie stymulować swobodę otrzymywania informacji i wyrażania opinii, a także zwiększy możliwości dochodzenia roszczeń przez użytkowników”⁹¹. Rozporządzenie miało pomóc „złagodzić ryzyko dyskryminacji, zwłaszcza w odniesieniu do tych grup lub osób, i przyczyni się do ochrony praw dziecka i prawa do godności ludzkiej w internecie. Zgodnie z wnioskiem wymagane będzie jedynie usuwanie nielegalnych treści i wprowadzone zostaną obowiązkowe zabezpieczenia w przypadku usunięcia informacji użytkownika, w tym udzielenie mu wyjaśnień, mechanizmy składania skarg wspierane przez dostawców usług, a także zewnętrzny mechanizm pozasądowego rozwiązywania sporów”⁹². Szczegółowa analiza proponowanych w rozporządzeniach mechanizmów oraz zakres i sposób definiowania nielegalnych treści dowodzą bowiem, jak zostało to wykazane, że być może będą one stanowić skuteczny instrument zarządzania treścią w internecie, ale nie zwiększają one pewności prawa ani – tym bardziej – nie wzmacniają wolności wypowiedzi w internecie. Wbrew bowiem wyrażanemu przez organy UE stanowisku istnieje wysokie ryzyko zawężenia, w stosunku do obecnie stosowanych, ram wolności wypowiedzi.

⁹⁰ Tamże.

⁹¹ Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie jednolitego rynku usług cyfrowych (akt o usługach cyfrowych) i zmieniające dyrektywę 2000/31/WE, <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020PC0825> (dostęp: 10.10.2023).

⁹² Wniosek AUC, s. 14–15.

C. Niezgoda z warunkami świadczenia usługi

Niezgoda zachowania odbiorcy usługi z warunkami jej świadczenia określonymi w obowiązujących u pośredników internetowych regulaminach może, równolegle albo niezależnie od innych podstaw prawnych wynikających *explicit*e z przepisów prawa UE lub prawa krajowego państw członkowskich, stanowić podstawę ograniczenia świadczenia usługi. Ograniczenie świadczenia usługi może następować „ze względu na fakt, iż informacje przekazane przez odbiorcę usługi stanowią nielegalne treści lub są niezgodne z warunkami korzystania z usług dostawcy” (art. 17 ust. 1 AUC). Ustalenie podstawy decyzji odnośnie do ograniczenia świadczenia usługi należy do dostawcy usług, który – jak wynika z treści AUC – jest kompetentny zarówno w zakresie ustalenia zaistnienia przesłanki „nielegalności” treści, jak i w zakresie ustalenia niezgodności zachowania się usługobiorcy z warunkami świadczenia usługi. Przesłanki uzasadniające decyzję o ograniczeniu świadczenia usług, tj. przesłanka „nielegalności treści” oraz przesłanka „niezgody działania usługobiorcy z warunkami świadczenia usługi”, są równoważne i mogą być stosowane kumulatywnie albo alternatywnie. Ustawodawca europejski powołuje obie te przesłanki równocześnie we wszystkich przepisach AUC i ARC, w których ustala dopuszczalność wprowadzenia ograniczeń w świadczeniu usług przez ich dostawców, w tym strażników dostępu, a także w tych miejscach, w których reguluje zasady wyłączania odpowiedzialności dostawców.

Ograniczenie przez usługodawcę świadczenia usługi ze względu na przesłankę rozpowszechniania przez usługobiorcę nielegalnych treści lub niezgodność z warunkami świadczenia usługi – w myśl motywu 26 AUC – nie osłabia ani nie uchyla prawa usługodawcy do korzystania ze wskazanych w art. 4–6 AUC okoliczności wyłączających ich odpowiedzialność. Jak wskazano w motywie 26 AUC, „sam fakt, iż dostawcy podejmują w dobrej wierze środki w celu spełnienia wymogów prawa Unii w odniesieniu do wdrożenia warunków korzystania z ich usług, nie powinien uniemożliwiać wyłączeń odpowiedzialności ustanowionych w tym rozporządzeniu. W związku z tym przy ustalaniu, czy dostawca może powoływać się na wyłączenie odpowiedzialności, w szczególności w odniesieniu do tego, czy świadczy on swoje usługi w sposób neutralny i w związku z tym może być objęty zakresem stosowania odpowiedniego przepisu, nie należy brać pod uwagę takich działań i środków, które dostawca

mógł podjąć, co nie oznacza jednak, że dostawca musi się koniecznie na takie wyłączenie powołać”. Tym bardziej zatem dobrowolne działania dostawców usług, w szczególności podejmowane z powołaniem się przez dostawcę na zawartą w art. 7 AUC klauzulę dobrego samarytanina, nie uchylają prawa dostawców do powoływania się na wskazane w rozporządzeniu kontratypy. Oznacza to zatem, że działania dostawcy zmierzające do ustalenia i wykrycia nielegalnych treści albo niezgodności zachowania usługobiorcy z warunkami świadczenia usługi, polegające w szczególności na monitorowaniu takich zachowań, śledzeniu użytkowników, a także zastosowaniu innych środków ingerujących w wolność wypowiedzi użytkowników, nie może stanowić podstawy do tego, by odmówić usługodawcy prawa do powoływania się na zasadę neutralności unormowaną w art. 4–6 AUC. Jak wskazywano we wcześniejszych fragmentach niniejszej pracy, zasada neutralności, z pewnymi modyfikacjami w zależności od rodzaju świadczonej usługi (art. 4 – *mere conduit*, art. 5 – *caching*, art. 6 – *hosting*), oznacza, że usługodawca nie ingeruje w treść przesyłanych lub przechowywanych przez niego informacji, nie modyfikuje jej, a nadto nie posiada wiedzy o jej nielegalnym charakterze, a w razie powzięcia takiej informacji niezwłocznie podejmuje działania w celu jej usunięcia albo zablokowania do niej dostępu.

Dostawcy usług podejmując decyzję o ograniczeniu świadczenia usługi, o ile podstawą tej decyzji jest kierowany pod adresem usługobiorcy zarzut rozpowszechniania nielegalnych treści lub naruszenia warunków świadczenia usługi, korzystają z domniemania zgodności z prawem. Ustawodawca wymaga jednak, by działanie usługodawcy było prowadzone w dobrej wierze i z zachowaniem należytej staranności. Warunkiem działania w dobrej wierze i z zachowaniem należytej staranności powinno być działanie w sposób obiektywny, niedyskryminacyjny i proporcjonalny, z należyтым uwzględnieniem praw i prawnie uzasadnionych interesów wszystkich zaangażowanych stron, oraz zapewnienie niezbędnych zabezpieczeń przed nieuzasadnionym usuwaniem legalnych treści, zgodnie z celem i wymogami niniejszego rozporządzenia. W tym celu zainteresowani dostawcy powinni np. podjąć rozsądne środki w celu zapewnienia, aby w przypadku wykorzystywania zautomatyzowanych narzędzi do prowadzenia takich działań dana technologia była wystarczająco wiarygodna, tak aby w jak największym stopniu ograniczyć liczbę błędów (motyw 26 AUC). Wobec powyższego przyjąć należy, że decyzja usługodawcy

korzysta co prawda z domniemania zgodności z prawem, jednakże jest to domniemanie prawne wzruszalne, które może zostać obalone poprzez wykazanie, że usługodawca działał w złej wierze albo jego działanie cechowało się arbitralnością i brakiem proporcjonalności względem zastosowanych środków.

Przesłanka „niezgodności z warunkami świadczenia usługi” upoważniająca usługodawcę do ograniczenia świadczenia usługi zostaje spełniona wobec stwierdzenia przez usługodawcę, że charakter aktywności usługobiorcy (użytkownika internetu) nie mieści się w kanonie oczekiwanych przez usługodawcę zachowań. Skoro przesłanka „niezgodności z warunkami świadczenia usługi” występuje równolegle z przesłanką „nielegalnych treści”, to oznacza, że warunki świadczenia usług u danego usługodawcy mogą przewidywać zarówno wymagania dotyczące powstrzymania się przed rozpowszechnianiem nielegalnych treści, jak i inne wymagania, niezwiązane z rozpowszechnianiem treści ani ich charakterem. Pośrednicy internetowi⁹³ uzyskali zatem w AUC upoważnienie do ograniczania świadczenia usług na innej podstawie niż zwalczanie nielegalnych treści. Zawsze jednak, w przypadku ograniczenia świadczenia usługi, niezależnie od wskazanej przez usługodawcę podstawy tej decyzji, ograniczenia doznaje wolność wypowiedzi użytkownika.

W niniejszej pracy przyjęto, biorąc pod uwagę szeroką wykładnię terminu „wypowiedź” dokonywaną przez ETPC na gruncie europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności, że wypowiedź może przyjmować postać nie tylko werbalną, ale także przejawiać się w innych rodzajach aktywności jednostki. Wypowiedzią może być zatem np. przeglądanie (ang. *scrolling*) stron internetowych przez pozostawianie „śladów” obrazujących miejsce i czas spędzony na stronie internetowej oraz liczbę i częstotliwość wyświetleń oraz abonowanie określonych rodzajów usług albo rezygnacja z abonamentu.

Szeroko rozumieć należy także termin „publicznego rozpowszechniania”, który ustawodawca europejski nakazuje definiować jako „udostępnianie informacji na żądanie odbiorcy usługi, który przekazał informacje, potencjalnie nieograniczonej liczbie osób trzecich” (ar. 3 lit. k AUC) i wyjaśnia,

⁹³ Nie może bowiem umykać z pola widzenia, że adresatami norm zawartych w rozporządzeniach cyfrowych są te podmioty, które świadczą usługi pośrednictwa internetowego, a zatem regulacje zawarte w AUC i ARC nie obejmują pozostałych podmiotów świadczących usługi społeczeństwa informacyjnego.

że „udostępnianie informacji potencjalnie nieograniczonej liczbie osób oznacza zapewnienie łatwego dostępu do informacji ogółowi odbiorców usługi bez konieczności podejmowania dalszych działań przez odbiorcę usługi zapewniającej te informacje, niezależnie od tego, czy osoby te faktycznie korzystają z dostępu do tych informacji” (motyw 14 AUC).

Rodzaje usług świadczonych przez pośredników internetowych, objęte zakresem art. 4–6 AUC, są użytkownikom internetu znane pod nazwami komercyjnymi nadawanymi im przez usługodawców, jak w szczególności Mapy Google, Apple Store, Wyszukiwarka Google, Tik Tok czy Facebook i Instagram. Do usług pośrednictwa internetowego zaliczone zostały zatem internetowe platformy handlowe, internetowe serwisy społecznościowe, wyszukiwarki internetowe, systemy operacyjne czy sklepy z aplikacjami⁹⁴. Z badań przeprowadzonych pod auspicjami KE wynika, że usługi cyfrowe mają następujące właściwości:

(i) są to wysoce skoncentrowane, wielostronne usługi platformowe, w przypadku których jedna duża platforma cyfrowa lub bardzo ograniczona liczba dużych platform cyfrowych ustala warunki handlowe, mając w tym zakresie znaczną autonomię; (ii) kilka dużych platform cyfrowych pełni rolę punktów dostępu umożliwiających użytkownikom biznesowym dotarcie do konsumentów i odwrotnie; oraz (iii) uprawnienia strażnika dostępu takich dużych platform cyfrowych są często nadużywane, co przejawia się nieuczciwym postępowaniem wobec ekonomicznie zależnych użytkowników biznesowych i konsumentów⁹⁵.

Zważywszy na wysoki poziom koncentracji niektórych usług cyfrowych, co powoduje, że są one świadczone przez niewielką grupę podmiotów służących jako punkty dostępu dla użytkowników biznesowych i użytkowników końcowych, sklasyfikowano je jako „podstawowe usługi platformowe”. Do podstawowych usług platformowych zaliczone zostały następujące:

- a) usługi pośrednictwa internetowego;
- b) wyszukiwarki internetowe;

⁹⁴ Wniosek ARC, s. 1.

⁹⁵ Tamże, s. 3.

- c) internetowe serwisy społecznościowe;
- d) usługi platformy udostępniania wideo;
- e) usługi łączności interpersonalnej niewykorzystujące numerów;
- f) systemy operacyjne;
- g) przeglądarki internetowe;
- h) wirtualni asystenci;
- i) usługi przetwarzania w chmurze;
- j) internetowe usługi reklamowe, w tym sieci reklamowe, giełdy reklamowe i inne usługi pośrednictwa w zakresie reklam (art. 2 ust. 2 ARC).

Realizacja każdej usługi cyfrowej sklasyfikowanej jako podstawowa usługa platformowa polega zarówno na rozpowszechnianiu treści, jak i na udzielaniu dostępu do treści. Transmisja, przechowywanie i udostępnianie treści stanowi bowiem istotę usług cyfrowych, w tym także usług pośrednictwa internetowego i usług sklasyfikowanych jako podstawowe usługi platformowe. Ustalenie warunków świadczenia usług platformowych przez dostawców tych usług oraz warunków korzystania z usług oddziałuje na sferę praw i wolności użytkowników internetu. W konsekwencji odmowa świadczenia usługi, ograniczenie jej świadczenia lub zaprzestanie świadczenia usługi ingeruje bezpośrednio w sferę wolności wypowiedzi użytkowników internetu. Ograniczenie świadczenia usługi platformowej wywiera bowiem skutek polegający na uniemożliwieniu użytkownikom dostępu do treści albo uniemożliwieniu ich udostępniania. Jeśli bowiem przyjąć, co wydaje się niesporne, że wolność wypowiedzi obejmuje zarówno prawo do rozpowszechniania treści, jak i prawo do uzyskiwania dostępu do nich, to oznacza, że każda forma ograniczenia korzystania z usług cyfrowych stanowi ingerencję w wolność wypowiedzi użytkowników internetu.

Zgodnie z art. 17 ust. 1 AUC ograniczenie świadczenia usług cyfrowych może przybierać postać:

- a) ograniczenia w zakresie widoczności określonych informacji przekazywanych przez dostawcę usługi, w tym usuwanie treści, uniemożliwianie dostępu do treści lub depozycjonowanie treści;
- b) zawieszenie, zakończenie lub inne ograniczenie płatności pieniężnych;
- c) zawieszenie lub zakończenie świadczenia usługi w całości lub w części;
- d) zawieszenie lub zamknięcie konta odbiorcy usługi.

Ustawodawca europejski upoważnia dostawców usług cyfrowych do ograniczenia świadczonych przez nich usług na rzecz użytkownika (usługobiorcy) w przypadku stwierdzenia, że usługobiorca naruszył „warunki korzystania z usług”.

Wyrażenie „warunki korzystania z usług” oznacza – zgodnie z definicją legalną zawartą w art. 3 lit. u AUC – „klauzule, niezależnie od ich nazwy lub formy, które regulują stosunek umowny między dostawcą usług pośrednich a odbiorcami usług”. Stosunek umowny stanowi wzajemną relację podmiotów, które do niego przystępują. Z jednej strony powstaje prawo żądania spełnienia określonego świadczenia (uprawnienie wierzyciela), z drugiej strony powstaje obowiązek spełnienia świadczenia przez działanie lub zaniechanie⁹⁶.

Na gruncie prawa krajowego istotne znaczenie ma art. 353(1) k.c.⁹⁷ statuujący zasadę swobody umów. Zgodnie z tym przepisem „strony zawierające umowę mogą ułożyć stosunek prawny według swego uznania, byleby jego treść lub cel nie sprzeciwiały się właściwości (naturze) stosunku, ustawie ani zasadom współżycia społecznego”. Ograniczeniem zasady swobody umów jest stosunek umowny, w którym zawarcie umowy następuje w sposób adhezyjny, tj. poprzez przystąpienie strony polegające na przyjęciu do stosowania wzorca umownego, w szczególności regulaminu. Zawarcie umowy przez przystąpienie do wzorca wyłącza możliwość negocjowania poszczególnych postanowień umownych, co w konsekwencji oznacza, że strona przystępująca nie może, przed zawarciem umowy, zakwestionować ich treści ani zakresu, jednocześnie przyjmując na siebie obowiązki, w tym także osobiste, których spełnienie będzie podlegało ocenie i może stanowić podstawę zmiany umowy albo jej wypowiedzenia.

Pośrednicy internetowi, w tym strażnicy dostępu, określają warunki świadczenia usług w regulaminach, które udostępniają na swoich stronach internetowych. 6 września 2023 r. Komisja Europejska wskazała sześciu strażników dostępu, tj. firmy Alphabet, Amazon, Apple, ByteDance, Meta i Microsoft i określiła jednocześnie 22 podstawowe usługi platformowe świadczone przez

⁹⁶ A. Cempura, A. Kasolik, *Metodyka sporządzania umów gospodarczych*, Warszawa 2016, s. 44.

⁹⁷ Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz.U. z 2023 r., poz. 1610 z późn. zm.).

te podmioty⁹⁸, z których korzysta więcej niż 45 mln aktywnych abonentów. Każdy ze strażników udostępniając regulamin na swojej stronie podmiotowej, wymaga⁹⁹, by podmiot, który jest zainteresowany świadczeniem przez pośrednika usług, po pierwsze potwierdził, że zapoznał się z regulaminem oraz, po drugie, zaakceptował jego warunki¹⁰⁰. Charakter notoryjny posiada zatem spostrzeżenie, że warunki korzystania z usług świadczonych przez pośredników internetowych, w szczególności strażników dostępu, nie podlegają uzgadnianiu przez strony w ramach indywidualnie prowadzonych negocjacji, a rozpoczęcie świadczenia usługi jest uzależnione od zaakceptowania przez użytkownika treści regulaminu.

⁹⁸ Są to usługi: dla Alphabet – Google Play, sprawa DMA.100002; Mapy Google, sprawa DMA.100011; Zakupy Google, sprawa DMA.100011; Wyszukiwarka Google, sprawa DMA.100004; YouTube, sprawa DMA.100005; Android Mobile, sprawa DMA.100009; Usługa reklamy online Alphabet, sprawa DMA.100010; Google Chrome, sprawa DMA.100008; dla Amazon.com – Market, sprawa DMA.100018; Reklama Amazon, sprawa DMA.100016; dla Apple Inc – AppStore, sprawa DMA.100013; iOS, sprawa DMA.100025; Safari, sprawa DMA.100027; dla ByteDance Ltd. – TikTok, sprawa DMA.100040; dla Meta Platforms Inc. – Facebook Marketplace, sprawa DMA.100044; Facebook, sprawa DMA.100020; Instagram, sprawa DMA.100020; WhatsApp, sprawa DMA.100024; Messenger, sprawa DMA.100024; Meta Ads, sprawa DMA.100035; dla Microsoft Corporation – LinkedIn, sprawa DMA.100017; Windows PC OS, sprawa DMA.100026, zob. *Strażnicy dostępu*, Komisja Europejska, https://digital-markets-act.ec.europa.eu/gatekeepers_pl?ettrans=pl (dostęp: 22.11.2023).

⁹⁹ Charakterystyczne jest, że – z wyłączeniem firmy Meta – strażnicy dostępu nie udostępniają regulaminu, który ma zastosowanie kompleksowo do wszystkich świadczonych przez nich usług. Opracowane przez nich regulaminy są zatem dedykowane poszczególnym usługom, jak w przypadku firmy Alphabet, która wymaga od użytkowników przystąpienia odrębnie do każdej świadczonej przez ten podmiot usługi.

¹⁰⁰ Alphabet (podmiot świadczący usługi Google) wskazuje, że „Aby korzystać z naszych usług, użytkownik musi zaakceptować niniejsze warunki [...] W przypadku niewyrażenia zgody na warunki użytkownik powinien usunąć swoje treści i zaprzestać używania usług” (Warunki korzystania z usług Google, <https://policies.google.com/terms?hl=pl#toc-intro>). Firma Meta wskazuje, że „Korzystanie przez użytkownika z Produktów Meta Platforms Technologies (zgodnie z poniższą definicją) podlega zarówno Regulaminowi Meta, jak i niniejszemu Regulaminowi uzupełniającemu Meta Platforms Technologies (dalej »Regulamin uzupełniający«), które łącznie stanowią umowę pomiędzy użytkownikiem a Meta Platforms Ireland Limited (dalej »Meta«, »firma«, »my« lub »nas«) [...] »Użytkownik musi zgodzić się na kilka wymogów, zanim będzie mógł utworzyć konto, aby skorzystać z naszych Produktów», <https://www.meta.com/pl/legal/supplemental-terms-of-service/> (dostęp: 15.10.2023).

Pośrednicy internetowi na podstawie postanowień AUC definiują łączący ich z użytkownikami stosunek prawny jako umowę¹⁰¹, do której stosować należy przepisy o wzajemnej odpowiedzialności stron. Mając jednakże na uwadze adhezyjny charakter umowy, jaka łączy użytkowników (usługobiorców) z pośrednikami internetowymi (usługodawcami), wątpliwości może budzić ustalenie jej statusu, a w szczególności ocena, w jakim zakresie strony w momencie zawarcia umowy korzystały ze swobody składania oświadczeń woli. Ograniczenie swobody strony w zakresie ustalania warunków umowy i składania oświadczeń woli stanowi przejaw ograniczenia zasady swobody umów zagwarantowanej w art. 353(1) k.c.¹⁰² i zbliża postać złożonych przez strony oświadczeń do wzorca umownego.

Wzorzec umowny stanowi „swoiste ograniczenie swobody umów, które polega na tym, że wzorce są przygotowane wyłącznie przez jedną stronę, a rola drugiej strony sprowadza się do zaakceptowania treści wzorca lub, ewentualnie, do wyboru jednego z kilku wariantów wzorców”¹⁰³. Wzorzec umowny, jak wskazuje się w literaturze, jest „kwalifikowanym oświadczeniem woli stanowiącym szczególną regulację. Za jego pomocą kształtowana jest treść stosunku prawnego poza umową stron. Stąd uznaje się, że wzorzec umowny nie jest częścią umowy i nie wymaga zgody kontrahenta”¹⁰⁴. W zasadzie kontrahent ma ograniczoną do minimum sferę autonomii woli. Może się zgodzić na określony wariant wzorca lub go odrzucić i nie zawierać umowy¹⁰⁵. Z taką właśnie sytuacją spotykają się użytkownicy internetu, układając stosunki prawne z pośrednikami internetowymi.

Jeśli do umowy (regulaminu), której wzorzec został przygotowany przez jedną ze stron, przystępuje osoba o statusie konsumenta, to ocena skuteczności

¹⁰¹ W przypadku firmy Alphabet wskazuje ona użytkownikom z Europejskiego Obszaru Gospodarczego, że w odniesieniu do usług Google zawierają oni umowę z Google Ireland Limited spółką zarejestrowaną i działającą zgodnie z prawem Irlandii, <https://policies.google.com/terms?hl=pl#toc-intro> (dostęp: 15.10.2023). W przypadku firmy Meta i świadczonej usługi portalu społecznościowego Facebook, wskazuje ona, że regulamin stanowi umowę pomiędzy użytkownikiem a Meta Platforms Ireland Limited, https://www.facebook.com/legal/terms_preview_europe (dostęp: 15.10.2023).

¹⁰² Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz.U. z 2023 r., poz. 1610 z późn. zm.).

¹⁰³ A. Cempura, A. Kasolik, *Metodyka...*, s. 75.

¹⁰⁴ Tamże, s. 44.

¹⁰⁵ Tamże, s. 75.

postanowień zawartych w umowie wymaga oceny zawartych w umowie klauzul, w szczególności braku klauzul niedozwolonych. Zgodnie bowiem z art. 385(1) § 1 k.c. postanowienia umowy zawieranej z konsumentem nieuzgodnione indywidualnie nie wiążą go, jeżeli kształtują jego prawa i obowiązki w sposób sprzeczny z dobrymi obyczajami, rażąco naruszając jego interesy (niedozwolone postanowienia umowne). W takim wypadku ocena treści regulaminów przewidujących warunki świadczenia usług pośrednictwa internetowego wymagałaby co najmniej oceny pod kątem istnienia lub nieistnienia takich postanowień umownych, które:

1. przyznają kontrahentowi konsumenta uprawnienia do dokonywania wiążącej interpretacji umowy;
2. uprawniają kontrahenta konsumenta do jednostronnej zmiany umowy bez ważnej przyczyny wskazanej w tej umowie;
3. przyznają tylko kontrahentowi konsumenta uprawnienie do stwierdzania zgodności świadczenia z umową;
4. przewidują wyłącznie dla kontrahenta konsumenta jednostronne uprawnienie do zmiany, bez ważnych przyczyn, istotnych cech świadczenia, mając na uwadze, że wskazane powyżej postanowienia stanowią, w świetle art. 385(3) k.c. niedozwolone klauzule umowne.

Ustawodawca europejski, jak się wydaje, przypisuje regulaminom obowiązującym u dostawców usług cyfrowych mieszany charakter. Z jednej strony zatem ujmuje je jako umowy i deklaruje powstrzymanie się przed ingerencją w ich treść przez wzgląd na zasadę swobody umów (motyw 45 AUC), z drugiej jednak strony nakłada na pośredników – w sposób stanowczy – obowiązki, których wykonanie ma uchronić użytkowników internetu przed nadużyciami ze strony pośredników internetowych. Wskazuje się zatem, że dostawcy usług mają obowiązek „ustanowić pewne zasady dotyczące treści, stosowania i egzekwowania warunków korzystania z usług tych dostawców w celu zapewnienia przejrzystości, ochrony odbiorców usługi oraz unikania nieuczciwych lub arbitralnych wyników. Dostawcy usług pośrednich w warunkach korzystania z ich usług powinni wyraźnie podawać i aktualizować informacje o powodach, dla których mogą ograniczyć świadczenie swoich usług. Warunki te powinny w szczególności zawierać informacje na temat wszelkich polityk, procedur, środków i narzędzi wykorzystywanych do celów moderowania treści, w tym algorytmicznego podejmowania decyzji i weryfikacji przez człowieka, a także

na temat regulaminu wewnętrznego systemu rozpatrywania skarg. Powinny one również zawierać łatwo dostępne informacje na temat prawa do zakończenia korzystania z usługi. Dostawcy usług pośrednich mogą wykorzystywać elementy graficzne w warunkach świadczenia usług, takie jak ikony lub obrazki, do zilustrowania głównych elementów wymogów informacyjnych określonych w niniejszym rozporządzeniu. Dostawcy powinni informować odbiorców swojej usługi za pomocą odpowiednich środków o istotnych zmianach wprowadzonych w warunkach korzystania z usług, np. w przypadku zmiany zasad dotyczących informacji dozwolonych na temat ich usługi, lub o innych tego rodzaju zmianach, które mogą mieć bezpośredni wpływ na zdolność odbiorców do korzystania z usługi” (motyw 45 AUC).

Dalej idące obowiązki dotyczące „warunków korzystania z usług” zawartych w regulaminach są adresowane do dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych, a zatem *de facto* do strażników dostępu. Wymogi te dotyczą udzielania informacji i zapewnienia przejrzystości ich warunków korzystania z usług. W motywie 48 AUC wskazano, że dostawcy bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych powinni udostępniać swoje warunki korzystania z usług w językach urzędowych wszystkich państw członkowskich, w których oferują swoje usługi, a także powinni przekazywać odbiorcom usług zwięzłe i łatwe do odczytania streszczenie głównych elementów warunków korzystania z usług. W streszczeniach takich należy wskazać główne elementy wymogów informacyjnych, w tym możliwość łatwego niezakoceptowania klauzul opcjonalnych.

Na pośredników internetowych nałożony został także obowiązek uzasadniania decyzji o ograniczeniu świadczenia usług. Dostawca ten powinien w sposób jasny i łatwo zrozumiały poinformować odbiorcę o swojej decyzji, powodach jej podjęcia oraz dostępnych możliwościach odwołania się od tej decyzji, mając na uwadze negatywne konsekwencje, jakie taka decyzja może mieć dla odbiorcy, w tym dla możliwości wykonywania przez niego prawa podstawowego do wolności wypowiedzi. Obowiązek ten powinien mieć zastosowanie niezależnie od powodów podjęcia decyzji, w szczególności niezależnie od tego, czy działanie podjęto ze względu na uznanie zgłoszonych informacji za nielegalne treści lub za informacje niezgodne z mającymi zastosowanie warunkami korzystania z usług. Jeżeli decyzję podjęto po otrzymaniu

zgłoszenia, dostawca usług hostingu powinien ujawnić odbiorcy usług tożsamość osoby lub podmiotu, które dokonały zgłoszenia, wyłącznie wówczas, gdy informacje te są niezbędne do stwierdzenia nielegalności treści, np. w przypadku naruszenia praw własności intelektualnej (motyw 54 AUC i art. 17 AUC). Nadto warunki korzystania z usług powinny uwzględniać występowanie ryzyka, w tym ryzyka systemowego, związanych z rozpowszechnieniem nielegalnych treści. Rodzi to potrzebę dokonywania ich przeglądu oraz dostosowania do zmieniających się okoliczności (motywy 84 i 87, a także art. 34 ust. 2 AUC).

Wskazane w rozporządzeniach cyfrowych wskazówki dotyczące obligatoryjnych postanowień umownych, w szczególności dotyczących warunków korzystania z usług, niewątpliwie ograniczają ryzyko wystąpienia arbitralności w działaniu dostawców usług cyfrowych, jednakże nie zmienia to faktu, że decyzje o zastosowaniu ograniczenia świadczenia usługi nadal pozostawać będą w gestii pośredników internetowych. Uchylenie lub zmiana decyzji o wprowadzonym przez pośredników ograniczeniu nie jest wykluczona, niemniej nadal należy do sfery jego dobrowolnego działania, w tym dokonania jego autokorekty.

O ile ustawodawca europejski zwraca uwagę na formalne aspekty związane z wydaniem i stosowaniem decyzji o ograniczeniu świadczenia usługi takie jak, w szczególności, potrzeba jej uzasadnienia, doręczenia, zapewnienie możliwości odwołania się od decyzji, to jednak pozostawia dostawcom usług cyfrowych daleko idącą swobodę w zakresie ustalania zaistnienia przesłanek do dokonywania ingerencji w swobodę wypowiedzi. Ustawodawca europejski ceduje zatem na podmioty prywatne quasi-sądowe upoważnienie do ustalania zaistnienia przesłanki „nielegalności treści” oraz „niezgodności z warunkami korzystania z usługi”.

Zważywszy, że w AUC i ARC nie przewidziano mechanizmu ani instrumentu służącego do pociągania do odpowiedzialności dostawców usług za podejmowanie wadliwych decyzji dotyczących wprowadzania ograniczenia świadczenia usługi, z wyjątkiem sankcji polegającej na uchyleniu decyzji i nakazaniu dostawcy dalszego świadczenia usługi, wydaje się, że dostawcy wykazywać będą, w większym stopniu, skłonność do wprowadzania ograniczenia świadczenia usługi, nie chcąc narazić się na zarzut KE dotyczący dopuszczenia do rozpowszechnienia nielegalnych treści, niż podejmowania

działań polegających na zapewnieniu realizacji swobody wypowiedzi użytkowników końcowych.

2. Usprawiedliwiona ingerencja – aspekty formalnoprawne

O ile przesłanka „nielegalnych treści” oraz „niezgodności z warunkami świadczenia usługi” stanowią materialnoprawną podstawę ingerencji w wolność wypowiedzi, o tyle wskazane w AUC i ARC obligatoryjne mechanizmy reagowania (art. 16 – *notice and takedown*; art. 20–21 – wewnętrzny system rozpatrywania skarg; art. 22 – zaufane podmioty sygnalizujące; art. 23 – oczywiście nielegalne treści, oczywiście bezzasadne skargi), a także przewidziane w AUC instrumenty ograniczania ryzyka systemowego (art. 34 – szacowanie ryzyka; art. 35 – zmniejszanie ryzyka; art. 36 – reagowanie kryzysowe; art. 67 – uprawnienia informacyjne KE; art. 69 – uprawnienia kontrolne KE) oraz wykonywanie nakazów wydawanych przez kompetentne organy (koordynatorów ds. usług cyfrowych, Komisję Europejską; Rada Usług Cyfrowych) dotyczących wykonywania, ograniczenia, zawieszenia lub zaprzestania świadczenia usług przez pośredników internetowych (art. 51 – uprawnienia koordynatorów; art. 52 – sankcje; art. 70 – środki tymczasowe; art. 73 – decyzje KE) stanowią podstawę formalną podejmowanych czynności, przy czym adresatem norm proceduralnych są zarówno dostawcy usług, jak i organy państw członkowskich odpowiedzialne za wdrożenie i stosowanie AUC i ARC (koordynatorzy ds. usług cyfrowych; organy wymiaru sprawiedliwości) oraz Komisja Europejska, jako organ centralny skupiający kompetencje kontrolne, nadzorcze i egzekucyjne, a nadto wyposażona w upoważnienia do wydawania aktów delegowanych i wykonawczych oraz wytycznych.

A. Mechanizm zgłaszania i reagowania (zawistość sporu) – środki zabezpieczające

Mechanizm „zgłaszania i reagowania” (ang. *notice and take down*) opisany w art. 16 AUC był początkowo stosowany w niektórych państwach członkowskich UE, a następnie został zaproponowany w Zaleceniu Komisji (UE) 2018/334 z dnia 1 marca 2018 r. w sprawie działań na rzecz skutecznego zwalczania nielegalnych treści w internecie¹⁰⁶ jako pożądany w całej Unii¹⁰⁷ instrument wspomagający zwalczanie nielegalnych treści, po to, by ostatecznie w rozporządzeniu o usługach cyfrowych (AUC) mógł zostać ustanowiony jako instrument obligatoryjny. Jego wdrożenie i stosowanie stało się obowiązkiem dostawców usług cyfrowych, w szczególności dostawców usług hostingu oraz dostawców platform internetowych.

Mechanizm *notice and take down* ma na celu „ułatwienie zawiadamiania odnośnego dostawcy usług o treściach, które strona zawiadamiająca uznaje za nielegalne – „zawiadomienie”, w następstwie czego dostawca ten może zdecydować, czy zgadza się z taką oceną i czy pragnie usunąć te treści lub uniemożliwić dostęp do nich – „działanie” (motyw 11 Zalecenia z 1 marca 2018 r.). Do dnia wejścia w życie AUC dostawcy usług pośrednich mogli skutecznie uchylić się od odpowiedzialności za rozpowszechnienie nielegalnych treści, o ile nie posiadali wiedzy, że rozpowszechniane informacje będące przedmiotem świadczonej przez nich usługi (hostingu, transmisji danych) są bezprawne. Do pośredników internetowych w ówczesnym stanie prawnym znajdowały zastosowanie przepisy o wyłączeniu odpowiedzialności pośredników zawarte w art. 12–15 dyrektywy o handlu elektronicznym. Jak kilkakrotnie zauważał Rzecznik Generalny UE, na mocy powyżej wskazanych przepisów usługodawca był w istocie zwolniony z wszelkiej odpowiedzialności, jaka może wynikać z niezgodnej z prawem informacji, którą przechowuje on na żądanie użytkownika swojej usługi, o ile – po pierwsze – nie miał o niej wiedzy

¹⁰⁶ Zalecenie Komisji (UE) 2018/334 z dnia 1 marca 2018 r. w sprawie działań na rzecz skutecznego zwalczania nielegalnych treści w internecie (Dz.U. UE L Nr 63, s. 50).

¹⁰⁷ W motywie 52 AUC wskazano, że „przepisy dotyczące takich mechanizmów zgłaszania i działania powinny być zharmonizowane na poziomie Unii, aby zapewnić terminowe i niearbitralne przetwarzanie zgłoszeń z zachowaniem należytej staranności na podstawie jednolitych, przejrzystych i jasnych zasad, które zapewniają solidne gwarancje ochrony praw i prawnie uzasadnionych interesów wszystkich zainteresowanych stron [...]”.

lub – po drugie – w danym wypadku niezwłocznie usunął informację lub uniemożliwił dostęp do niej. W praktyce od takiego usługodawcy nie oczekiwano, że będzie on nadzorował informacje obecne na jego serwerach i że będzie aktywnie poszukiwał informacji o bezprawnym charakterze, które się tam znajdują¹⁰⁸. Natomiast jeżeli go poinformowano o istnieniu i miejscu takiej niezgodnej z prawem informacji, co do zasady za pośrednictwem zawiadomienia wysłanego przez osobę trzecią, ów usługodawca powinien zareagować, usuwając daną informację lub uniemożliwiając dostęp do niej – zgodnie z systemem „zastrzeżenia i usunięcia” (ang. *notice and take down*)¹⁰⁹.

Dostawcy usług cyfrowych nie byli, co do zasady, zainteresowani wprowadzaniem procedury *notice and take down* ani ułatwianiem zgłaszania przez użytkowników nielegalnych treści z tego przede wszystkim powodu, że przyjęcie przez dostawcę zgłoszenia obligowało go do działania. Brak reakcji, w szczególności nieusunięcie bezprawnych treści, rodziło ryzyko poniesienia przez dostawcę odpowiedzialności jak za jej rozpowszechnienie.

W aktualnym stanie prawnym¹¹⁰ ustawodawca europejski oczekuje, że mechanizm „zgłaszania i reagowania” będzie łatwy do zidentyfikowania oraz co najmniej tak łatwy do znalezienia i wykorzystania, jak mechanizmy zgłaszania treści naruszających warunki korzystania z usług dostawcy usług. Osoby lub podmioty powinny mieć możliwość zgłaszania wielu potencjalnie nielegalnych treści w jednym zgłoszeniu w celu zapewnienia skutecznego działania i reagowania. Mechanizm zgłaszania powinien umożliwiać identyfikację osoby lub podmiotu dokonujących zgłoszenia, ale nie powinien jej wymagać. W przypadku niektórych rodzajów zgłaszanych informacji tożsamość osoby lub podmiotu dokonujących zgłoszenia może być konieczna do ustalenia, czy dane informacje stanowią potencjalne treści nielegalne. Obowiązek wprowadzenia mechanizmów zgłaszania i działania powinien mieć zastosowanie np. do usług przechowywania i udostępniania plików, usług

¹⁰⁸ Opinia Rzecznika Generalnego w sprawie RP przeciwko PE i Radzie, pkt 105.

¹⁰⁹ Opinia Rzecznika Generalnego UE przedstawiona w dniu 16 lipca 2020 r. w sprawie Frank Peterson przeciwko Google LLC, YouTube LLC, YouTube Inc., Google Germany GmbH, C-682/18 i C 683/18, oraz Elsevier Inc. przeciwko Cyando AG, C-683/18, pkt 173–196, <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:62018CCo682&from=IT> (dostęp: 22.11.2023).

¹¹⁰ Mam na myśli stan prawny na dzień 17 lutego 2024 r., tj. datę, od której AUC będzie stosowane w całej UE.

hostingu stron internetowych (motyw 50 AUC). Dostawcy usług hostingowych po otrzymaniu takiego powiadomienia powinni działać „bez zbędnej zwłoki, z uwzględnieniem rodzaju nielegalnych treści, które są zgłaszane, i pilności działań, które mają zostać podjęte”. Powiadomienia mają być przetwarzane w sposób niearbitralny i niedyskryminujący oraz z poszanowaniem praw podstawowych, w tym wolności słowa¹¹¹.

Reagowanie przez dostawcę usługi cyfrowej na przekazane mu powiadomienie w ramach mechanizmu *notice and take down* powinno obejmować różne płaszczyzny działania, w tym także miałyby polegać na przekazywaniu informacji odpowiednim służbom odpowiedzialnym za utrzymanie bezpieczeństwa publicznego. Już w zaleceniu KE z 2018 r. wskazano, że działania pośrednika powinny w szczególności obejmować współpracę z odpowiednimi organami i Europol w związku ze zgłoszeniami, które stanowią specyficzny sposób powiadamiania dostawców usług hostingowych, dostosowany w szczególności do właściwości walki np. z treściami o charakterze terrorystycznym (motyw 34 zalecenia). Przekazując zgłoszenie, właściwe organy i Europol powinny mieć zarazem możliwość wystąpienia z wnioskiem o usunięcie treści, którą uważają za posiadającą charakter terrorystyczny, lub uniemożliwienie dostępu do niej, albo powołując się na odpowiednie przepisy mające zastosowanie, albo na warunki świadczenia usług przez danego dostawcę usług hostingowych (tamże).

Kierunek ten został utrzymany w AUC. W motywie 56 nałożono na dostawców usług obowiązek zawiadamiania odpowiednich organów w razie powzięcia wiadomości o tym, że „odbiorca usługi mógł popełnić, może właśnie popełniać lub może popełnić przestępstwo zagrażające życiu lub bezpieczeństwu osoby lub osób [...] Przykładowo określone treści mogą rodzić podejrzenie, że stanowią zagrożenie publiczne, takie jak podżeganie do terroryzmu w rozumieniu art. 21 dyrektywy (UE) 2017/541. W takich przypadkach dostawca usług hostingu powinien niezwłocznie poinformować właściwe organy ścigania o takim podejrzeniu”. Nadto pomimo uczynionego zastrzeżenia, że AUC „nie stanowi podstawy prawnej do profilowania odbiorców

¹¹¹ K. Sobczak, *UE: Powstają przepisy mające zwalczać nielegalne treści w internecie* 20.01.2022, Prawo dla każdego, <https://www.prawo.pl/prawo/zwalczanie-nielegalnych-tresci-w-internecie-przepisy-ue,512983.html> (dostęp: 21.11.2023).

usług w celu ewentualnego identyfikowania przestępstw” (motyw 56), to jednak w tej samej jednostce redakcyjnej nałożono na dostawcę usługi szereg obowiązków, których wypełnienie ułatwia ustalenia tożsamości osoby, która udostępniła publicznie nielegalne treści. Wskazano zatem, że „dostawca usług hostingu powinien przekazać wszystkie dostępne mu informacje na ten temat, w tym, w stosownych przypadkach, daną treść i, jeżeli jest dostępny, czas publikacji tej treści, wraz ze wskazaną strefą czasową, wyjaśnienie swoich podejrzeń oraz informacje niezbędne do zlokalizowania i zidentyfikowania odpowiedniego odbiorcy usługi. Informując organy ścigania, dostawcy usług hostingu powinni również przestrzegać innych mających zastosowanie przepisów prawa Unii lub prawa krajowego dotyczących ochrony praw i wolności osób” (motyw 56 AUC).

Dostawca usług pośrednich, na gruncie AUC, może uchylić się od odpowiedzialności, wskazując, kumulatywnie bądź alternatywnie, na jedną z dwóch podstaw prawnych. Po pierwsze pośrednik może zatem wskazywać, że wypełnienie przez niego obowiązku reagowania, w tym zawiadomienie organów bezpieczeństwa publicznego, stanowi pozytywną przesłankę pozwalającą dostawcy usługi na wykazanie, że dochował należytej staranności, a w konsekwencji, że jego działanie jest zgodne z AUC i nie rodzi po jego stronie odpowiedzialności. Po drugie nawet wówczas, gdy w ramach procedury *notice and take down* pośrednik uzyska informacje dotyczące nielegalnych treści i choćby nie podjął żadnego związanego z tym działania, to nadal będzie mógł uchylić się od odpowiedzialności, powołując się na zasadę neutralności (art. 4–6 AUC) i wykazując, że uzyskane przez niego w ramach mechanizmu *notice and take down* informacje nie stanowiły „faktycznej wiedzy”. Dostawca ma bowiem obowiązek działania, ale tylko wówczas, gdy „takie zgłoszenia są wystarczająco precyzyjne i odpowiednio uzasadnione, aby umożliwić działającemu z należytą starannością podmiotowi gospodarczemu rozsądną identyfikację i ocenę potencjalnie nielegalnych treści oraz, w stosownych przypadkach, podjęcie przeciwko nim działań. Takiej faktycznej wiedzy lub wiadomości nie można jednak uznać za uzyskane wyłącznie na podstawie tego, że dostawca jest ogólnie świadomy faktu, że jego usługa jest również wykorzystywana do przechowywania nielegalnych treści. Co więcej, fakt, że dostawca dokonuje automatycznej indeksacji informacji zamieszczonych w ramach jego usługi, że usługa ta zawiera funkcję wyszukiwania, lub

że rekomenduje informacje na podstawie profilu lub ustawień odbiorców usługi, nie jest wystarczający, aby uznać, że dostawca ten posiada „konkretną” wiedzę o nielegalnych działaniach podejmowanych za pośrednictwem tej platformy lub o przechowywaniu na niej nielegalnych treści” (motyw 22).

Ustawodawca europejski opisując ciążące na pośredniku internetowym obowiązki wynikające z mechanizmu *notice and take down*, zastosował zatem taką konstrukcję prawną, która pozwala pośrednikowi, bez ryzyka utraty możliwości powoływania się na wskazane w AUC kontratypy, czynnie uczestniczyć w praktykach monitorowania i wykrywania, a następnie usuwania nielegalnych treści z internetu. Dostawca usług posiada interes w tym, by współdziałać z różnymi podmiotami, a także z własnej inicjatywy podejmować działania w zakresie ustalania i eliminowania nielegalnych treści. Działania te nie tylko bowiem nie uchylają jego prawa do korzystania ze wskazanych w AUC kontratypów, ale nadto pozwalają wykazywać, że świadczył usługi z należytą starannością¹¹².

Ustawodawca europejski ustanawiając obligatoryjność stosowania mechanizmu „zgłaszania i reagowania”, dostrzegał ryzyko naruszenia praw podstawowych, w tym wolności wypowiedzi, jakie generuje zastosowanie tego mechanizmu. By zminimalizować to ryzyko, nałożono na dostawców wymóg stosowania „jednolitych, przejrzystych i jasnych zasad, które zapewniają solidne gwarancje ochrony praw i prawnie uzasadnionych interesów wszystkich zainteresowanych stron, w szczególności ich praw podstawowych zagwarantowanych w Karcie praw podstawowych, niezależnie od państwa członkowskiego, w którym strony te mają siedzibę lub miejsce pobytu, oraz niezależnie od odnośnej dziedziny prawa. Te prawa podstawowe obejmują między innymi w przypadku odbiorców usług: prawo do wolności wypowiedzi i informacji, prawo do poszanowania życia prywatnego i rodzinnego, prawo do ochrony danych osobowych, prawo do niedyskryminacji oraz prawo do skutecznego środka prawnego; w przypadku dostawców usług: wolność prowadzenia działalności gospodarczej, w tym swobodę zawierania umów; w przypadku stron poszkodowanych przez nielegalne treści: prawo

¹¹² Instytucji dobrego samarytanina zawartej w art. 7 AUC oraz znaczeniu, jakie posiada wykazanie przez dostawcę, że działał ze szczególną starannością, poświęcono analizę zawartą w kolejnych fragmentach niniejszej pracy.

do godności ludzkiej, prawa dziecka, prawo do ochrony własności, w tym własności intelektualnej, oraz prawo do niedyskryminacji” (motyw 52 AUC). W konsekwencji przyjęto, że „wszelkie działania podejmowane przez dostawcę usług hostingu w związku z otrzymaniem zgłoszenia powinny być ściśle ukierunkowane, to znaczy powinny służyć usunięciu określonych informacji uznanych za nielegalne treści lub uniemożliwieniu dostępu do nich, jednak bez nadmiernego naruszania wolności wypowiedzi i informacji odbiorców usług” (motyw 54 AUC).

Skoro ustawodawca europejski oczekuje, że mechanizm *notice and take down* nie będzie prowadził do „nadmiernego naruszania wolności wypowiedzi i informacji” (motyw 54), to oznacza, że co do zasady, dopuszcza zaistnienie naruszeń, a nawet zakłada, że ingerencja w wolności wypowiedzi jest niejako częścią mechanizmu „zgłaszania i reagowania”. Ustawodawca oczekuje jedynie, by naruszenie nie było „nadmierne”. Wywodzić można stąd także inny wniosek, a mianowicie taki, że ustawodawca europejski legalizuje naruszenie wolności wypowiedzi, udzielając prymatu ochrony innym wartościom. Nadto ceduje na podmioty prywatne upoważnienie do dokonywania oceny legalności/nielegalności treści w oparciu o ich powszechną – a zatem nieprofesjonalną – wiedzę, co w oczywisty sposób rodzi niebezpieczeństwo pomyłek i nadużyć. W art. 16 ust. 3 AUC wskazano, że ustalenie nielegalnego charakteru treści może następować „bez szczegółowej analizy prawnej”. Posłużono się także terminem „oczywiście nielegalnych treści”, ustalając, że:

informacje należy uważać za stanowiące oczywiście nielegalne treści, jeżeli dla osoby nieposiadającej wiedzy fachowej jest oczywiste, bez przeprowadzenia jakiegokolwiek merytorycznej analizy, że treści są nielegalne (motyw 63 AUC).

Pozostawienie usługodawcom prawa do dokonywania oceny charakteru treści, w tym kwalifikowania ich do kategorii „oczywiście nielegalnych treści” i powiązanie wyniku tych ocen z sankcją polegającą na ograniczeniu świadczenia usług, nakładaną w drodze jednostronnej decyzji przez pośrednika internetowego, sytuuje podmioty prywatne na równi z podmiotami publicznymi, wyposażając je w szeroki zakres władztwa uprawniającego te podmioty do ingerowania w sferę praw podstawowych. Zaakceptowanie tego stanowiska

nakazuje zweryfikować pogląd dotyczący charakteru stosunków prawnych łączących pośredników internetowych z usługobiorcami, w szczególności podaje w wątpliwość ich kontraktowy charakter.

Jeśli jednak uznać, że stosunek prawny łączący dostawców usług cyfrowych z użytkownikami internetu ma charakter umowny, na co wskazuje gros postanowień zawartych w AUC, to wzmocnienie pozycji jednej strony tego stosunku prawnego, jakim są dostawcy usług, kosztem ich kontrahentów (odbiorców usług) skutkujące przyznaniem dostawcom uprawnień do dokonywania, w drodze jednostronnych oświadczeń woli, zmiany istotnych elementów łączącej strony umowy, stanowi rażące naruszenie interesów kontrahenta. Nawet bowiem zakładając, że pośrednicy internetowi dążyć będą do stworzenia zobiektywizowanego modelu przeprowadzania oceny zgłoszeń dokonywanych w ramach mechanizmu *notice and take down*, to nie eliminuje to ryzyka nadużyć polegających na nadmiernej, a zatem nieproporcjonalnej ingerencji w wolność wypowiedzi usługobiorców.

W efekcie przyjętych w AUC rozwiązań, wynik dokonywanej przez pośredników oceny legalności lub nielegalności treści, jest w większym stopniu wypadkową prowadzonych przez usługodawców spekulacji niż racjonalnej wykładni. Intuicyjne, niepoparte zobiektywizowaną wykładnią stanowisko jest jednak na gruncie AUC dopuszczalne i usprawiedliwione. AUC nie zawiera bowiem przepisów sankcjonujących wadliwe ustalenia, tak co do prawa, jak i co do faktów dokonywane przez pośredników internetowych. Od pośredników nie wymaga się bowiem ani tego, by weryfikowali pod kątem prawdziwości informacje zawarte w zgłoszeniach, ani by niewadliwie ustalali podstawę prawną decyzji stwierdzających nielegalność treści. W motywie 30 AUC wskazano jednoznacznie, że żadnego z przepisów rozporządzenia nie należy interpretować jako nałożenia na pośredników ogólnego obowiązku „aktywnego ustalania faktów”. Pośrednicy nie mają zatem obowiązku ustalania faktów, w szczególności dokonywania oceny prawdziwości informacji (motyw 74). Podobne zastrzeżenia dotyczą także bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych (motyw 109).

W konsekwencji, decyzje pośredników o nałożeniu ograniczeń podejmowane na podstawie dokonywanych – w tym także anonimowo (art. 16 ust. 2 lit. c AUC) – zgłoszeń dotyczyć mogą także „potencjalnie nielegalnych treści”, a zatem również wówczas, gdy istnieje jedynie prawdopodobieństwo,

że informacja może zawierać treści niezgodne z prawem. Terminem „potencjalnie nielegalne treści” ustawodawca europejski posługuje się w art. 17 ust. 3 lit. d AUC, wskazując, że w przypadku wydania przez usługodawcę decyzji dotyczącej „potencjalnie nielegalnych treści” usługodawca powinien wskazać podstawę prawną tej decyzji.

Mechanizm *notice and take down* funkcjonuje jako uzupełnienie mechanizmów zawiadamiania, w tym przez zaufane podmioty sygnalizujące, oraz dobrowolnie podejmowanych przez dostawców usług czynności wykrywających polegających w szczególności na filtrowaniu i monitorowaniu treści. Status „zaufanego podmiotu sygnalizującego” jest przyznawany na wniosek dowolnego podmiotu przez koordynatora ds. usług cyfrowych państwa członkowskiego, w którym wnioskodawca ma siedzibę, wnioskodawcy, który wykaże, że spełnia wszystkie następujące warunki:

- a) dysponuje szczególną wiedzą ekspercką i kompetencjami do celów wykrywania, identyfikowania i zgłaszania nielegalnych treści;
- b) jest niezależny od dostawców platform internetowych;
- c) podejmuje działania mające na celu dokonywanie zgłoszeń w sposób dokładny i obiektywny oraz z zachowaniem należytej staranności (art. 22 ust. 2 AUC).

Na gruncie zalecenia KE z 2018 r. zdefiniowano „zaufany podmiot sygnalizujący” jako „osobę fizyczną lub podmiot, który jest przez dostawcę usług hostingowych uważany za osobę fizyczną lub podmiot posiadający szczególną wiedzę fachową i odpowiedzialność w zakresie walki z nielegalnymi treściami w internecie” (Rozdział I lit. g zalecenia). Na dostawców platform internetowych nałożony został obowiązek zapewnienia priorytetowego traktowania zgłoszeń dokonywanych przez zaufane podmioty sygnalizujące. Obowiązek priorytetowego traktowania przez dostawców usług zgłoszeń dokonywanych przez „zaufane podmioty sygnalizujące” rozkłada ciężar ustalania przesłanki „nielegalności” treści pomiędzy te podmioty a dostawców.

Zaufany podmiot sygnalizujący jest łącznikiem pomiędzy organem publicznym, tj. pomiędzy koordynatorem ds. usług cyfrowych, a dostawcami usług. Okoliczność, że status zaufanego podmiotu jest nadawany przez koordynatora ds. usług cyfrowych, oraz wynikający z art. 22 ust. 1 AUC nakaz priorytetowego traktowania zgłoszeń pochodzących od podmiotów sygnalizujących sprowadza działalność dostawców usług do funkcji wykonawczej.

W praktyce bowiem trudno sobie wyobrazić, że pośrednicy internetowi będą kwestionować stanowisko podmiotów sygnalizujących. Zarazem podmioty te, z racji łączącego ich związku zależności od koordynatora ds. usług, będą realizować, jak należy się spodziewać cele organów publicznych, dokonując ustaleń w sposób odpowiadający realizowanej przez te organy polityce.

Podsumowując, należy stwierdzić, że ustanowione na gruncie AUC mechanizmy, tj. mechanizm *notice and take down* stanowiący uzupełnienie instytucji „zaufanych podmiotów sygnalizujących” legitymizują działania dostawców usług cyfrowych, w szczególności świadczących usługę hostingu, w zakresie, w jakim podejmują one aktywność polegającą na ograniczeniu świadczenia usług poprzez zmniejszanie widoczności treści, ich usuwanie, blokowanie, uniemożliwianie dostępu lub depozycjonowanie (art. 17 ust. 1 lit. a AUC). Zarówno mechanizm „zgłaszania i reagowania”, jak i działalność „zaufanych podmiotów sygnalizujących” zostały ukierunkowane na zwalczanie nielegalnych treści, a w konsekwencji na eliminowanie z obiegu publicznego i usuwanie z debaty publicznej niektórych informacji, uznanych za nielegalne lub szkodliwe. Wskazane w AUC mechanizmy, jakkolwiek ustanowione dla realizacji szczytnych celów, stanowią niebezpieczne narzędzie ingerujące w wolność wypowiedzi i swobodę debaty publicznej. Zastosowanie tych instrumentów powoduje, że na płaszczyźnie jednolitego rynku cyfrowego następuje odejście od klasycznych, znanych poza internetem, mechanizmów wytyczania granic swobody wypowiedzi i debaty publicznej, co uwidacznia się w usuwaniu z obiegu publicznego tych informacji i opinii, które bulwersują, oburzają lub wprowadzają niepokój. Idea „rynku opinii”, znana z klasycznego standardu wolności wypowiedzi, która zasadzała się na zaakceptowaniu jako pożądanych i użytecznych dla demokracji, nawet nieprawdziwych i oburzających wypowiedzi zostaje, na gruncie AUC, zastąpiona działaniem organów publicznych, które w sposób władczy wkraczają w sferę praw i wolności osobistych obywateli jednostronnie ustalając granice wolności wypowiedzi.

B. Ryzyko systemowe – środki prewencyjne

Obok mechanizmu „zgłaszania i reagowania” oraz powiązanego z nim systemu „zaufanych podmiotów sygnalizujących”, które to instrumenty stanowią formalną podstawę obligującą dostawców usług cyfrowych, w szczególności dostawców hostingu, do reagowania na szkodliwe lub nielegalne treści, przewidziano na gruncie AUC szczególne obowiązki adresowane do dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych nazywanych – na gruncie rozporządzenia ARC – strażnikami dostępu.

Status strażnika dostępu, zgodnie z decyzją KE z dnia 6 września 2023 r., posiada sześciu dostawców usług cyfrowych¹¹³. Zgodnie z art. 2 pkt 1 ARC „strażnik dostępu” oznacza przedsiębiorstwo – świadczące podstawowe usługi platformowe¹¹⁴ – które:

- a) wywiera znaczący wpływ na rynek wewnętrzny;
- b) świadczy podstawową usługę platformową będącą ważnym punktem dostępu, za pośrednictwem którego użytkownicy biznesowi docierają do użytkowników końcowych; oraz
- c) zajmuje ugruntowaną i trwałą pozycję w zakresie prowadzonej przez siebie działalności lub można przewidzieć, że zajmie taką pozycję w niedalekiej przyszłości.

Strażnicy dostępu ze względu na wpływ, jaki posiadają „na bezpieczeństwo w internecie, kształtowanie opinii publicznej i dyskursu publicznego, a także handel w internecie”, (motyw 79 AUC) mają obowiązek reagowania na ryzyko systemowe, badania prawdopodobieństwa wystąpienia takiego ryzyka,

¹¹³ Komisja Europejska wskazała 6 września 2023 r. po raz pierwszy sześciu strażników dostępu – firmy Alphabet, Amazon, Apple, ByteDance, Meta i Microsoft – na podstawie aktu o rynkach cyfrowych. Wskazaniem objęto łącznie 22 podstawowe usługi platformowe świadczone przez strażników dostępu; zob. akt o rynkach cyfrowych: Komisja wskazała sześciu strażników dostępu, https://poland.representation.ec.europa.eu/news/akt-o-rynkach-cyfrowych-straznicy-dostepu-2024-03-07_pl (dostęp: 25.11.2023).

¹¹⁴ Zgodnie z art. 2 pkt 2 ARC katalog podstawowych usług platformowych obejmuje: a) usługi pośrednictwa internetowego, b) wyszukiwarki internetowe, c) internetowe serwisy społecznościowe, d) usługi platformy udostępniania wideo, e) usługi łączności interpersonalnej niewykorzystujące numerów, f) systemy operacyjne, g) przeglądarki internetowe, h) wirtualnych asystentów, i) usługi przetwarzania w chmurze, j) internetowe usługi reklamowe, w tym sieci reklamowe, giełdy reklamowe i inne usługi pośrednictwa w zakresie reklam.

podejmowania środków zmniejszających ryzyko oraz reagowania na sytuację kryzysową, o ile taka wystąpi. W AUC nałożony został na platformy internetowe zakaz wprowadzania w błąd lub nakłaniania usługobiorców do określonego działania za pomocą zwodniczych interfejsów. Bardzo duże platformy internetowe mają zapobiegać rozpowszechnianiu dezinformacji. W tym celu w AUC znalazły się przepisy dotyczące ryzyka systemowego, a w szczególności obowiązkowej oceny ryzyka, środków ograniczających ryzyko, niezależnych audytów i przejrzystości systemów rekomendacji (algorytmów, które określają, co widzą użytkownicy)¹¹⁵.

Ryzyko systemowe powstaje w wyniku „funkcjonowania i korzystania z usług bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych, a także z potencjalnego nadużywania usług przez odbiorców usługi” (motyw 79). Istnieją cztery kategorie ryzyka systemowego:

- a) ryzyko rozpowszechniania nielegalnych treści za pośrednictwem ich usług;
- b) ryzyko wystąpienia faktycznych lub przewidywalnych negatywnych skutków dla wykonywania praw podstawowych, w szczególności prawa podstawowego do godności ludzkiej zapisanego w art. 1 Karty, do poszanowania życia prywatnego i rodzinnego zapisanego w art. 7 Karty, do ochrony danych osobowych zapisanego w art. 8 Karty, do wolności wypowiedzi i informacji, w tym wolności i pluralizmu mediów, zapisanego w art. 11 Karty, do niedyskryminacji zapisanego w art. 21 Karty, do przestrzegania praw dziecka zapisanego w art. 24 Karty i do wysokiej jakości ochrony konsumentów zapisanego w art. 38 Karty;
- c) ryzyko wystąpienia faktycznych lub przewidywalnych negatywnych skutków dla dyskursu obywatelskiego i procesów wyborczych oraz dla bezpieczeństwa publicznego;
- d) ryzyko wystąpienia faktycznych lub przewidywalnych negatywnych skutków w odniesieniu do przemocy ze względu na płeć, ochrony zdrowia publicznego i małoletnich, oraz poważnych negatywnych skutków dla fizycznego i psychicznego dobrostanu osoby (art. 34 ust. 1 AUC).

¹¹⁵ K. Sobczak, *UE: Powstają przepisy mające zwalczać nielegalne treści w internecie*, Prawo dla każdego, LEX/el.

Ustawodawca europejski stwierdza, że:

cztery kategorie ryzyka systemowego wymagają dogłębnej oceny ze strony dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych. Pierwsza kategoria dotyczy ryzyka związanego z rozpowszechnianiem nielegalnych treści, między innymi rozpowszechnianiem materiałów przedstawiających niegodziwe traktowanie dzieci w celach seksualnych lub nielegalne nawoływanie do nienawiści lub inne rodzaje nadużywania ich usług do celów przestępczych, a także dopuszczaniem się nielegalnych działań, takich jak sprzedaż produktów lub usług zakazanych prawem Unii lub prawem krajowym, w tym produktów niebezpiecznych lub podrobionych, oraz nielegalny handel zwierzętami. Na przykład takie rozpowszechnianie lub działania mogą stanowić znaczące ryzyko systemowe w przypadku, gdy dostęp do nielegalnych treści może szybko i szeroko rozprzestrzeniać się za pośrednictwem kont o szczególnie dużym zasięgu lub innych środków akcentujących. Dostawcy bardzo dużych platform internetowych oraz bardzo dużych wyszukiwarek internetowych powinni oceniać ryzyko rozpowszechniania nielegalnych treści niezależnie od tego, czy dane informacje są również niezgodne z warunkami korzystania z ich usług. Ocena ta pozostaje bez uszczerbku dla osobistej odpowiedzialności odbiorcy usługi bardzo dużych platform internetowych lub właścicieli stron internetowych indeksowanych przez bardzo duże wyszukiwarki internetowe za ewentualny nielegalny charakter ich działalności na podstawie obowiązującego prawa (motyw 80).

Druga kategoria dotyczy faktycznego lub przewidywalnego wpływu usługi na wykonywanie chronionych Kartą praw podstawowych, w tym godności ludzkiej, wolności wypowiedzi i informacji, w tym wolności i pluralizmu mediów, prawa do życia prywatnego, ochrony danych, prawa do niedyskryminacji, praw dziecka i ochrony konsumentów. Takie ryzyko może wystąpić np. w związku z projektem systemów algorytmicznych wykorzystywanych przez bardzo dużą platformę internetową lub bardzo dużą wyszukiwarkę internetową lub z nadużywaniem ich usług polegającym na dokonywaniu zgłoszeń stanowiących nadużycie lub stosowaniu innych metod tłumienia wypowiedzi lub ograniczania konkurencji (motyw 81 AUC).

Trzecia kategoria ryzyka dotyczy faktycznego lub przewidywalnego negatywnego wpływu na procesy demokratyczne, dyskurs obywatelski i procesy wyborcze, a także na bezpieczeństwo publiczne (motyw 82 AUC). Czwarta kategoria ryzyka wynika z podobnych obaw związanych z projektowaniem i funkcjonowaniem bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych lub korzystaniem z nich, w tym poprzez manipulację, co ma faktyczny lub przewidywalny negatywny wpływ na ochronę zdrowia publicznego, małoletnich oraz poważne negatywne konsekwencje dla fizycznego i psychicznego dobrostanu osoby, lub na przemoc ze względu na płeć. Takie ryzyko może również wynikać ze skoordynowanych kampanii dezinformacyjnych dotyczących zdrowia publicznego lub z projektowania interfejsów internetowych, które mogą stymulować uzależnienia behawioralne u odbiorców usług (motyw 83 AUC).

Wszystkie cztery rodzaje ryzyka składające się na ryzyko systemowe łączy jeden czynnik, a mianowicie korzystanie z wolności wypowiedzi. Ryzyko systemowe powstaje w wyniku nadużycia swobody wypowiedzi, przy czym tylko pierwsza kategoria ryzyka systemowego powstaje w wyniku nadużycia wolności wypowiedzi przez usługobiorców. Pozostałe trzy kategorie ryzyka – tj.:

1. ryzyko związane z naruszeniem praw podstawowych;
2. ryzyko związane z przebiegiem procesów demokratycznych oraz
3. ryzyko manipulacji zasobami informacji i danych – powstają jako rezultat działania dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek.

Nie ulega wątpliwości, że pierwsza kategoria ryzyka związana z rozpowszechnieniem nielegalnych treści powstaje jako rezultat zachowania się usługobiorców. Inaczej mówiąc, ryzyko to by nie istniało, gdyby nie rozpowszechnianie przez usługobiorców nielegalnych treści. W odniesieniu do drugiej kategorii ryzyka stwierdzić natomiast należy, że z całą pewnością ryzyko to także powstaje w wyniku rozpowszechnienia nielegalnych treści, jednakże uzyskuje ono postać kwalifikowaną (tj. staje się ryzykiem systemowym) nie dlatego, że działania usługobiorców generują obawę o powstanie ponadprzeciętnej szkody lub krzywdy, lecz obawa ta powstaje ze względu na niepewne, nieprzewidywalne zachowanie się pośredników internetowych. Ze względu bowiem na ich niejednolite, zatem niekiedy nadmierne, a niekiedy nieproporcjonalnie wstrzemięźliwe reakcje, które skutkują wysokim

pozycjonowaniem niektórych treści przy jednoczesnym depozycjonowaniu innych, generuje powstanie ryzyka związanego z naruszeniem praw podstawowych. Pośrednicy internetowi posiadając takie narzędzia jak moderowanie treści, zarządzanie obrazem, w szczególności układem interfejsów oraz monitorowanie, ograniczanie i pozycjonowanie treści, *de facto* sztucznie „podbijają” wagę niektórych informacji kosztem innych, co w konsekwencji prowadzić może do naruszenia praw podstawowych usługobiorców, zarówno tych, na których żądanie doszło do rozpowszechnienia treści, jak i tych, którzy jedynie uzyskują do niej dostęp. Gdyby zatem nie następowało włączenie się do debaty pośredników internetowych, którzy co prawda nie dostarczają treści, lecz nią – co jest ważniejsze – zarządzają, ryzyko systemowe, kwalifikowane w AUC jako drugi rodzaj ryzyka, miałoby jedynie śladowe znaczenie.

Należy zwrócić uwagę, że ryzyka naruszenia praw podstawowych w związku z rozpowszechnieniem nielegalnych lub szkodliwych treści (druga kategoria ryzyka systemowego) nie tylko nie da się wyeliminować, ale próby jego wyeliminowania są szkodliwe dla tych samych praw podstawowych, które działanie to miałoby chronić. Usunięcie ryzyka musiałoby się bowiem wiązać z prewencyjnym usuwaniem jeszcze nierozpowszechnionych treści ze względu na podejrzenie, że są one nielegalne. Skutkiem takiego działania byłoby zaniechanie prowadzenia debaty publicznej na jakikolwiek temat ze względu na ryzyko rozpowszechnienia potencjalnie nielegalnych treści.

Należy wskazać, że rodzaj ryzyka określony w AUC jako druga kategoria ryzyka systemowego, wymieniona także w art. 34 ust. 1 lit. b AUC, towarzyszy każdej debacie polegającej na wymianie poglądów i przytaczaniu twierdzeń, choćby miały się one ostatecznie okazać nieprawdziwe lub niesłuszne. Opinie i twierdzenia mają zarazem wartość właśnie z tego powodu, że pomimo ich dotkliwości i dyskomfortu, jaki wywołują, są społecznie użyteczne i nie powinny uchodzić za bezprawne. Próba prewencyjnego eliminowania takich treści z przestrzeni publicznej jest zatem szkodliwa dla debaty publicznej, a w konsekwencji prowadzi do jej ustania. Ryzyko systemowe (druga kategoria) powstaje zatem nie dlatego, że usługobiorcy rozpowszechniają nielegalne treści, ale jest ono wynikiem kierunkowego i celowego nimi zarządzania przez pośredników internetowych.

Nie jest zarazem bez znaczenia, że wejście w życie AUC niczego nie zmienia w odniesieniu do zasad, zakresu i trybu ponoszenia odpowiedzialności

usługobiorców za rozpowszechniane przez nich treści. W motywie 27 AUC podkreśla się, że:

Chociaż w przepisach niniejszego rozporządzenia dotyczących odpowiedzialności dostawców usług pośrednich skoncentrowano się na wyłączeniu odpowiedzialności dostawców usług pośrednich, należy przypomnieć, że pomimo ogólnie istotnej roli, jaką odgrywają tacy dostawcy, problemu nielegalnych treści i działań w internecie nie należy rozwiązywać, skupiając się wyłącznie na odpowiedzialności i obowiązkach takich dostawców. W miarę możliwości osoby trzecie, poszkodowane przez nielegalne treści przekazywane lub przechowywane w internecie, powinny starać się rozwiązywać konflikty związane z takimi treściami bez angażowania odpowiednich dostawców usług pośrednich. Odbiorców usługi należy pociągać do odpowiedzialności, jeżeli stanowią tak mające zastosowanie przepisy prawa Unii i prawa krajowego określające taką odpowiedzialność, za nielegalne treści, które przekazują i mogą rozpowszechniać publicznie za pomocą usług pośrednich. W stosownych przypadkach w zapobieganiu rozpowszechnianiu nielegalnych treści w internecie, zgodnie z mającymi zastosowanie przepisami prawa, powinny również pomagać inne podmioty, takie jak moderatorzy grup w zamkniętych środowiskach internetowych, w szczególności w przypadku dużych grup. Ponadto w przypadku gdy konieczny jest udział dostawców usług społeczeństwa informacyjnego, w tym dostawców usług pośrednich, wszelkie żądania lub nakazy dotyczące takiego udziału należy co do zasady kierować do konkretnego dostawcy posiadającego techniczną i operacyjną możliwość podjęcia działań przeciwko określonym nielegalnym treściom, aby zapobiec ewentualnym negatywnym skutkom dla dostępności i osiągalności informacji, które nie stanowią nielegalnych treści, oraz zminimalizować takie skutki.

Również trzeci i czwarty rodzaj ryzyka systemowego powstaje w wyniku działania pośredników internetowych. Błędne jest założenie obciążające, a w konsekwencji także przypisujące odpowiedzialność za ich powstanie usługobiorcom. O ile w odniesieniu do czwartej kategorii ryzyka ustawodawca europejski założył, że ryzyko to wynika z obaw związanych z projektowaniem i funkcjonowaniem bardzo dużych platform internetowych i bardzo dużych

wyszukiwarek internetowych, w tym korzystaniem z nich, w tym poprzez manipulację, to jednak nadal jako sprawców tego ryzyka wskazuje się usługobiorców. Nie wykluczając, że odbiorcy w różnych celach – w tym także przestępnych – wykorzystują dostępne narzędzia internetowe i informatyczne, to jednak dowodzi to tylko tego, że narzędzia te nie są odpowiednio zabezpieczone. Zaniechanie dostawców usług pośrednich w zakresie zapewnienia, by prowadzona w internecie debata była zbliżona do debaty w świecie realnym, a zatem, w szczególności, by żaden z uczestników debaty nie był w niej nadreprezentowany lub arbitralnie depozycjonowany, generuje powstanie wskazanych powyżej rodzajów ryzyka.

Nałożone na strażników dostępu obowiązki obejmujące wdrażania środków zmniejszających ryzyko, a także przeprowadzania corocznych audytów dotyczących, w szczególności, stosowania mechanizmu *notice and take down* oraz priorytetowego traktowania zgłoszeń dokonywanych przez zaufane podmioty sygnalizujące, wymuszają na dostawcach usług angażowanie się w działalność polegającą nie tylko na zwalczaniu, lecz także przeciwdziałaniu rozpowszechnianiu nielegalnych treści. Zgodnie z art. 35 ust. 1 AUC strażnicy dostępu mają obowiązek wdrażania „rozsądnych, proporcjonalnych i skutecznych środków zmniejszających ryzyko, dopasowanych do konkretnego ryzyka systemowego, ze szczególnym uwzględnieniem wpływu takich środków na prawa podstawowe”.

Zaangażowanie się strażników dostępu w realizację nałożonych przez UE obowiązków zmniejszania ryzyka systemowego *de facto* oznacza przeciwdziałanie powstawania takiego ryzyka, a zatem przyjmowanie przez strażników dostępu rozwiązań, które będą stymulowały zachowania usługobiorców w internecie. Stymulowanie zachowań stanowi *per se* samoistną i najbardziej idącą ingerencję w prawa podstawowe. Strażnicy dostępu będą zatem występowali w charakterze wychowawców stosujących wobec usługobiorców odpowiednie bodźce, w tym uzależniając świadczenie usług od modelowych wzorców zachowań. UE wymaga od strażników dostępu, by zważywszy na poszczególne kategorie ryzyka systemowego, „dostosowali swój projekt, jego cechy lub funkcjonowanie usług, a także dostosowali warunki korzystania

z usług i ich egzekwowanie oraz dostosowali procesy moderowania treści” (art. 35 ust. 1 lit. a–c AUC)¹¹⁶.

Stymulowanie zachowań jest nie do pogodzenia z prawem jednostek do respektowania wolności i swobód. Zalegalizowanie takich zachowań powoduje istotną zmianę w modelu wolności wypowiedzi. Zmiana ta polega przede wszystkim na tym, że na gruncie AUC dopuszczalne staje się sankcjonowanie zachowań jeszcze niedokonanych, pozostających dopiero w zamiarze, przy czym ocena nagannego charakteru takiego zachowania następuje na podstawie prawdopodobieństwa, że do niego dojdzie. Strażnicy dostępu mogą zatem ograniczać świadczenie usług już wówczas, gdy powezmą podejrzenie o potencjalnie nielegalnych treściach (art. 17 ust. 3 lit. d AUC). Zastosowana przez dostawców usług sankcja przyjmuje jedną z postaci ograniczenia świadczenia usługi, przy czym zastosowane ograniczenie, ze względu na jego istotę, zawsze oddziałuje na sferę wolności wypowiedzi usługodawcy.

¹¹⁶ Obok wymienionych w niniejszym akapicie obowiązków, z postanowień zawartych w art. 35 ust. 1 wynika, że na dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych nałożone zostały, w celu przeciwdziałania i zmniejszania ryzyka systemowego, także inne obowiązki, tj.: a) testowanie i dostosowywanie ich systemów algorytmicznych, w tym systemów rekomendacji; b) dostosowanie ich systemów reklam i przyjęcie ukierunkowanych środków mających na celu ograniczenie lub dostosowanie prezentowania reklam w związku ze świadczoną przez nich usługą; c) wzmocnienie wewnętrznych procesów, zasobów, testowania, dokumentowania lub nadzoru nad ich działaniami, w szczególności w zakresie wykrywania ryzyka systemowego; d) inicjowanie lub dostosowanie współpracy z zaufanymi podmiotami sygnalizującymi zgodnie z art. 22 oraz wykonywanie decyzji organów pozasądowego rozstrzygania sporów na podstawie art. 21; e) inicjowanie lub dostosowanie współpracy z innymi dostawcami platform internetowych lub wyszukiwarek internetowych za pomocą kodeksów postępowania i protokołów kryzysowych, o których mowa w, odpowiednio, art. 45 i 48; f) podejmowanie działań uświadamiających i dostosowywanie ich interfejsu internetowego w celu udzielenia odbiorcom usługi większej ilości informacji; g) podejmowanie ukierunkowanych działań w celu ochrony praw dziecka, w tym stosowanie narzędzi weryfikacji wieku i kontroli rodzicielskiej, narzędzi mających na celu pomaganie małoletnim sygnalizować niegodziwe traktowanie lub, w stosownych przypadkach, uzyskanie wsparcia; h) zapewnienie, aby informację – bez względu na fakt czy stanowi ona wygenerowany lub zmanipulowany obraz, treść dźwiękową lub treść wideo, które ludzko przypominają istniejące osoby, obiekty, miejsca lub inne podmioty lub zdarzenia, przez co osoba będąca ich odbiorcą niesłusznie uznaje je za autentyczne lub prawdziwe – można było rozróżnić dzięki widocznym oznaczeniom, gdy prezentuje się ją na ich interfejsach internetowych, oraz dodatkowo udostępnienie łatwej w użyciu funkcji umożliwiającej odbiorcom usługi wskazanie takiej informacji.

Świadomość rozmiarów wpływu, jaki strażnicy dostępu wywierają na rynek wewnętrzny¹¹⁷, która legła u podstaw wdrożenia rozwiązań zawartych w rozporządzeniach cyfrowych, powoduje, że przyjęte w AUC i ARC rozwiązania stanowią element inżynierii społecznej. Stały się one skutecznym, a zarazem społecznie usprawiedliwionym, w ocenie organów UE, instrumentem ograniczania wolności wypowiedzi realizowanym w całej UE na podstawie zharmonizowanych przepisów prawa zawartych w AUC i ARC.

C. Wykonywanie nakazów

Wobec zaistnienia okoliczności uzasadniających podejrzenie, że działalność dostawcy usług cyfrowych albo działalność odbiorcy tych usług są niezgodne z rozporządzeniem (AUC), organy administracyjne, sądowe i organy ścigania mogą wydawać nakazy, których celem jest zapobieżenie dalszym naruszeniom i przywrócenie stanu zgodnego z prawem. Nakazy odpowiedniego zachowania mogą być zatem wydawane zarówno w toku postępowań, jak i przed ich wszczęciem, a także – jako rozstrzygnięcia merytoryczne – w wyniku ich zakończenia.

Nakazy sądowe oraz nakazy wydawane przez organy administracji publicznej mogą stanowić formalną podstawę czynności podejmowanych przeciwko nielegalnym treściom. Zważywszy, że są one wymierzone, co do zasady, w aktywność polegającą na rozpowszechnianiu treści, ich skutkiem jest ograniczenie wolności wypowiedzi. Nakazy mogą zobowiązywać do zaprzestania naruszania lub zapobieżenia mu, w tym również usunięcia nielegalnych treści określonych w takich nakazach lub uniemożliwienia dostępu do nich (motyw 25 AUC).

¹¹⁷ We wniosku KE do PE w sprawie przyjęcia ARC wskazano, że pełniąc funkcję strażników dostępu, platformy takie wywierają znaczny wpływ na rynki cyfrowe, mają znaczną kontrolę nad dostępem do rynków cyfrowych oraz mają na nich ugruntowaną pozycję, w wyniku czego wielu użytkowników biznesowych w znacznym stopniu jest uzależnionych od wspomnianych strażników dostępu, co w niektórych przypadkach skutkuje nieuczciwym postępowaniem wobec tych użytkowników biznesowych. Ponadto ma to również niekorzystny wpływ na kontestowalność podstawowych usług platformowych. Takiego wpływu nie da się wyeliminować w ramach podejmowanych przez państwa członkowskie inicjatyw regulacyjnych, które bez działania na szczeblu UE mogłyby skutkować fragmentacją rynku wewnętrznego (ARC).

W polskiej doktrynie prawa zauważono, że „pojęcie nakazu sądowego, dobrze znane innym systemom prawnym, w zasadzie nie pojawia się w polskich opracowaniach”¹¹⁸. Według klasycznych definicji właściwych dla reżimu *common law* – nakaz (*injunction*) to postanowienie sądu nakazujące pewne działanie lub zapobiegające jego podjęciu (*a court order commanding or preventing an action*). Jego odmianą jest *permanent injunction*, tj. nakaz wydawany po ostatecznym rozpatrzeniu sprawy co do jej istoty¹¹⁹. Na gruncie krajowych rozwiązań instytucja nakazu sądowego stanowić może zarówno jeden ze składników sentencji wyroku, jak i może być odrębnym, wydanym w danej sprawie orzeczeniem¹²⁰.

Ustawodawca europejski wskazał, że w zależności od systemu prawnego każdego państwa członkowskiego i odnośnej dziedziny prawa, krajowe organy sądowe lub administracyjne mogą nakazać dostawcom usług pośrednich podjęcie działań przeciwko pewnym określonym nielegalnym treściom. Takie nakazy, w szczególności, gdy dotyczą one zapobiegania przez dostawcę ponownemu pojawieniu się danych nielegalnych treści, należy wydawać zgodnie z prawem Unii, zwłaszcza z zakazem nakładania ogólnych obowiązków nadzoru, zgodnie z wykładnią Trybunału Sprawiedliwości Unii Europejskiej¹²¹.

Dopuszczalność wydawania nakazów oraz ich zakres przedmiotowy i terytorialny wynika zarówno z tego, który organ (organ sądowy, organ administracyjny, organ ścigania) wydał nakaz, jak i z tego, jaki akt prawny stanowił podstawę jego wydania (prawo krajowe, prawo UE) oraz z tego, czy nakaz został wydany w ramach toczącego się postępowania jako środek zabezpieczający, czy ma charakter rozstrzygnięcia merytorycznego.

Nakaz może dotyczyć zarówno udzielenia informacji, jak i podjęcia wskazanych w jego treści czynności zmierzających do usunięcia lub zablokowania dostępu do nielegalnych treści. Adresatem nakazu są, co do zasady, dostawcy usług pośrednich, w szczególności strażnicy dostępu, jednakże – jak wynika z motywu 141 AUC oraz art. 51 ust. 1 lit. a – mogą być nimi także „inne osoby,

¹¹⁸ C. Celińska-Grzegorzczuk, *Sądowa kontrola administracji publicznej*, t. 10, R. Hauser, Z. Niewiadomski, A. Wróbel (red.), Warszawa 2016, s. 668 (System Prawa Administracyjnego).

¹¹⁹ Tamże, s. 669.

¹²⁰ M. Baran, *Europeizacja prawa administracyjnego*, t. 3, R. Hauser, Z. Niewiadomski, A. Wróbel (red.), Warszawa 2014, s. 408 (System Prawa Administracyjnego).

¹²¹ Wniosek ARC, s. 4.

działające w celach związanych z ich działalnością handlową, gospodarczą, rzemieślniczą lub zawodową, w przypadku których można zasadnie oczekiwać, że dysponują informacjami związanymi z podejrzeniem naruszenia rozporządzenia” (art. 51 ust. 1 lit. a AUC). W szczególności tak krajowi koordynatorzy ds. usług cyfrowych, jak i Komisja Europejska będą mogli, powołując się na potrzebę zwalczania nielegalnych treści, zażądać nie tylko od dostawców usług pośrednich, lecz także „wszelkich innych osób fizycznych lub prawnych”¹²² zarówno udzielenia informacji, jak i określonego zachowania – działania lub zaniechania.

Podstawę prawną wydawanych nakazów stanowić mogą przepisy zawarte w – innych niż AUC – aktach prawa krajowego i prawa UE, o których naruszenie podejrzewa się usługobiorców lub dostawców usług cyfrowych w związku z rozpowszechnieniem nielegalnych treści w internecie¹²³. Warunki i wymogi określone w AUC, które mają zastosowanie do nakazów podjęcia działań przeciwko nielegalnym treściom, pozostają – jak wskazano w motywie 34 – bez uszczerbku dla innych aktów Unii, w których przewidziano podobne systemy podejmowania działań przeciwko konkretnym rodzajom nielegalnych treści, takich jak rozporządzenie (UE) 2021/784¹²⁴, rozporządzenie

¹²² Zgodnie z motywem 142 AUC Komisja powinna mieć możliwość zażądania bezpośrednio – w drodze należycie uzasadnionego wniosku o udzielenie informacji – od odpowiedniego dostawcy bardzo dużej platformy internetowej lub bardzo dużej wyszukiwarki internetowej, a także od wszelkich innych osób fizycznych lub prawnych działających w celach związanych z ich działalnością handlową, gospodarczą, rzemieślniczą lub zawodową, w przypadku których można zasadnie oczekiwać, że dysponują informacjami związanymi z podejrzeniem naruszenia lub naruszeniem, stosownie do przypadku, przekazania wszelkich istotnych dowodów, danych i informacji. Ponadto na potrzeby niniejszego rozporządzenia Komisja powinna mieć możliwość zwrócenia się o wszelkie istotne informacje do dowolnego organu publicznego, podmiotu lub agencji w państwie członkowskim.

¹²³ Zgodnie z motywem 34 AUC przyjęto, że odpowiednie organy krajowe powinny mieć możliwość wydawania takich nakazów w odniesieniu do treści uznanych za nielegalne lub nakazów udzielenia informacji na podstawie prawa Unii lub prawa krajowego zgodnego z prawem Unii, w szczególności z Kartą, i kierowania tych nakazów do dostawców usług pośrednich, w tym dostawców mających siedzibę w innym państwie członkowskim.

¹²⁴ Rozporządzenie w sprawie treści terrorystycznych.

(UE) 2019/1020¹²⁵ lub rozporządzenie (UE) 2017/2394¹²⁶, w którym przyznano szczególne uprawnienia do wydawania nakazu udzielenia informacji organom ścigania w zakresie ochrony konsumentów państw członkowskich, natomiast warunki i wymogi mające zastosowanie do nakazów udzielenia informacji pozostają bez uszczerbku dla innych aktów Unii zawierających podobne odpowiednie przepisy dla poszczególnych sektorów. Zawsze zatem gdy dopuszczalne jest wydanie na podstawie przepisów szczególnych, w tym sektorowych, przez organy sądowe lub administracyjne rozstrzygnięcia albo zastosowanie środków zabezpieczających, mogą zostać nim objęci także dostawcy usług cyfrowych oraz usługobiorcy.

Nakazy mogą być wydawane zarówno przez organy administracji krajowej, właściwe w zakresie usług cyfrowych (koordynator ds. usług cyfrowych), jak i Komisję Europejską oraz krajowe i europejskie organy sądowe oraz organy ścigania.

Koordinator ds. usług cyfrowych, jako organ krajowy „odpowiedzialny za nadzorowanie dostawców usług pośrednich i egzekwowanie rozporządzenia” (art. 49 ust. 1 AUC), jest uprawniony do:

1. żądania od wszelkich podmiotów, tj. zarówno dostawców usług, jak i osób fizycznych i prawnych, udzielenia informacji dotyczących naruszenia rozporządzenia AUC;
2. prowadzenia kontroli lub zwrócenia się do organu sądowego w ich państwie członkowskim o nakazanie przeprowadzenia kontroli we wszelkich pomieszczeniach, których tacy dostawcy lub takie osoby używają do celów związanych z ich działalnością handlową, gospodarczą, rzemieślniczą lub zawodową, lub do żądania tego od innych organów publicznych w celu zbadania, zajęcia, wykonania lub uzyskania kopii informacji związanych z podejrzeniem naruszenia w jakiejkolwiek postaci, niezależnie od nośnika, na jakim są przechowywane;

¹²⁵ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1020 z dnia 20 czerwca 2019 r. w sprawie nadzoru rynku i zgodności produktów oraz zmieniające dyrektywę 2004/42/WE oraz rozporządzenia (WE) nr 765/2008 i (UE) nr 305/2011 (Dz.U. UE L Nr 169, s. 1).

¹²⁶ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/2394 z dnia 12 grudnia 2017 r. w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów i uchylające rozporządzenie (WE) nr 2006/2004 (Dz.U. UE L Nr 345, s. 1 z późn. zm.).

3. żądania, aby członek personelu lub przedstawiciel takich dostawców lub osób złożył wyjaśnienia w odniesieniu do wszelkich informacji związanych z podejrzeniem naruszenia oraz do rejestracji za ich zgodą, za pomocą wszelkich środków technicznych, odpowiedzi (art. 51 ust. 1 lit. a–c AUC).

Koordinatorom ds. usług cyfrowych przysługuje, w szczególności, uprawnienie do nakazania zaprzestania naruszeń i, w stosownych przypadkach, nakładania środków zaradczych proporcjonalnych do naruszenia i niezbędnych do skutecznego zakończenia naruszenia lub zwrócenia się do organu sądowego w ich państwie członkowskim o dokonanie takich czynności (art. 51 ust. 2 lit. c AUC), a także uprawnienie do przyjmowania środków tymczasowych lub zwrócenia się do właściwego krajowego organu sądowego w ich państwie członkowskim o przyjęcie środków tymczasowych, aby zapobiec ryzyku wyrządzenia poważnych szkód (art. 51 ust. 2 lit. e AUC). W AUC zastrzeżono, że jakikolwiek nakazany środek musi być proporcjonalny do charakteru, ciężaru, powtarzalności i czasu trwania naruszenia i nie może ograniczać w nienależyty sposób dostępu odbiorców danej usługi do zgodnych z prawem informacji.

Koordinator krajowy jako organ właściwy w sprawach usług cyfrowych, w tym przede wszystkim odpowiedzialny za zapewnienie przestrzegania aktu o usługach cyfrowych (AUC) został wyposażony w uprawnienie do prowadzenia postępowań sprawdzających oraz postępowań wykonawczych (art. 51 ust. 1 i 2 AUC). Nadto – uzupełniając – na wypadek, gdyby koordinator uznał, że pomimo wcześniej zastosowanych środków „dostawca usług pośrednich nie spełnił w wystarczający sposób wymogów i, że naruszenie nie zostało usunięte lub nadal trwa i wyrządza poważne szkody oraz że naruszenie to wiąże się z przestępstwem zagrażającym życiu lub bezpieczeństwu osób” – koordinator może zwrócić się do sądu o nakazanie zastosowanie środka najbardziej dolegliwego zarówno dla dostawcy usług, jak i usługobiorców, tj. tymczasowego ograniczenia dostępu odbiorców do usługi, której dotyczy naruszenie (art. 51 ust. 3 AUC). Ograniczenie dostępu do usługi może być nakazane na cztery tygodnie, z zastrzeżeniem możliwości, którą dysponuje właściwy organ sądowy, i która polega na umożliwieniu za pomocą wydanego nakazu koordinatorowi ds. usług cyfrowych przedłużenia tego okresu o kolejne okresy tej samej długości, z zastrzeżeniem maksymalnej liczby przedłużeń określonej przez ten organ sądowy (art. 51 ust. 3 lit. b AUC).

Koordinator ustanowiony w danym państwie członkowskim współpracuje z koordynatorami krajowymi innych państw UE, z Radą Usług Cyfrowych i Komisją oraz organami krajowymi (art. 49 ust. 2 AUC). Państwa członkowskie mają obowiązek zagwarantować autonomię koordynatorom w wykonywaniu swoich zadań, a w szczególności zapewnić, by koordynator był niezależny od innych krajowych organów publicznych (art. 50 ust. 2 AUC)¹²⁷, przy czym niezależność tę gwarantować ma „autonomia w zarządzaniu budżetem w ramach ogólnych limitów budżetowych, tak aby nie wpływać negatywnie na niezależność koordynatora ds. usług cyfrowych” (art. 50 ust. 1 AUC).

Najszerszy zakres uprawnień, w tym do stosowania środków tymczasowych nawet przed wszczęciem postępowania sprawdzającego (art. 65 ust. 1 AUC), został przyznany Komisji Europejskiej. Zgodnie z art. 70 AUC w toku postępowań w przypadkach naglących ze względu na ryzyko wyrządzenia poważnej szkody odbiorcom usługi, Komisja może, w drodze decyzji, przyjąć środki tymczasowe przeciwko danemu dostawcy bardzo dużej platformy internetowej lub bardzo dużej wyszukiwarki internetowej na podstawie stwierdzenia naruszenia *prima facie*. Na gruncie AUC przyjęto, że Komisja powinna mieć możliwość zażądania bezpośrednio – w drodze należycie uzasadnionego wniosku o udzielenie informacji – od odpowiedniego dostawcy bardzo dużej platformy internetowej lub bardzo dużej wyszukiwarki internetowej, a także od wszelkich innych osób fizycznych lub prawnych działających w celach związanych z ich działalnością handlową, gospodarczą, rzemieślniczą lub zawodową, w przypadku których można zasadnie oczekiwać, że dysponują informacjami związanymi z podejrzeniem naruszenia lub naruszeniem, stosownie do przypadku, przekazania wszelkich istotnych dowodów, danych i informacji. Ponadto przyjęto, że Komisja powinna mieć możliwość zwrócenia się o wszelkie istotne informacje do dowolnego organu publicznego, podmiotu lub agencji w państwie członkowskim (motyw 142).

Nakazy mogą dotyczyć udzielenia informacji, a także podjęcia działań przeciwko nielegalnym treściom. Nakazy udzielenia informacji dotyczą przedstawienia konkretnych informacji na temat indywidualnych odbiorców

¹²⁷ Zgodnie z tym przepisem: „Podczas wykonywania swoich zadań i uprawnień zgodnie z niniejszym rozporządzeniem koordynatorzy ds. usług cyfrowych działają w sposób w pełni niezależny. Pozostają oni wolni od jakichkolwiek bezpośrednich i pośrednich wpływów zewnętrznych, nie zwracają się do żadnego innego organu publicznego ani podmiotu prywatnego o instrukcje, ani nie przyjmują takich instrukcji”.

danej usługi pośredniej wskazanych w tych nakazach w celu ustalenia, czy odbiorcy usług przestrzegają mających zastosowanie przepisów Unii lub przepisów krajowych (motyw 37 AUC). Takie nakazy zobowiązują do udzielenia informacji mających na celu umożliwienie identyfikacji odbiorców danej usługi. W związku z tym wymogi dotyczące udzielenia informacji nie obejmują nakazów odnoszących się do informacji na temat grupy odbiorców usługi, którzy nie są wyraźnie wskazani, w tym nakazów udzielenia zbiorczych informacji wymaganych do celów statystycznych lub kształtowania polityki opartej na dowodach. Dostawca usług pośrednich powinien bez zbędnej zwłoki informować organ wydający o wszelkich działaniach następczych (motyw 33 AUC).

Nakazy podjęcia działań przeciwko nielegalnym treściom i udzielenia informacji podlegają przepisom zabezpieczającym kompetencje państwa członkowskiego, w którym dostawca, do którego skierowany jest nakaz, ma siedzibę, oraz przepisom ustanawiającym w niektórych przypadkach możliwe odstępstwa od tych kompetencji, określone w art. 3 dyrektywy 2000/31/WE, o ile spełniono warunki wymienione w tym artykule. Biorąc pod uwagę, że przedmiotowe nakazy odnoszą się odpowiednio do określonych nielegalnych treści i informacji, w przypadku gdy są skierowane do dostawców usług pośrednich z siedzibą w innym państwie członkowskim, co do zasady nie ograniczają one swobody tych dostawców w zakresie transgranicznego świadczenia usług (motyw 38 AUC).

W razie wydania nakazu adresowanego do dostawcy usług cyfrowych, nie może on chronić się przed jego wykonaniem, powołując się na wskazany w art. 4–6 AUC kontratyp neutralności. Ustawodawca europejski przesądził na gruncie AUC, że zawarte w tych przepisach okoliczności wyłączające odpowiedzialność nie mają wpływu na ocenę dopuszczalności wydawania różnego rodzaju nakazów wobec dostawców usług pośrednich. Także w odniesieniu do udostępniania treści online, zgodnie z dyrektywą 2004/48/WE Parlamentu Europejskiego i Rady¹²⁸, właściwe organy sądowe mają możliwość wystawiania nakazów przeciwko pośrednikowi, którego usługi są wykorzystywane przez osobę trzecią do naruszania prawa własności intelektualnej¹²⁹.

¹²⁸ Dyrektywa 2004/48/WE Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie egzekwowania praw własności intelektualnej (Dz.U. UE L Nr 157, s. 45).

¹²⁹ Zalecenie Komisji UE 2018/334 z dnia 1 marca 2018 r. w sprawie działań na rzecz skutecznego zwalczania nielegalnych treści w internecie (Dz.U. UE L Nr 63, s. 50).

Wskazuje się w AUC, że krajowy organ sądowy lub administracyjny wydający nakaz, którym może być również organ ścigania, powinien zrównoważyć cel, jaki nakaz ma osiągnąć, zgodnie z podstawą prawną umożliwiającą jego wydanie, z prawami i prawnie uzasadnionymi interesami wszystkich osób trzecich, na które nakaz może mieć wpływ, w szczególności z ich prawami podstawowymi wynikającymi z Karty. W szczególności w kontekście transgranicznym nakaz powinien być w zasadzie skuteczny tylko na terytorium wydającego nakaz państwa członkowskiego, chyba że nielegalny charakter treści wynika bezpośrednio z prawa Unii lub organ wydający nakaz uważa, że odpowiednie prawa wymagają szerszego zakresu terytorialnego, zgodnie z prawem Unii i prawem międzynarodowym oraz przy uwzględnieniu interesów kurtuazji międzynarodowej (motyw 36 AUC).

Akt o usługach cyfrowych nie zawiera postanowień dotyczących środków i mechanizmów odwoławczych, jakie winny przysługiwać podmiotom, wobec których zastosowane zostały nakazy AUC¹³⁰. Obowiązek ustanowienia „skutecznego środka ochrony” sędowano na państwa członkowskie, wskazując, że „państwa członkowskie powinny przestrzegać podstawowego prawa do skutecznego środka prawnego i dostępu do bezstronnego sądu” (motyw 39 AUC). W art. 51 ust. 5 AUC postanowiono, że państwa członkowskie ustanawiają szczególne zasady i procedury dotyczące wykonania uprawnień przez koordynatorów ds. usług cyfrowych, a zatem także wydawanych przez nich nakazów:

¹³⁰ W motywie 39 wskazano, że wymogi dotyczące udzielania informacji o mechanizmach odwoławczych, dostępnych dla dostawcy usługi pośredniej i odbiorcy usługi, który przekazał treści, obejmują wymóg udzielenia informacji na temat administracyjnych mechanizmów rozpatrywania skarg oraz sądowych środków odwoławczych, w tym odwołań od nakazów wydanych przez organy sądowe. Ponadto koordynatorzy ds. usług cyfrowych mogą opracować krajowe narzędzia i wytyczne dotyczące mechanizmów wnoszenia skarg i mechanizmów odwoławczych mających zastosowanie na ich terytorium, aby ułatwić odbiorcom usługi dostęp do takich mechanizmów. Ponadto stosując niniejsze rozporządzenie, państwa członkowskie powinny przestrzegać podstawowego prawa do skutecznego środka prawnego i dostępu do bezstronnego sądu ustanowionego w art. 47 Karty. Niniejsze rozporządzenie nie powinno zatem uniemożliwiać odpowiednim krajowym organom sądowym lub administracyjnym wydawania, na podstawie mającego zastosowanie prawa Unii lub prawa krajowego, nakazu przywrócenia treści, w przypadku gdy treści te były zgodne z warunkami korzystania z usług dostawcy usług pośrednich, ale zostały błędnie uznane przez tego dostawcę za nielegalne i usunięte.

zapewniając, aby wykonywanie tych uprawnień podlegało odpowiednim zabezpieczeniom ustanowionym w mającym zastosowanie prawie krajowym zgodnym z Kartą oraz z ogólnymi zasadami prawa Unii. W szczególności takie środki przyjmuje się wyłącznie w zgodności z prawem do poszanowania życia prywatnego i prawem do obrony, w tym z prawem do bycia wysłuchanym i prawem dostępu do akt, oraz z zastrzeżeniem prawa do skutecznego środka prawnego przysługujących wszystkim stronom, których środki dotyczą.

Postępowanie prowadzone przed Komisją Europejską, a także przed koordynatorem ds. usług cyfrowych ma charakter quasi-inkwizycyjny¹³¹. Zgodnie z motywem 139 AUC przyjęto, że Komisja powinna korzystać:

z pewnego marginesu uznaniowości, jeżeli chodzi o decyzje o wszczęciu postępowania przeciwko dostawcom bardzo dużych platform internetowych lub bardzo dużych wyszukiwarek internetowych.

Komisja – jak przyjęto w AUC – powinna także móc z własnej inicjatywy badać naruszenia, zgodnie z uprawnieniami przewidzianymi w AUC, m.in. poprzez zwracanie się o dostęp do danych, o informacje lub przeprowadzanie kontroli, a także poprzez korzystanie ze wsparcia koordynatorów ds. usług cyfrowych (motyw 138). Komisja powinna mieć możliwość koordynowania działań i korzystania z wiedzy eksperckiej i zasobów (motyw 137), powinna być także uprawniona do przeprowadzania kontroli niezbędnych do egzekwowania odpowiednich przepisów rozporządzenia (motyw 141).

¹³¹ Proces inkwizycyjny charakteryzuje się skupieniem w ręku organu procesowego trzech funkcji, tj. rozstrzygania sporu, oskarżenia i obrony oskarżonego. W procesie inkwizycyjnym organ procesowy występuje zatem w roli oskarżyciela, obrońcy i arbitra. W postępowaniu tym nie występują strony bądź rola ich jest bardzo ograniczona. W końcu należy wyróżnić formę mieszaną, czyli proces mieszany, w którym nastąpiło połączenie elementów formy skargowej oraz inkwizycyjnej. W procesie mieszanym formę inkwizycyjną ma z reguły postępowanie przedsądowe (przygotowawcze) oraz postępowanie wykonawcze, a formę skargową – postępowanie sądowe (J. Skorupka, *Istnienie stron procesowych*, [w:] T. Grzegorzczak, *System Prawa Karnego Procesowego. Dopuszczalność procesu*, t. 4, M. Jeż-Ludwichowska, A. Lach (red. nauk.), Warszawa 2015, s. 434).

Rola stron w tych postępowaniach jest zasadniczo sprowadzona do wykonywania nakazów wydawanych przez te organy, a także, w razie gdy sposób lub zakres wykonania nakazów jest – w ocenie tych organów – niezadowalający, sprowadza się do obowiązku wykonania zastosowanych przez sąd na wniosek koordynatora środków tymczasowych. Ustawodawca europejski zapewnia co prawda zaskarżalność decyzji wydanych przez te organy, ale także środki tymczasowe i zabezpieczające. Komisja przypomina ponadto, że właściwe organy krajowe mogły już na gruncie wcześniejszych przepisów wydawać nakazy wobec dostawców usług pośrednich, których usługi są wykorzystywane do rozpowszechniania nielegalnych treści w internecie. KE jest zdania, że to niezwykle ważne, aby właściwe organy krajowe szybko identyfikowały takie nielegalne treści w internecie i wydawały nakazy ich usunięcia na gruncie swoich systemów krajowych. Z art. 9 rozporządzenia (UE) 2022/2065 jasno wynika, że takie nakazy mogą być wydawane w wymiarze transgranicznym. Ze względu na ryzyko incydentów sprawą najwyższej wagi jest, by właściwe organy gromadziły wszelkie niezbędne dowody, żeby umożliwić stosowanie skutecznych środków w przypadku nagłaśniania w internecie nielegalnych treści dotyczących często groźnych przestępstw, oraz aby organy te korzystały z uprawnień przyznanych im na mocy różnych instrumentów prawa Unii w celu zwalczania nielegalnych treści.

3. Przestanki legalizujące ingerencję w wolność wypowiedzi (granice ograniczeń)

A. *Ex post* – test szkodliwości

W ujęciu normatywnym ograniczenie wolności wypowiedzi stanowi ingerencję w podstawowe prawa i wolności człowieka i obywatela. Wolność wypowiedzi została zaliczona w polskiej Konstytucji¹³² do wolności i praw osobistych¹³³.

¹³² Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. Nr 78, poz. 483 z późn. zm.)

¹³³ Gwarancje wolności wypowiedzi zostały zawarte w art. 54 Konstytucji RP usytuowanym w podrozdziale II zatytułowanym *Wolności i prawa osobiste*.

Na gruncie europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności stanowi wartość ogólnospołeczną, a zarazem jest warunkiem *sine qua non* rozwoju osobistego człowieka i obywatela. Europejski Trybunał Praw Człowieka wolność wypowiedzi nazywa „filarem demokratycznego społeczeństwa, podstawą jego rozwoju i warunkiem samorealizacji jednostki”¹³⁴.

Zarówno na gruncie prawa ponadnarodowego, jak i w prawie krajowym państw stron europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności, a także państw członkowskich UE, wolność wypowiedzi, pomimo wysokiej rangi w hierarchii wartości prawnie chronionych, nie stanowi wartości absolutnej¹³⁵ i może – jak wynika *explicite* z treści art. 10 ust. 2 EKPC:

odpowiadać takim wymogom formalnym, warunkom, ograniczeniom i sankcjom, jakie są przewidziane przez ustawę i niezbędne w społeczeństwie demokratycznym w interesie bezpieczeństwa państwowego, integralności terytorialnej lub bezpieczeństwa publicznego ze względu na konieczność zapobieżenia zakłóceniu porządku lub przestępstwu, z uwagi na ochronę zdrowia i moralności, ochronę dobrego imienia i praw innych osób oraz ze względu na zapobieżenie ujawnieniu informacji poufnych lub na zagwarantowanie powagi i bezstronności władzy sądowej.

Ograniczenie wolności wypowiedzi jest także dopuszczalne na gruncie polskiej Konstytucji. Zgodnie z art. 31 ust. 3 Konstytucji:

Ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw.

¹³⁴ Wyrok ETPC w sprawie Handyside przeciwko Wielkiej Brytanii, § 49.

¹³⁵ Trybunał Konstytucyjny zauważył, że wolności wyrażone w art. 14 i art. 54 ust. 1 Konstytucji nie mają w państwach demokratycznych wymiaru absolutnego. Ich ograniczeniem jest odpowiedzialność, której rola polega na stworzeniu równowagi między niejednokrotnie sprzecznymi dążeniami i celami podmiotów realizujących swe konstytucyjne prawa (Zob. Wyrok TK z dnia 12 maja 2008 r., SK 43/05, OSNP A 2008, nr 4, poz. 57).

O ile ograniczenie wolności wypowiedzi jest – co do zasady – dopuszczalne, to jednak może zostać usprawiedliwione (zalegalizowane) tylko wówczas, gdy ma charakter następczy, co bywa nazywane cenzurą represyjną. Cenzura występuje bowiem w dwóch formach – „jako cenzura prewencyjna, poddająca kontroli przygotowane do rozpowszechnienia wypowiedzi bądź jako cenzura represyjna, dopuszczająca odpowiedzialność za nadużycie wolności wypowiedzi”¹³⁶. W art. 54 ust. 2 Konstytucji RP ustrojodawca wprost zakazał cenzury prewencyjnej środków społecznego przekazu oraz koncesjonowania prasy. Ustrojodawca nie zakazuje natomiast cenzury represyjnej¹³⁷.

Cenzura prewencyjna *sensu stricto* to „znajdujące się w rękach władzy państwowej narzędzie kształtowania i utrzymywania pewnej ideologii; dotyczy wszelkich środków komunikacji społecznej, w szczególności zaś prasy”¹³⁸. Jak zauważa J. Sobczak, w orzecznictwie Trybunału Konstytucyjnego ugruntowany został pogląd, że jednym z elementów wolności słowa jest wolność od cenzury prewencyjnej¹³⁹. Trybunał Konstytucyjny stwierdzał bowiem wielokrotnie, że:

jednym z elementów istoty wolności słowa jest wolność od cenzury prewencyjnej, rozumianej jako przyznanie organom państwowym kompetencji do kontrolowania treści wypowiedzi przed ich przekazaniem odbiorcy, a także do uzależnienia przekazania wypowiedzi odbiorcom od uprzedniej zgody organu państwowego. Państwo może ustanawiać mechanizmy następczej odpowiedzialności za nadużycie wolności słowa, natomiast ingerencja uprzednia może być dopuszczona tylko wyjątkowo, jako uboczny efekt innych, legitymowanych konstytucyjnie działań państwa (np. ścigania przestępstw czy zapewnienia prawidłowego działania wymiaru sprawiedliwości)¹⁴⁰.

¹³⁶ J. Sobczak, Hasło: *cenzura*, [w:] *Leksykon terminów medialnych: A–L*, K. Wolny-Zmorzyński (red.), Toruń 2024, s. 104.

¹³⁷ Tamże, s. 105.

¹³⁸ E. Nowińska, *Wolność wyrażania poglądów a cenzura prewencyjna. Próba interpretacji Konstytucji*, [w:] *Wolność wypowiedzi prasowej*, Warszawa 2007, s. 55.

¹³⁹ Tamże, s. 105.

¹⁴⁰ Uchwała TK z dnia 2 marca 1994 r., W 3/93, OSNAP 1994, nr 1, poz. 17.

Wynikający z art. 54 ust. 2 Konstytucji zakaz cenzury prewencyjnej wiąże także sądy orzekające w sprawach o ochronę dóbr osobistych i obejmuje zakaz stosowania środków ochrony równoważnych względem takiej cenzury¹⁴¹.

Nałożenie sankcji za nadużycie wolności wypowiedzi może zatem następować, ale – co do zasady – tylko *ex post*, tj. w następstwie rozgłoszenia wypowiedzi oraz w rezultacie przeprowadzenia sądowej oceny treści i formy wypowiedzi oraz zachowania sprawcy (autora wypowiedzi lub innej osoby, która przyczyniła się do rozpowszechnienia szkodliwej wypowiedzi). W doktrynie zauważa się, że zakaz cenzury prewencyjnej istnieje *erga omnes* i odnosi się nie tylko do władzy państwowej i zakazu stanowienia norm prawnych umożliwiającego wprowadzanie cenzury prewencyjnej, ale także do podmiotów prywatnych i organizacji społecznych, które „nie mogą dokonywać cenzury prewencyjnej i tworzyć jakichkolwiek organów do jej przeprowadzenia, w tym organów społecznych”¹⁴². E. Nowińska podkreśla, że:

Cenzura może być wprowadzona zarówno przez organizacje niepaństwowe (np. Kościół), jak i państwowe. W reżimach totalitarnych i autorytarnych polega ona na szczegółowym badaniu przez specjalne organy wypowiedzi pod kątem tego, czy nie zawierają treści, które mogłyby być uznane za wyraz protestu przeciwko systemowi politycznemu lub sprawującym władzę¹⁴³.

Obecnie – jak zauważono w literaturze – zasadniczo w żadnym państwie demokratycznym nie ma zinstytucjonalizowanej formy cenzury prewencyjnej. Gwarantuje się za to wolność wypowiedzi z zastrzeżeniem, iż wolność ta nie może naruszać innych praw, w tym bezpieczeństwa i dobrego imienia zarówno obywateli, jak i państwa i jego organów¹⁴⁴.

W przeciwieństwie do cenzury prewencyjnej, nie zakazuje się w ustawodawstwach państw demokratycznych stosowania cenzury represyjnej. Nawet jednak następcze ograniczenia wolności wypowiedzi nie może przybierać dowolnej postaci ani następować w dowolny sposób, w szczególności

¹⁴¹ Wyrok SN z dnia 19 października 2023 r., II CSKP 13/22, LEX nr 3617342.

¹⁴² E. Nowińska, *Wolność wyrażania poglądów...*, s. 105.

¹⁴³ Tamże, s. 45.

¹⁴⁴ Tamże, s. 55.

nie może pozostawać poza kontrolą sądu jako bezstronnego i stosującego zobiektywizowane kryteria oceny organu upoważnionego do zapewnienia równowagi ochrony i praw konstytucyjnych i konwencyjnych wartości, które w okolicznościach faktycznych danej sprawy pozostają w kolizji.

Ingerencja w wolność wypowiedzi jednostki, by mogła zostać uznana za dopuszczalną (legalną), wymaga przeprowadzenia kontroli następczej dokonywanej przez organy wymiaru sprawiedliwości. W pierwszej kolejności będą to sądy krajowe, a po wyczerpaniu drogi krajowej kompetencje do ustalenia zakresu i dopuszczalności ingerencji w wolność wypowiedzi należeć będą do sądów i trybunałów międzynarodowych, przy czym rozpoznanie sprawy następuje przed organami międzynarodowej kontroli sądowej.

Powyższe spostrzeżenia prowadzą do wniosku, że – po pierwsze – na gruncie klasycznego, pozainternetowego standardu wolności wypowiedzi (standard offline), co do zasady, za niedopuszczalne, a zatem niemieszczące się w tym standardzie, było uznawane działanie polegające na zakazaniu rozpowszechnienia wypowiedzi, po drugie – za niezgodne z tym standardem należałoby uznać także działanie niepoparte nakazem sądowym polegające na ingerowaniu w wolność wypowiedzi jednostki, a także – po trzecie – ingerowanie w wolność wypowiedzi było nieuprawnione, jeśli ingerencja nie spełniła zobiektywizowanych kryteriów oceny jej skutków (szkodliwości) dla praw i wolności jednostki oraz wartości ogólnospołecznych, w szczególności takich jak swobodna debata publiczna w sprawach budzących powszechne zainteresowanie. Za nadmierne, nieusprawiedliwione i niezgodne z prawem uchodziło zatem, na gruncie klasycznego standardu (standardu offline), takie działanie, które ma charakter arbitralny i następuje w rezultacie decyzji podjętej poza kontrolą sądową, a przedmiotem tej decyzji jest jeszcze nierozpowszechniona wypowiedź (*ex ante*).

Ustalanie granicy wolności wypowiedzi stanowiło, na gruncie klasycznego standardu, prerogatywę sądów. Tylko zarazem organy wymiaru sprawiedliwości były upoważnione do dokonywania wiążącej oceny dopuszczalności ingerowania w wolność wypowiedzi, w szczególności poprzez usuwanie wypowiedzi, ograniczanie do niej dostępu lub nakładanie sankcji na autora. Organy wymiaru sprawiedliwości dokonywały legalności ograniczenia przy zastosowaniu kryteriów (przesłanek) zawartych w art. 10 ust. 2 EKPC, a na gruncie prawa polskiego ocena ta następowała przy uwzględnieniu art. 31 ust. 3 Konstytucji RP. Zawarte w tych przepisach kryteria oceny są w doktrynie

ujmowane jako tzw. trójstopniowy (trójelementowy) test¹⁴⁵ albo jako test szkodliwości (ang. *harm test*)¹⁴⁶.

Sformułowany w orzecznictwie ETPC ogólny test (ang. *harm test*) oceny zgodności ograniczenia swobody wypowiedzi z art. 10 EKPC składa się z trzech podstawowych przesłanek¹⁴⁷. Po pierwsze, ograniczenie swobody wypowiedzi musi być przewidziane przez prawo (kryterium legalności). Po drugie, ograniczenie tego prawa podstawowego musi służyć ochronie jednej z wartości wymienionych w art. 10 ust. 2 EKPC (kryterium celowości). Po trzecie, zastosowane w konkretnej sprawie ograniczenie musi być konieczne w demokratycznym społeczeństwie (kryterium niezbędności).

Kryterium legalności jest spełnione, gdy ograniczenie swobody wypowiedzi ma oparcie w przepisach prawa krajowego oraz przepisy te są sformułowane w taki sposób, że jednostka samodzielnie lub po konsultacji z prawnikiem może racjonalnie przewidzieć konsekwencje prawne swojego zachowania¹⁴⁸. Nie jest przy tym konieczne, by konsekwencje te były „absolutnie pewne”¹⁴⁹, ponieważ od prawodawcy krajowego nie można oczekiwać stanowienia wyłącznie kazuistycznie sformułowanych przepisów. Dozwolone jest zatem posługiwanie się pojęciami nieostryimi, których ostateczna treść zostanie sprecyzowana dopiero w praktyce stosowania¹⁵⁰ przez organy administracji lub sądy krajowe. Jak wskazuje Sąd Najwyższy¹⁵¹, należy

¹⁴⁵ I.C. Kamiński, *Ograniczenia swobody wypowiedzi...*, s. 43; także: P. Ślęzak, *Ograniczenia swobody wypowiedzi*, [w:] *Prawo mediów*, P. Ślęzak (red.), Warszawa 2020, pkt 1.3.8; K. Kunc-Urbańczyk, *Wprowadzenie*, [w:] *Prawo sztucznej inteligencji i nowych technologii 2*, B. Fischer, A. Pązik, M. Świerczyński (red.), Warszawa 2022; A. Hańderek, *Uwagi na tle art. 35 pr. aut.*, [w:] A. Hańderek, *Naruszenie praw autorskich i praw pokrewnych w związku z funkcjonowaniem wyszukiwarek internetowych*, Warszawa 2024.

¹⁴⁶ J. Sobczak, *Komentarz do art. 8*, [w:] *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz. Tom I (art. 1–89)*, D. Miąsik, N. Półtorak, A. Wróbel (red.), Warszawa 2012; K. Chałubińska-Jentkiewicz, J. Taczkowska-Olszewska, *Świadczenie usług drogą elektroniczną. Komentarz*, Warszawa 2019, s. 145; G. Szpor, *Jawność i jej ograniczenia. Idee i pojęcia*, t. 1, Warszawa 2016, s. 24.

¹⁴⁷ Wyrok SN z dnia 2 lipca 2013 r., III SK 42/12, OSNP 2014, nr 11, poz. 163.

¹⁴⁸ Wyroki ETPC: w sprawie VgT Verein Gegen Tierfabriken przeciwko Szwajcarii, § 52 i 55; w sprawie Sigma Radio Television Ltd. przeciwko Cyprowi, § 194.

¹⁴⁹ Wyrok ETPC w sprawie VgT Verein Gegen Tierfabriken przeciwko Szwajcarii, § 55.

¹⁵⁰ Wyroki ETPC: w sprawie VgT Verein Gegen Tierfabriken przeciwko Szwajcarii, § 55; w sprawie Sigma Radio Television Ltd. przeciwko Cyprowi, § 194.

¹⁵¹ Wyrok SN z dnia 2 lipca 2013 r., III SK 42/12, OSNP 2014, nr 11, poz. 163.

wymienić np., że za „przewidziane prawem” ograniczenie swobody wypowiedzi uznano ustawowy zakaz reklamy politycznej i jego zastosowanie do reklamy stowarzyszenia zajmującego się ochroną zwierząt, która to reklama zachęcała do ograniczenia spożycia mięsa¹⁵².

Kryterium celowości odnosi się z kolei do powodów ograniczenia swobody wypowiedzi. Wartościami najczęściej uwzględnianymi jako uzasadniające ingerencję w swobodę wypowiedzi jest ochrona praw innych osób oraz moralności publicznej¹⁵³.

Kryterium konieczności wymaga zaś stwierdzenia, czy ingerencja w swobodę wypowiedzi uzasadniona była istnieniem pilnej potrzeby społecznej, czy interwencja była proporcjonalna do realizacji zgodnego z prawem celu oraz czy wskazane przez organy administracji lub sądy powody tej interwencji były właściwe i wystarczające¹⁵⁴. Przy analizie przesłanki konieczności ograniczenia swobody wypowiedzi uwzględnia się kontekst historyczny i społeczny, w jakim wyrażono opinię, w tym zaszłości historyczne. Na tej podstawie ograniczenie swobody wypowiedzi polegające na zakazie posługiwania się plakatami kampanii społecznej dotyczącej ochrony zwierząt pod hasłem „Holocaust na Twoim talerzu” w Niemczech uznano za uzasadnione z uwagi na trywializację losu ofiar Holocaustu¹⁵⁵. Uwzględnia się także rodzaj medium, za pośrednictwem którego dana wypowiedź została rozpowszechniona. Wreszcie, ocenia się również przysługujący państwom stronom Konwencji margines swobody ocen. Margines ten jest, zgodnie z dotychczasową linią orzecniczą ETPC, węższy w przypadku wypowiedzi dotyczących spraw o znaczeniu publicznym (zwanych także sprawami budzącymi publiczne zainteresowanie lub ważnymi sprawami publicznymi) w porównaniu ze swobodą wypowiedzi komercyjnej¹⁵⁶.

¹⁵² Wyrok ETPC w sprawie VgT Verein Gegen Tierfabriken przeciwko Szwajcarii, § 57–58.

¹⁵³ Wyroki ETPC: w sprawie Sigma Radio Television Ltd. przeciwko Cyprowi, § 196; w sprawie Peta Deutschland przeciwko Niemcom, § 44.

¹⁵⁴ Wyrok ETPC w sprawie Sigma Radio Television Ltd. przeciwko Cyprowi, § 199; w sprawie Peta Deutschland przeciwko Niemcom, § 45.

¹⁵⁵ Wyrok ETPC w sprawie Peta Deutschland przeciwko Niemcom, § 48–49. Bierze się pod uwagę rodzaj i surowość sankcji (tamże, § 50).

¹⁵⁶ Wyroki ETPC: w sprawie VgT Verein Gegen Tierfabriken przeciwko Szwajcarii, § 70–71; w sprawie Peta Deutschland przeciwko Niemcom, § 46.

W orzecznictwie ETPC, jak zauważył Sąd Najwyższy¹⁵⁷, zwraca się także uwagę na to, czy środki wyrazu użyte w wypowiedzi, z tytułu której jednostka doznała ograniczenia swobody wypowiedzi, przyczyniają się do debaty o sprawach publicznych¹⁵⁸. Tendencja ta jest wyraźna przede wszystkim w sprawach, w których dochodzi do kolizji między prawem do prywatności a swobodą wypowiedzi, niemniej w piśmiennictwie bazującym na tego rodzaju orzeczeniach wskazuje się, że aby dana wypowiedź w środkach masowego przekazu korzystała z szerszej ochrony przysługującej wypowiedziom dotyczącym spraw o znaczeniu publicznym, konieczne jest, aby treść wypowiedzi, oceniana obiektywnie, odnosiła się do zagadnienia o znaczeniu publicznym i wzbogacała dyskusję, jaka wokół tego zagadnienia się toczy¹⁵⁹.

Podobnie, jak ma to miejsce w ramach standardu konwencyjnego, konstytucyjna wolność wypowiedzi może doznawać ograniczeń w związku z art. 31 ust. 3 Konstytucji¹⁶⁰, o ile ograniczenia te są przewidziane w ustawie, są konieczne dla ochrony wymienionych w tym przepisie wartości (w szczególności moralności publicznej) oraz będą dotyczyły korzystania z tej wolności, nie naruszając przy tym jej istoty. W zakresie dotyczącym kontroli konstytucyjności interwencji prawodawcy w sferę wolności mediów i swobody wypowiedzi Trybunał Konstytucyjny opowiedział się za szczególnie surową kontrolą precyzji przepisów wprowadzających ograniczenia w korzystaniu z tej wolności¹⁶¹. Orzecznictwo konstytucyjne potwierdza wszakże, iż dozwolone jest wprowadzanie przez ustawodawcę różnych form odpowiedzialności za rozpowszechnione treści¹⁶². Zwrócić należy również uwagę, że analogicznie jak ma to miejsce w standardzie konwencyjnym, w orzeczeniu Trybunału Konstytucyjnego z dnia 7 czerwca 1994 r. uznano za dopuszczalne wprowadzenie przez władzę publiczną ograniczeń wolności słowa dalej idących w przypadku środków masowego przekazu o szerokim spektrum oddziaływania niż w sytuacjach, gdy przekazywanie podobnej lub nawet identycznej treści miałoby miejsce wobec ograniczonego kręgu odbiorców¹⁶³.

¹⁵⁷ Wyrok SN z dnia 2 lipca 2013 r., III SK 42/12, OSNP 2014, nr 11, poz. 163.

¹⁵⁸ Wyrok ETPC w sprawie Axel Springer AG przeciwko Niemcom, § 90.

¹⁵⁹ Wyrok ETPC w sprawie Leempoel przeciwko Belgii.

¹⁶⁰ Wyrok TK z dnia 12 maja 2008 r., SK 43/05.

¹⁶¹ Wyrok TK z dnia 23 marca 2006 r., K 4/06.

¹⁶² Wyrok TK z dnia 9 listopada 2010 r., K 13/07.

¹⁶³ Wyrok TK z dnia 7 czerwca 1994 r., K 17/93, OSNAP 1994, cz. I, poz. 11.

Trójelementowy test stanowi narzędzie wykorzystywane w toku kontroli sądowej w odniesieniu do tych kategorii wypowiedzi, które korzystają z ochrony konwencyjnej. Niektóre wypowiedzi nie korzystają jednak z dobrodziejstwa ochrony z art. 10 Konwencji¹⁶⁴. Dotyczy to wypowiedzi, które miały na celu odejście od jego faktycznego celu poprzez wykorzystanie prawa do wolności wypowiedzi w sposób jednoznacznie sprzeczny z wartościami Konwencji. Podstawę dokonania takiej oceny stanowi art. 17 EKPC, zgodnie z którym „żadne z postanowień konwencji nie może być interpretowane jako przyznanie jakiegokolwiek państwu, grupie lub osobie prawa do podjęcia działań lub dokonania aktu zmierzającego do zniweczenia praw i wolności wymienionych w niniejszej konwencji albo ich ograniczenia w większym stopniu, niż to przewiduje konwencja”. Kwestią rozstrzygającą w świetle art. 17 jest to, czy celem wypowiedzi jest podżeganie do nienawiści lub przemocy, lub czy poprzez takie wypowiedzi dąży się do powołania się na Konwencję w sposób pozwalający na prowadzenie działalności lub popełnianie czynów w zamiarze zniweczenia praw i wolności w Konwencji chronionych¹⁶⁵.

Jak zauważono we wcześniejszych fragmentach rozważań, na gruncie AUC zasadnicze znaczenie dla ustalenia zakresu i zasad ochrony wolności wypowiedzi ma nie tyle wynik stosowanego – na etapie sądowym – testu szkodliwości, co przede wszystkim wynik oceny prejudycjalnej, która nie jest, co do zasady, dokonywana przez sądy, lecz przez Komisję Europejską i powiązane z nią krajowe organy nadzorcze, a także przez dostawców usług cyfrowych, w szczególności dostawców platform i wyszukiwarek internetowych na podstawie upoważnień zawartych w AUC. Kluczowe znaczenie ma zatem wynik dokonywanego przez te podmioty przedsądu, którego rezultatem jest kwalifikowanie wypowiedzi jako legalnych albo nielegalnych. Wypowiedzi nielegalne nie podlegają ochronie konwencyjnej, a w konsekwencji nie znajduje do nich zastosowania test szkodliwości. Nie można bowiem oceniać legalności wypowiedzi, która uprzednio została uznana przez upoważniony do tego organ za nielegalną. Podstawę dokonywania oceny stanowi art. 17 EKPC, zgodnie z którym ryzyko nadmiernego, naruszającego istotę wolności wypowiedzi ograniczenia pojawia się wówczas, gdy w miejsce organu

¹⁶⁴ Wyrok ETPC w sprawie *Belkacem* przeciwko Belgii.

¹⁶⁵ Tamże.

sądowego jego kompetencje przejmują inne podmioty publiczne lub prywatne. Wyposażenie tych podmiotów w upoważnienie do oceny legalności treści oraz usuwania treści, które te podmioty uznały za nielegalne, a nadto legitymowanie ich do działań polegających na filtrowaniu, monitorowaniu i blokowaniu treści jeszcze przed ich publicznym udostępnieniem, prowadzi do marginalizowania, a nawet trywializowania dotychczasowych wzorców ochrony i wyeliminowania narzędzi służących równoważeniu praw i wolności.

Problematyczny nie jest zatem sposób wytyczania granic wolności wypowiedzi przy zastosowaniu testu szkodliwości, ale wątpliwości budzi jego niestosowanie w odniesieniu do wypowiedzi uznanych za nielegalne oraz pozostawienie do uznania organów pozasądowych oceny, kwalifikacji i decyzji dotyczących odmowy przyznania ochrony niektórym wypowiedziom. W Rezolucji Parlamentu Europejskiego z dnia 20 października 2020 r. w sprawie aktu prawnego o usługach cyfrowych i związanych z nim kwestii z zakresu praw podstawowych¹⁶⁶, poprzedzającej uchwalenie aktu o usługach cyfrowych, PE wezwał dostawców usług cyfrowych do usuwania treści internetowych ocenionych jako nielegalne. PE uznał, że „niezbędne jest szybkie i konsekwentne usuwanie treści niezgodnych z prawem w celu zwalczania czynów zabronionych i naruszeń praw podstawowych” (pkt 3). PE przyznał zarazem, że wystarczające jest, by oceny takiej dokonywali dostawcy usług, a przy kwalifikacji treści jako nielegalnych i ich usuwaniu „zachowali staranność, proporcjonalność i zasadę niedyskryminacji, z należyтым uwzględnieniem wszystkich okoliczności dotyczących praw podstawowych użytkowników” (pkt 4). W efekcie stosowanie trójelementowego testu straciło na znaczeniu, albowiem realne wytyczanie ram wolności wypowiedzi i budowanie nowego standardu (standard online) następuje na etapie oceny przedsądowej wykonywanej przez organy niejurydyczne i dokonywanej poza kontrolą niezależnych i niezawisłych sądów.

¹⁶⁶ Akt prawny o usługach cyfrowych i związane z nim kwestie z zakresu praw podstawowych, Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. w sprawie aktu prawnego o usługach cyfrowych i związanych z nim kwestii z zakresu praw podstawowych.

B. Antycypacyjne (*ex ante*)

Pakiet cyfrowy (AUC i ARC) odwraca zasady reagowania na nadużycia wolności wypowiedzi, wprowadzając – w miejsce kontroli następczej – mechanizmy legitymizujące dokonywanie uprzedniej oceny treści i formy wypowiedzi (*ex ante*) i upoważnia do jej wykonywania dostawców usług cyfrowych, w szczególności pośredników internetowych świadczących usługę hostingu (dostawców platform internetowych). Wszystkie nałożone w AUC na dostawców platform internetowych obowiązki legalizują *de facto* stosowane już wcześniej, tj. przed przyjęciem AUC, przez pośredników narzędzia kontroli treści, a nadto wyposażają i usprawiedliwiają stosowanie nowych instrumentów reagowania na potencjalne, prawdopodobne lub rzeczywiste nadużycia prawa w internecie, w tym wolności wypowiedzi.

Nawet prawo do sądu, potwierdzone w art. 21 ust. 1 akapit 3 AUC, obejmuje wyłącznie roszczenia *ex post*, które odbiorca usługi może skierować przeciwko dostawcy usług cyfrowych dopiero wówczas, gdy pośrednik internetowy faktycznie dokonał już ograniczenia świadczonej usługi i to niezależnie od tego, czy wskazaną przez pośrednika podstawę ograniczenia stanowiło naruszenie warunków świadczenia usługi (art. 14 ust. 1 AUC), czy przekonanie dostawcy o istniejącym niebezpieczeństwie (ryzyku) rozpowszechnienia nielegalnych treści (art. 16 i 17 AUC). W art. 21 ust. 1 akapit 3 wskazano, że zainteresowany odbiorca, niezależnie od mechanizmów pozasądowego rozstrzygania sporów oferowanych przez dostawcę usługi, ma prawo, na każdym etapie, wszcząć postępowanie sądowe przeciwko dostawcy usługi zgodnie z przepisami prawa krajowego¹⁶⁷. Zarazem jednak roszczenie to służy

¹⁶⁷ W tłumaczeniu na język polski art. 21 ust. 1 akapit 3 AUC pojawia się niejasność, która może prowadzić do błędnej interpretacji tego przepisu i jego nieprawidłowego zastosowania. W polskiej wersji językowej przepis ten ma brzmienie: „Akapit pierwszy pozostaje bez uszczerbku dla prawa zainteresowanego odbiorcy usługi do wszczęcia na każdym etapie postępowania w celu zaskarżenia tych decyzji przez dostawców platform internetowych przed sądem zgodnie z mającym zastosowanie prawem”. Wątpliwości może budzić *passus*: „[...] w celu zaskarżenia tych decyzji przez dostawców platform internetowych przed sądem [...]”. Nie jest bowiem jasne, który z podmiotów posiada legitymację do wszczynania postępowań sądowych – czy jest nim dostawca platformy, czy odbiorca. Prawo do sądu jest kluczowe dla realizacji pozostałych praw, na które mogą powoływać się odbiorcy usług, w tym wolności wypowiedzi. Konieczne jest zatem uchylenie istniejących wątpliwości w drodze sprostowania polskiej wersji językowej. W wersji

zakwestionowaniu decyzji uprzednio wydanych¹⁶⁸ przez dostawców platform. Ochrona interesu prawnego i faktycznego odbiorcy usługi jest zatem iluzoryczna. Nawet bowiem jeśli sąd podzieli stanowisko odbiorcy usługi i uchyli decyzje dostawcy platformy, to jednak faktycznie wystąpił już niekorzystny dla odbiorcy skutek, w szczególności wówczas, gdy przedmiotem sądowej oceny była dopuszczalność (legalność) treści lub formy wypowiedzi.

Ustanowiony w AUC mechanizm prewencyjnego i uprzedniego reagowania na rozpowszechnienie potencjalnie nielegalnych lub szkodliwych treści jest skomponowany z wielu składników. Należy do nich, w pierwszej kolejności, sposób normowania kontratypów, a także – co stanowi tego konsekwencję – znaczenie, jakie ustawodawca europejski nadaje obowiązkowi należytej staranności nałożonemu na dostawców usług. Po drugie, zapewnieniu skuteczności i efektywności systemu reagowania *ex ante* służą nowe, wykreowane w AUC narzędzia i instrumenty, w szczególności system tzw. zaufanych podmiotów reagujących na przypadki rozpowszechnienia nielegalnych treści, przy czym uzupełnienie zawartych w AUC regulacji stanowić będą inne akty prawne, w tym dyrektywa PE i Rady w sprawie ochrony osób zgłaszających naruszenia prawa Unii (dyrektywa o ochronie sygnalistów)¹⁶⁹. Po trzecie, zasadniczy składnik i trzon mechanizmu reagowania *ex ante* stanowi niejednorodny, otwarty, szeroki katalog uprawnień przyznanych Komisji Europejskiej, która uzyskała w AUC kompetencje do bezpośredniego i dyskrecyjnego reagowania w każdym przypadku i wobec każdego podmiotu, także wówczas, gdy Komisja stwierdziła *prima facie* naruszenie obowiązków wynikających z AUC przez dostawcę bardzo dużej platformy internetowej lub bardzo dużej wyszukiwarki internetowej.

francuskiej przepis ten ma następujące brzmienie: „Le premier alinéa est sans préjudice du droit du destinataire du service concerné d'engager, à tout moment, une procédure pour contester lesdites décisions prises par les fournisseurs de plateformes en ligne devant une juridiction conformément au droit applicable”. Z jego treści wynika jasno, że uprawnienie do wszczęcia postępowania przysługuje odbiorcom usług przeciwko dostawcom platform internetowych. Zarazem jednak roszczenie służy zakwestionowaniu wydanych uprzednio decyzji (fr. *pour contester lesdites décisions*) przez dostawców platform.

¹⁶⁸ W języku francuskim chodzi o passus: „pour contester lesdites décisions prises par les fournisseurs de plateformes en ligne”.

¹⁶⁹ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii (Dz.U. UE L Nr 305, s. 17 z późn. zm.).

Legalizowanie ingerencji *ex ante* w wolność wypowiedzi nie następuje ze względu na wyraźne przesądzenie w AUC albo w innym akcie prawa powszechnie obowiązującego o dopuszczalności zastosowania przez pośredników internetowych ograniczenia wolności wypowiedzi wobec usługobiorcy (użytkownika) przed wydaniem w tym zakresie prawomocnego orzeczenia sądowego, ale działania *ex ante* są legalizowane poprzez przyjęty zarówno w AUC i ARC, jak i w DSM¹⁷⁰ mechanizm przypisywania odpowiedzialności za naruszenia prawa spowodowane rozpowszechnieniem wypowiedzi. Pośrednicy internetowi, podobnie jak dostawca usług udostępniania treści online, co ma miejsce na gruncie DSM, mogą uchylić się od ponoszenia odpowiedzialności za rozpowszechnienie nielegalnych lub szkodliwych treści po wykazaniu, że działali z należytą starannością. Warunkiem *sine qua non* uchylenia się od odpowiedzialności jest wykazanie przez pośrednika internetowego, inaczej niż na gruncie nieobowiązujących już przepisów zawartych w art. 12–15 dyrektywy 2000/31 o handlu elektronicznym¹⁷¹, gdzie warunkiem uzyskania ochrony było zachowanie przez pośrednika postawy pasywnej, że świadczy usługi z należytą starannością, a zatem konieczne jest wykazanie przez niego aktywności. O ile zatem na gruncie dyrektywy o handlu elektronicznym przesłanką wyłączenia odpowiedzialności było wykazanie przez pośredników neutralnej postawy i nieingerowania, niemoodyfikowania treści i nieinicjowania przekazu (komunikacji), o tyle na gruncie AUC i ARC, a także DSM, przesłanki te – co prawda – zostały utrzymane, ale ich stosowanie powiązano z oceną stopnia staranności pośredników przy wykonywaniu ich usług.

Działanie z należytą starannością jest, na gruncie AUC i ARC oraz DSM, kluczowym obowiązkiem dostawców usług (pośredników internetowych). W doktrynie wskazano, że „należyta staranność jest kluczową wartością wyrażoną w rozporządzeniu i jest ona rozumiana jako wymóg właściwego podejścia przez dostawców usług pośrednich do problemu nielegalnych treści,

¹⁷⁰ Dyrektywa DSM.

¹⁷¹ Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (Dz.U. UE L z 2000 r. Nr 178, s. 1 z późn. zm.).

dezinformacji online i innych zagrożeń społecznych”¹⁷². W myśl motywu 3 AUC „Odpowiedzialne zachowanie i działanie z należytą starannością dostawców usług pośrednich ma zasadnicze znaczenie dla bezpiecznego, przewidywalnego i godnego zaufania środowiska internetowego [...]”. Zgodnie z motywem 40 AUC konieczny jest „jasny, skuteczny, przewidywalny i wyważony zestaw zharmonizowanych obowiązków w zakresie należytej staranności dla dostawców usług pośrednich”. Na staranne działanie jako obowiązek wskazano także wprost w rozdziale III AUC zatytułowanym „Obowiązki w zakresie należytej staranności na potrzeby przejrzystego i bezpiecznego środowiska internetowego”. W myśl art. 7 AUC (klauzula dobrego samarytana) sposobem realizacji tego obowiązku jest „prowadzenie przez dostawców usług z własnej inicjatywy dobrowolnych czynności sprawdzających lub podejmowanie innych środków mających na celu wykrycie, identyfikację i usunięcie nielegalnych treści lub uniemożliwienie do nich dostępu”. Filtrowanie treści jest ze swej natury „środkiem zapobiegawczym” w ramach kontroli informacji rozpowszechnianych w tych usługach, a środki blokujące, które mogą z tego wynikać, stanowią „uprzednie ograniczenia” w rozumieniu orzecznictwa ETPC dotyczącego art. 10 EKPC¹⁷³. Rzecznik generalny wskazał, że uzasadnieniem dla stosowania kontroli *ex ante* jest cel, „by nie karać, ale zapobiec ewentualnym naruszeniom prawa. Informacje, które użytkownicy zamierzają umieścić online, są kontrolowane, a informacje uznawane za mogące powodować takie naruszenie podlegają ograniczeniu przed ich rozpowszechnieniem”¹⁷⁴. W tych sytuacjach, zdaniem Rzecznika, użytkownicy nie mają zatem „swobody” w zakresie zamieszczania online treści według własnej woli. Środki filtrowania i blokowania stosowane przez ich dostawców ograniczają treści, które użytkownicy ci mogą zamieszczać. Wynika z tego „ingerencja” w korzystanie z wolności komunikacji przez wspomnianych użytkowników. Filtrowanie i blokowanie treści przed ich

¹⁷² D. Lubasz, *Artykuł 1*, [w:] *Akt o usługach cyfrowych. Komentarz*, D. Lubasz, M. Namysłowska (red.), Warszawa 2024.

¹⁷³ Wyroki ETPC: w sprawie Ahmet Yildirim przeciwko Turcji, § 55; z dnia 23 czerwca 2020 r. w sprawie Kharitonov przeciwko Rosji, § 36; a także: z dnia 30 kwietnia 2019 r. w sprawie Kablis przeciwko Rosji, § 90.

¹⁷⁴ Opinia Rzecznika Generalnego w sprawie RP przeciwko PE i Radzie, pkt. 79.

rozpowszechnieniem pociągają ponadto za sobą „ingerencję” w powszechną wolność otrzymywania informacji¹⁷⁵.

Na gruncie AUC, jak wskazano w art. 7, działanie polegające na wykonywaniu „dobrowolnych czynności sprawdzających lub podejmowaniu innych środków mających na celu wykrycie, identyfikację i usunięcie nielegalnych treści lub uniemożliwienie do nich dostępu” nie wyłącza możliwości powoływania się przez dostawców usług na przesłanki dotyczące neutralności zawarte w art. 4–6 AUC. Stosowanie wskazanych środków polegających na filtrowaniu, wykrywaniu i usuwaniu nielegalnych treści potwierdza bowiem jedynie, że dostawcy wykonują nałożony na nich obowiązek starannego działania.

Na gruncie AUC przyjęto założenie o niekolizyjności przesłanki starannego działania (rozdział III AUC w zw. z art. 7 AUC) z przesłankami zawartymi w art. 4–6 AUC odnoszącymi się do neutralności działania dostawcy usług pośrednich. Przyjęto zatem, że dostawca usług, chcąc uniknąć odpowiedzialności prawnej za rozpowszechnienie nielegalnych treści, może jednocześnie powoływać się na zwarte w art. 4–6 AUC okoliczności świadczące o zachowaniu przez dostawcę usług neutralnej postawy wobec rozpowszechnianych treści, a zarazem jest w stanie wykazać, że wywiązał się z obowiązku starannego działania. W założeniu tym tkwi sprzeczność. Skoro bowiem wywiązanie się z obowiązku należytej staranności polegać winno na działaniu, w szczególności na podjęciu aktywności wykrywczej, kontrolnej, a nawet nadzorczej i egzekucyjnej, to nie jest możliwe wykazanie przez tego samego dostawcę usługi, że jego zachowanie miało charakter bierny, a podjęte czynności miały wyłącznie techniczny wymiar. W istocie zatem, odmiennie niż miało to miejsce na gruncie dyrektywy o handlu elektronicznym, ustawodawca europejski wymaga od pośrednika internetowego aktywnego działania, którego zaniechanie *de facto* pozbawiać będzie dostawcę usługi możliwości skutecznego uchylenia się od odpowiedzialności.

Jak zauważył Rzecznik generalny UE w sprawie C-401/19¹⁷⁶, w konsekwencji w celu wykazania, że pośrednicy dołożyli „wszelkich starań – zgodnie z wysokimi standardami staranności zawodowej w sektorze”, aby „zapewnić brak dostępu” i aby „zapobiec ich przyszłemu zamieszczaniu” w swoich

¹⁷⁵ Tamże, pkt 80.

¹⁷⁶ Wyrok TS w sprawie RP przeciwko PE i Radzie.

usługach, dostawcy usług muszą w dużej liczbie przypadków wprowadzić narzędzia automatycznego rozpoznawania treści, aby filtrować treści, jakie użytkownicy zamieszczają online, a w razie potrzeby blokować niektóre z nich przed ich zamieszczeniem¹⁷⁷. Rzecznik generalny odnosił się, co należy odnotować, do art. 17 DSM, jednakże zawarte w jego opinii uwagi mogą mieć zastosowanie *per analogiam* także do uchylania się od odpowiedzialności przez pośredników internetowych na zasadach określonych w art. 5–7 AUC. Rzecznik wskazał, że filtrowanie, monitorowanie, a w konsekwencji blokowanie treści użytkowników przez dostawców usług, choćby wynikało z przyjętych przez dostawców usług regulaminów korzystania z usług, a zatem również pomimo tego, że dostawcy usług są podmiotami prywatnymi, to jednak stosowanej przez nich ingerencji w wolność wypowiedzi nie można uznawać za wynikającą z woli stron wyrażonej w stosunkach prywatnoprawnych, ale należy upatrywać jej źródła w woli prawodawcy unijnego. „Ingerencję” w wolność wypowiedzi użytkowników można przypisać prawodawcy Unii. Jest on bowiem jej inicjatorem¹⁷⁸. Rzecznik wskazał bowiem, że przesadzające jest ustalenie, że stosowanie przez podmioty prywatne określonych środków ma na celu przestrzeganie unijnego prawa. Bez znaczenia jest zatem, że dostawcy usług udostępniania treści mogą w ramach wolności prowadzenia działalności gospodarczej i swobody umów, które są im zagwarantowane w art. 16 karty, określić w warunkach korzystania z ich usługi lub też w „normach wspólnoty” politykę w zakresie treści i z własnej inicjatywy realizować formę „samoregulacji” poprzez filtrowanie i blokowanie treści, które ich zdaniem naruszają te normy. W tej sytuacji – jak zauważył Rzecznik – nie ma „ingerencji władz publicznych” w rozumieniu art. 10 EKPC i art. 11 Karty w wolność wypowiedzi użytkowników. Jednakże zdaniem rzecznika przesadzające jest, że filtrowanie i blokowanie treści jest realizowane w celu przestrzegania przepisów prawa unijnego¹⁷⁹. O ile zatem na gruncie DSM konieczne jest przestrzeganie art. 17 tego aktu prawnego, który nakłada na dostawców usług obowiązek przeciwdziałania rozpowszechnieniu treści potencjalnie

¹⁷⁷ Opinia Rzecznika Generalnego w sprawie RP przeciwko PE i Radzie, pkt 69.

¹⁷⁸ Tamże, pkt 84.

¹⁷⁹ Tamże, pkt 83.

stanowiących naruszenie praw własności intelektualnej¹⁸⁰, to analogicznie do art. 17 DSM i na gruncie AUC i ARC prawodawca UE uzależnił, co nastąpiło tu w bardziej zdecydowany i konkretny sposób, dopuszczalność uchylenia się od odpowiedzialności przez dostawców usług od wykazania przez dostawcę, że dochował należytej staranności, w szczególności, że podjął on środki służące wykrywaniu i usuwaniu nielegalnych lub szkodliwych treści¹⁸¹.

W takiej zatem sytuacji, gdy ustawodawca europejski kreuje kontratyp, którego istotą jest ingerowanie w wolność wypowiedzi, oznacza to, że zezwala na stosowanie tego ograniczenia i je legalizuje. Co więcej, legalizacja ingerencji w wolność wypowiedzi dotyczy uprzedniej ingerencji (*ex ante*), tj. mającej na celu zapobieżenie rozpowszechnieniu treści, niedopuszczenie do rozpowszechnienia treści w publicznym obiegu, a zatem przechwycenie treści, zanim zostanie ona dostępna dla użytkowników internetu. Ograniczenie *ex ante* oznacza także, że działanie pośredników polegające na zablokowaniu dostępu do treści przed jej publicznym udostępnieniem nie jest poprzedzone oceną sądu, wyrażoną choćby w postępowaniu zabezpieczającym. Ograniczenie *ex ante* następuje zatem poza kontrolą sądu. Rozumieć przez to należy – po pierwsze – że dostawca usług jest prawnie legitymowany do wstrzymania, blokowania lub usuwania treści, zanim w przedmiocie tego działania wypowie się sąd w prawomocnym rozstrzygnięciu, a nadto – po drugie – działanie dostawcy jest legalne nawet wówczas, gdy jego skutkiem jest wyeliminowanie z publicznego obiegu treści przed ich rozpowszechnieniem także wówczas, gdy niestosowność, karygodność czy też nielegalność treści

¹⁸⁰ Jak szczegółowo omówiono tę kwestię we wcześniejszych partiach pracy, wskazać należy w tym miejscu, że chodzi o treść art. 17 ust. 4 lit. b DSM, w którym postanowiono, że dostawcy usług udostępniania treści online mogą uchylić się od odpowiedzialności za naruszenie praw autorskich, jeśli wykażą, że: „dołożyli wszelkich starań – zgodnie z wysokimi standardami staranności zawodowej w sektorze – aby zapewnić brak dostępu do poszczególnych utworów i innych przedmiotów objętych ochroną, w odniesieniu do których podmioty uprawnione przekazały dostawcom usług odpowiednie i niezbędne informacje; oraz w każdym przypadku”. Z przepisu tego wywodzi się bowiem wniosek o ciążącym na dostawcach usług udostępniania treści online obowiązku filtrowania treści przed ich udostępnieniem oraz blokowania treści naruszających prawa twórców.

¹⁸¹ Przesądza o tym nie tylko treść przepisów zawartych w rozdziale III AUC, lecz także klauzula dobrego samarytanina, która *de facto* stanowi domniemanie zgodności z prawem każdej ingerencji w wolność wypowiedzi użytkowników internetu wówczas, gdy – jak wskazano w art. 16 ust. 3 – bez szczegółowej analizy prawnej możliwe jest stwierdzenie przez dostawcę usług nielegalnego charakteru danej działalności lub informacji.

nie stanowiła przedmiotu oceny sądu¹⁸². Obowiązek starannego działania, rozumianego jako przechwytywanie potencjalnie nielegalnych treści i ich usuwanie z obiegu publicznego, ma – jak wskazano w motywie 40 AUC – charakter zharmonizowany, co oznacza, że powinien być jednolicie rozumiany i wykonywany przez wszystkich dostawców usług pośrednich.

Rzecznik generalny celnie spostrzegł, że „Prawodawca unijny, zamiast bezpośrednio przewidzieć obowiązek wprowadzenia narzędzi legalizujących kontrolę ex-ante, narzucił je pośrednio, za pomocą przesłanek wyłączenia odpowiedzialności przewidzianych w przepisach prawa”¹⁸³. Słusznie Rzecznik generalny UE zauważył, że:

w tym przypadku w ramach tej wolności powstaje pytanie, w jakim zakresie, zważywszy na znaczenie, jakiego nabrały usługi pośrednictwa internetowego będące obecnie kluczową infrastrukturą dla wykonywania wolności komunikacji online – ich dostawcy muszą przestrzegać praw podstawowych użytkowników i w jakim zakresie władze publiczne są zobowiązane, z tytułu „pozytywnych obowiązków” wynikających z tych artykułów, do przyjęcia „pozytywnych środków ochronnych” gwarantujących rzeczywiste korzystanie z tej wolności w stosunkach między użytkownikami a dostawcami usług udostępniania treści¹⁸⁴.

Pozornie obowiązek ten spoczywa na Komisji Europejskiej. Zgodnie z art. 70 AUC Komisja Europejska „przyjmuje decyzję stwierdzającą nieprzestrzeganie przepisów, jeżeli uzna, że dany dostawca bardzo dużej platformy internetowej lub bardzo dużej wyszukiwarki internetowej: a) nie przestrzega odpowiednich przepisów niniejszego rozporządzenia; b) nie zastosowywał się do środków tymczasowych przyjętych zgodnie z art. 70; lub c) nie wykonał zobowiązań, które uczyniono wiążącymi zgodnie z art. 71. Komisja może podejmować środki tymczasowe w formie decyzji nawet na podstawie stwierdzenia na pierwszy rzut oka naruszenia przepisów AUC¹⁸⁵.

¹⁸² Dostawcy usług są uprawnieni do stosowania środków zapobiegawczych w celu minimalizowania tzw. ryzyka systemowego (motyw 86).

¹⁸³ Opinia Rzecznika Generalnego w sprawie RP przeciwko PE i Radzie, pkt. 62.

¹⁸⁴ Tamże, przypis nr 90.

¹⁸⁵ U. Góral, *Artykuł 70*, [w:] *Akt...*

W doktrynie optymistycznie założono, że „regulacja dotycząca środków tymczasowych ma na celu umożliwienie szybkiej reakcji Komisji w sytuacjach awaryjnych, aby chronić użytkowników i utrzymać porządek w przestrzeni internetowej”¹⁸⁶. Jest to założenie o tyle zasadne, o ile istniałby konsensus w zakresie ustalenia źródeł i przedmiotu potencjalnych zagrożeń dla bezpieczeństwa użytkowników internetu oraz interpretacji celu, dla którego ustawodawca europejski zdecydował się na uchwalenie AUC, tj. stworzenie „bezpiecznego, przewidywalnego i godnego zaufania środowiska internetowego (art. 1 AUC)”¹⁸⁷. Ani jednak z treści AUC, ani innych wiążących aktów prawnych nie wynika jednolita definicja tych pojęć lub jednolita ich interpretacja. Przeciwnie, ustawodawstwo krajowe zarówno w obszarze państw UE, jak i – porównawczo – państw spoza tego obszaru, charakteryzuje się bardzo zróżnicowanym poziomem spójności normatywnej w odniesieniu do typologii rodzajów nielegalnych treści. O ile istnieje znaczny konsensus co do globalnej niedopuszczalności niektórych treści (takich jak materiały przedstawiające niegodziwe traktowanie dzieci w celach seksualnych)¹⁸⁸, o tyle jednak istnieją duże różnice co do stosowanych kryteriów służących ograniczaniu wielu innych rodzajów treści, w tym podżegania do przemocy, mowy nienawiści, nękania, zniesławienia lub dezinformacji. Prawodawstwo państw odzwierciedla – co jest zrozumiałe i uzasadnione – specyficzną kulturową, historyczną, polityczną i religijną wrażliwość społeczności lokalnych w odniesieniu do tego, jakie treści są dopuszczalne, a jakie nie. W badaniach prowadzonych na potrzeby organizacji międzynarodowych, w tym ONZ, Rady Europy i Unii Europejskiej, sformułowano pogląd, zgodnie z którym „państwa w odniesieniu, przede wszystkim, do sankcjonowania nieodpowiednich treści w internecie, nie zawsze w pełni respektują międzynarodowe standardy praw człowieka i gwarancje rzetelnego procesu”¹⁸⁹.

Na płaszczyźnie rozporządzeń cyfrowych przyjęto, że państwa członkowskie UE jednolicie posługują się terminem „nielegalne treści”, co nie

¹⁸⁶ Tamże.

¹⁸⁷ Ustawodawca europejski posługuje się tą zbitką słowną wielokrotnie (motyw 3, 9, 12, 40, 72, 109, 155, a także art. 1 ust. 1 AUC), jednakże nie wyjaśnia treści jej składników.

¹⁸⁸ *Content & Jurisdiction Program. Operational Approaches Norms, Criteria and Mechanisms*, s. 7, <https://www.internetjurisdiction.net/uploads/pdfs/Papers/Content-Jurisdiction-Program-Operational-Approaches.pdf> (dostęp: 20.06.2024).

¹⁸⁹ Tamże, s. 8.

znajduje jednak odzwierciedlenia w praktyce normatywnej i jurysdykcyjnej¹⁹⁰. Przy założeniu, że hipoteza o wspólnym, jednolitym definiowaniu nielegalnych treści jest prawdziwa, udzielono upoważnienia podmiotom prywatnym (dostawcy usług pośrednich) oraz organowi publicznemu, tj. Komisji Europejskiej, do uprzedniego i dyskrejonowego ingerowania w wolność wypowiedzi użytkowników internetu. Komisja Europejska została legitymowana do wkraczania *ex ante* w prawa i wolności zagwarantowane w Karcie praw podstawowych i w EKPC, w tym wolność wypowiedzi użytkowników internetu (usługobiorców). Uprawnienia KE wynikają w szczególności z art. 70 w zw. z art. 73 AUC. Komisja ma prawo podjąć „środki tymczasowe” w drodze decyzji. To oznacza, że ma możliwość wprowadzenia szybkich i natychmiastowych środków w przypadku naruszenia przepisów. Ingerencja KE może nastąpić po „stwierdzeniu naruszenia *prima facie*, co sugeruje, że Komisja może działać na podstawie oczywistego, widocznego naruszenia, niekoniecznie musząc czekać na pełne dochodzenie lub udowodnienie naruszenia w pełnym zakresie”¹⁹¹.

Odrębną płaszczyznę regulacji obejmującą mechanizmy legalnego i skutecznego ingerowania *ex ante* w wolność wypowiedzi użytkowników internetu

¹⁹⁰ Nie ma porozumienia co do norm, zachowań i rodzajów treści, które są powszechnie akceptowane i nieakceptowane. Różnice międzynarodowe są ogromne. Treść może być w orzecznictwie jednego państwa zaklasyfikowana jako mowa nienawiści, podczas gdy w innych przypadkach może być ona dopuszczalna. Eksperti, z którymi przeprowadzono wywiady przy przygotowaniu raportu o stanie internetu (zob. D. Jerker, B. Svantesson, *Global status...*, s. 63), podkreślili tę kwestię, porównując sposób, w jaki USA i Niemcy traktują mowę nienawiści. W raporcie z 2012 r. dla ONZ na temat wolności słowa wskazano na trzy różne rodzaje wypowiedzi: 1) wypowiedzi, które stanowią przestępstwo w świetle prawa międzynarodowego i mogą być ścigane karnie; 2) wyrażenie, które nie podlega karze, ale może uzasadniać ograniczenie i pozew cywilny; oraz 3) wypowiedzi, które nie powodują sankcji karnych lub cywilnych, ale nadal budzą obawy w zakresie tolerancji, uprzejmości i szacunku dla innych. Jest to nadal przydatna kategoryzacja, a jak zauważono w *Specjalnym Raporcie ONZ*, te kategorie wypowiedzi stwarzają różne problemy wymagające różnych reakcji prawnych i politycznych; zob. *Roczne sprawozdanie Specjalnego Sprawozdawcy Organizacji Narodów Zjednoczonych ds. Promocji i Ochrony Prawa do Wolności Opinii i Wypowiedzi dla Zgromadzenia Ogólnego*, 7.09.2012, pkt 2, <https://undocs.org/en/A/67/357> (dostęp: 15.10.2023). Wysiłki koordynacyjne dodatkowo komplikują zasadnicze różnice w podejściu państw do roli, jaką demokracja i religia powinny odgrywać w kwestiach prawnych. Złożoność tej sytuacji będzie się tylko pogłębiać, ponieważ coraz więcej krajów rozwijających się będzie odgrywać większą rolę w Internecie (zob. D. Jerker, B. Svantesson, *Global status...*, s. 63).

¹⁹¹ U. Góral, *Artykuł 70, [w:] Akt...*

stanowią przepisy o ochronie sygnalistów nazywanych na gruncie AUC „zaufanymi podmiotami sygnalizującymi”. Celem działania zaufanych podmiotów sygnalizujących jest wykrywanie, identyfikowanie i zgłaszanie nielegalnych treści (art. 22 ust. 2 lit. a AUC). Dostawcy platform internetowych zostali zobowiązani do „wprowadzenia środków technicznych i organizacyjnych w celu zapewnienia priorytetowego traktowania zgłoszeń dokonywanych przez zaufane podmioty sygnalizujące, działające w wyznaczonych dziedzinach, w których dysponują wiedzą ekspercką” (art. 22 ust. 1 AUC). Zaufanym podmiotem sygnalizującym jest dowolny podmiot, któremu taki status został przyznany przez krajowego koordynatora ds. usług cyfrowych (art. 22 ust. 2 AUC). Podmioty ubiegające się o uzyskanie takiego statusu powinny wykazać się „między innymi, że posiadają szczególną wiedzę ekspercką i kompetencje w zakresie zwalczania nielegalnych treści oraz że działają w sposób dokładny, obiektywny i z zachowaniem należytej staranności” (art. 22 ust. 2 AUC).

Jak zastrzeżono w motywie 62 AUC, dostawcy platform internetowych mogą korzystać z podobnych do wskazanych w art. 22 AUC mechanizmów uzyskiwania informacji w celu podejmowania szybkich i rzetelnych działań przeciwko treściom, które są niezgodne z warunkami korzystania z usług tych dostawców, w szczególności przeciwko treściom, które są szkodliwe dla odbiorców usługi podatnych na zagrożenia. W konsekwencji także w odniesieniu do usług pośrednictwa internetowego znajdować będą zastosowanie postanowienia dyrektywy w sprawie ochrony osób zgłaszających naruszenia prawa Unii¹⁹² oraz ustawy o ochronie sygnalistów¹⁹³ implementującej postanowienia tej dyrektywy. Sygnalistą, w rozumieniu ustawy z dnia 14 czerwca 2024 r. o ochronie sygnalistów:

jest osoba fizyczna, która zgłasza lub ujawnia publicznie informację o naruszeniu prawa uzyskaną w kontekście związanym z pracą, w tym:

- 1) pracownik;
- 2) pracownik tymczasowy;

¹⁹² Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii (Dz.U. UE L Nr 305, s. 17 z późn. zm.).

¹⁹³ Ustawa z dnia 14 czerwca 2024 r. o ochronie sygnalistów (Dz.U., poz. 928) – dalej: uos.

- 3) osoba świadcząca pracę na innej podstawie niż stosunek pracy, w tym na podstawie umowy cywilnoprawnej;
- 4) przedsiębiorca;
- 5) prokurent;
- 6) akcjonariusz lub wspólnik;
- 7) członek organu osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej;
- 8) osoba świadcząca pracę pod nadzorem i kierownictwem wykonawcy, podwykonawcy lub dostawcy;
- 9) stażysta;
- 10) wolontariusz;
- 11) praktykant;
- 12) funkcjonariusze: ABW, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, Centralnego Biura Antykorupcyjnego, Straży Granicznej, Straży Marszałkowskiej, Służby Ochrony Państwa, Państwowej Straży Pożarnej, Służby Celno-Skarbowej i Służby Więziennej, a także
- 13) żołnierze, a także osoba fizyczna w przypadku zgłoszenia lub ujawnienia publicznego informacji o naruszeniu prawa uzyskanej w kontekście związanym z pracą przed nawiązaniem stosunku pracy lub innego stosunku prawnego stanowiącego podstawę świadczenia pracy lub usług lub pełnienia funkcji w podmiocie prawnym lub na rzecz tego podmiotu, lub pełnienia służby w podmiocie prawnym lub już po ich ustaniu (art. 4 uos).

Sygnalista może dokonywać zgłoszeń anonimowo, a podmioty prawne oraz RPO i podmioty publiczne mają obowiązek takie zgłoszenie przyjąć i procedować (art. 7 uos). Dane sygnalisty nie mogą być ujawnione nieupoważnionym osobom (art. 8 ust. 1 uos). Sygnalista podlega ochronie od chwili dokonania zgłoszenia lub ujawnienia publicznego, pod warunkiem, że miał uzasadnione podstawy sądzić, że informacja będąca przedmiotem zgłoszenia lub ujawnienia publicznego jest prawdziwa w momencie dokonywania zgłoszenia lub ujawnienia publicznego i że stanowi informację o naruszeniu prawa (art. 6 uos).

Wszystkie powyżej wskazane instytucje prawne przesądzają o legalności ingerencji w wolność wypowiedzi także wówczas, gdy ma ona charakter uprzedni. W efekcie następuje odejście od klasycznego standardu wolności wypowiedzi, realizowanego poza sferą cyfrową, którego istotę stanowiła niedopuszczalność prewencyjnego ograniczenia wolności wypowiedzi. W klasycznym standardzie przyjmowano bowiem, że o ile możliwe, a niekiedy konieczne jest ograniczenie wolności wypowiedzi, to jednak nie jest dopuszczalne blokowanie dostępu do treści i dokonywanie jej oceny, zanim wypowiedź zostanie rozpowszechniona, jak również tylko w skrajnych i rzadkich okolicznościach uznawano za legalne całkowite usunięcie wypowiedzi z obiegu publicznego. Wielokrotnie ETPC podkreślał, że „funkcja nadzorcza wymusza na Trybunale zwrócenie szczególnej uwagi na zasady charakterystyczne dla »społeczeństwa demokratycznego«”¹⁹⁴. ETPC wskazywał zatem, że „Wolność wyrażania opinii stanowi jeden z podstawowych fundamentów takiego społeczeństwa, jeden z najważniejszych warunków rozwoju społeczeństwa jako całości, jak i rozwoju każdej jednostki. Z zastrzeżeniem ust. 2 art. 10 Konwencji, wolność ta odnosi się nie tylko do »informacji« czy »poglądów«, które spotykają się z przychylną reakcją lub są uznawane za nieobraźliwe, lub indyferentne, ale również do tych, które obrażają, szokują, czy wzbudzają niepokój Państwa, czy jakiegokolwiek grupy społecznej. Takie są wymogi pluralizmu, tolerancji oraz otwartości światopoglądowej, bez których nie można mówić o »społeczeństwie demokratycznym«. To oznacza między innymi, że jakikolwiek wymóg formalny, warunek, ograniczenie i sankcja dotyczący tej sfery powinien być proporcjonalny do realizowanego prawnie uzasadnionego celu”¹⁹⁵.

W realiach jednolitego rynku cyfrowego prawodawca europejski uznał, że klasyczny standard wolności wypowiedzi, w którym wartością kluczową jest swoboda debaty publicznej obejmująca wygłaszanie także takich poglądów, które „oburzają, obrażają i wprowadzają niepokój”¹⁹⁶ nie może zostać utrzymany. Uznano bowiem, że niekontrolowana debata publiczna, jeśli toczy się w internecie, przestaje być wartością dla demokracji i staje się dla niej

¹⁹⁴ Wyrok ETPC w sprawie Handyside przeciwko Wielkiej Brytanii.

¹⁹⁵ Tamże.

¹⁹⁶ Wyroki ETPC: w sprawie Jersild przeciwko Danii, § 31; w sprawie Peta Deutschland przeciwko Niemcom, § 46.

zagrożeniem. Zauważono, że w odniesieniu do swobody wypowiedzi w internecie obecnie pytanie nie brzmi, czy regulować zasady debaty publicznej, ale w jaki sposób i kto powinien to robić¹⁹⁷. Zauważono, że:

stosowanie przedinternetowych pojęć prawnych często wiąże się z poszukiwaniem odpowiednich analogii. Pojęcia prawne są przestarzałe. Stwarza to „sztuczne wyzwania regulacyjne”, ponieważ stosowane ramy i koncepcje są niewystarczające, aby rozwiązać te problemy; innymi słowy, nieadekwatność narzędzi może powodować nowe wyzwania regulacyjne¹⁹⁸.

Zmiana standardu wolności wypowiedzi oznacza *de facto* uchylenie standardu klasycznego i wypracowanie nowego modelu, adekwatnego do uwarunkowań rynku cyfrowego. Jednym z elementów konstruujących cyfrowy standard wolności wypowiedzi jest zalegalizowanie ingerencji *ex ante* oraz przeniesienie kompetencji w zakresie dokonywania ustalenia legalności wypowiedzi z organów sądowniczych na organy wykonawcze państwa, a następnie współdzielenie tych kompetencji z podmiotami prywatnymi, jakimi są dostawcy usług cyfrowych, w tym pośrednicy internetowi. Jeśli zatem poszukiwać odpowiedzi na pytanie o zakres i sposób wykorzystania na jednolitym rynku cyfrowym testu szkodliwości, który stanowił podstawowe narzędzie (model) ustalania dopuszczalności ingerencji w wolność wypowiedzi w sferze pozainternetowej (offline), to trzeba dostrzec, że jego zastosowanie zostało ograniczone do etapu sądowego (orzeczniczego). Nadal będzie on zatem znajdował zastosowanie, jednakże tylko na etapie kontroli sądowej (sporu sądowego) wykonywanej w trybie następczym w związku z zainicjowaniem postępowania przez podmiot, którego ograniczenie dotyczyło. Szukając uzasadnienia dla przyjętej na gruncie AUC regulacji, trzeba założyć, że prawodawca unijny działał w przekonaniu, że utrzymanie klasycznego standardu było nie do pogodzenia z realizacją wskazanego w art. 1 ust. 1 AUC celu, jakim jest stworzenie „bezpiecznego, przewidywalnego i budzącego zaufanie środowiska internetowego”.

¹⁹⁷ D. Jerker, B. Svantesson, *Global status...*

¹⁹⁸ Tamże, s. 33.

Podsumowując, należy stwierdzić, że zaproponowany w AUC mechanizm reagowania na nielegalne treści, którego istotą i celem jest uzyskanie skutku polegającego – po pierwsze – na niedopuszczeniu do rozpowszechnienia niechcianych treści na forum publicznym; po drugie – usunięciu takich treści z powszechnego obiegu informacji; po trzecie – ograniczeniu dostępu do takich treści; po czwarte – na identyfikowaniu autora i dystrybutora treści; po piąte – zapobieżeniu podjęciu w przyszłości prób ich rozpowszechnienia – stanowi, co wydaje się bezsporne, ingerencję w wolność wypowiedzi. Szczególny wymiar regulacji zawartych w AUC ujawnia się w tym, że prawodawca unijny nie tylko zalegalizował działania skutkujące naruszeniem swobody wypowiedzi użytkowników internetu, ale ponadto wymaga i oczekuje ich stosowania. Prawodawca unijny zalegalizował także ingerencje w sferę aktywności komunikacyjnej obywateli dokonywane przez podmioty publiczne i prywatne, których motywem jest hipotetyczne i wyobrażone, a zatem jedynie prawdopodobne rozpowszechnienie treści, która potencjalnie jest nielegalna. Ingerencja *ex ante* oznacza bowiem, co do zasady, blokowanie treści jeszcze nierozpowszechnionych. Stanowi to odejście od klasycznej koncepcji ochrony wolności wypowiedzi realizującej wzorzec normatywny powstały na gruncie art. 10 EKPC, w którym bez wolności wypowiedzi nie istnieje system demokratyczny.

Zawarta w AUC regulacja dopuszczająca ingerencję *ex ante* w wolność wypowiedzi stanowi instrument bez precedensu w aktach normujących prawa i wolności człowieka. Wyjątkowość tej regulacji tkwi nie tylko w tym, że prawodawca europejski zdecydował się na zalegalizowanie aktów naruszania swobody wypowiedzi w stosunkach prywatnoprawnych, uszczuplając zakres korzystania z tej wolności, ale w uruchomieniu nowej formuły działania państwa, które – jak wynika z zakresu uprawnień przypisanych Komisji Europejskiej – może reglamentować korzystanie z wolności wypowiedzi, zmieniając swój status z gwaranta praw i wolności na jej dysponenta.

Zakończenie

Badania przeprowadzone na potrzeby niniejszej pracy potwierdziły, że wolność wypowiedzi nadal ma wysoką rangę w hierarchii uniwersalnych wartości, których gwarancje ochronne zostały zawarte w aktach prawnych zarówno w krajowym porządku prawnym, jak i w prawie międzynarodowym. Wolność wypowiedzi nie została co prawda z tych systemów wyrugowana, co pozwala nadal nazywać ją „wartością prawnie chronioną”, niemniej jej znaczenie, co uwidacznia się z zakresu i sposobach udzielonej ochrony, maleje, a jej ranga spada. Przeprowadzone badania, których wyniki zostały zaprezentowane na kartach niniejszej pracy, wskazują na ryzyko dewaluacji tej wartości. Źródeł tego stanu rzeczy upatrywać należy nie tyle w zmianie społecznej, zdarzeniu prawnym lub momencie historycznym, co przede wszystkim w konkretnie wyrażonej woli – racjonalnie działającego – europejskiego prawodawcy. Prawodawca europejski na podstawie wzorców zawartych w niemieckiej nauce prawa, co zostało zasygnalizowane w pracy, zmierza w kierunku normowania wolności wypowiedzi na kształt publicznych praw podmiotowych. W konsekwencji wolność wypowiedzi rozumiana jako prawo podmiotowe powiązane z określonym roszczeniem, którego rodzaj i zakres normuje państwo w prawie pozytywnym, staje się elementem polityki państwa. Jeśli koncepcja umieszczenia wolności wypowiedzi w katalogu publicznych praw podmiotowych oddziałuje na sposób postrzegania wolności i praw wewnątrz organizacji międzynarodowej, której państwo jest członkiem, wolność wypowiedzi staje się instrumentem polityki tej organizacji.

Poczynione spostrzeżenia stanowią rezultat ustaleń dokonanych na gruncie prawa europejskiego w związku z uchwaleniem przez Parlament Europejski rozporządzeń cyfrowych, których zasadniczym przedmiotem regulacji była aktywność pośredników internetowych i przeciwdziałanie rozpowszechnieniu nielegalnych treści. W pracy przyjęto założenie o istnieniu nowego podejścia prawodawcy europejskiego do problematyki regulowania wolności wypowiedzi w internecie, w szczególności podyktowanego potrzebą zwalczania nielegalnych treści. Założenie to się potwierdziło. Podobnie jak prawdziwe okazały się także założenia dotyczące wpływu regulacji cyfrowych na kształt wolności wypowiedzi i – w konsekwencji – zmianę jego standardu.

Jeśli zatem trudno wyobrazić sobie, że – wobec intensywniej aktywności komunikacyjnej użytkowników internetu – nie istnieje żaden standard wolności wypowiedzi, co musiałoby oznaczać dowolność, a zarazem prawną dopuszczalność rożgłoszenia każdego twierdzenia i każdej opinii bez względu na ich stopień szkodliwości i bez względu na to, czy mają podstawy faktyczne, to jednak trudny do zaakceptowania byłby taki standard, który przewiduje kontrolowanie wypowiedzi przed ich rozpowszechnieniem, a także arbitralne rozstrzygnięcie przez organ państwowy o ich legalności lub nielegalności, a w konsekwencji standard, który zakłada usuwanie i blokowanie treści. Niemniej właśnie taki kształt wolności wypowiedzi rysuje się na gruncie unormowań zawartych w rozporządzeniach cyfrowych. Prowadzona w ramach niniejszej dysertacji analiza miała, co do zasady, charakter czysto teoretyczny (dogmatyczno-prawny), co daje nadzieję, że zawarte wnioski, pomimo że – zdaniem Autorki – wypływają z rzetelnie i skrupulatnie przeprowadzonych ustaleń przy zastosowaniu prawidłowej metody wnioskowania, ostatecznie nie zostaną potwierdzone w praktyce działalności podmiotów i organów, które uzyskały silne prerogatywy w dziedzinie kształtowania pożądanych wzorców zachowań komunikacyjnych, a zatem także w budowaniu standardu wolności wypowiedzi.

O ile zatem nie można zaprzeczyć stanowisku, że standard wolności wypowiedzi nadal istnieje, to jednak trzeba podkreślić, że jest to standard zmieniony (zniekształcony). Jego konkretyzację stanowić będą decyzje podejmowane przez podmioty prywatne (pośredników internetowych) pod kontrolą organu publicznego (Komisja Europejska) dotyczące konkretnych aktów komunikacyjnych realizowanych przez użytkowników internetu. Tworzenie

standardu wolności wypowiedzi powierzono zatem podmiotom prywatnym. Okoliczność ta nie wyłącza, co oczywiste, kontroli sądowej, jednakże istota i powaga zmiany modelu ochrony wolności zasadza się w zaakceptowaniu prewencyjnej kontroli wypowiedzi i zalegalizowaniu aktów i czynności polegających na blokowaniu treści przed jej publicznym udostępnieniem. Nowy standard wolności wypowiedzi zwraca zatem szczególną uwagę, odmiennie niż w klasycznym standardzie, na ochronę adresatów (odbiorców) wypowiedzi, blokując im dostęp do potencjalnie szkodliwych dla nich treści. Wolność wypowiedzi w epoce przedinternetowej hołdowała przekonaniu potwierdzonemu licznymi judykataми ETPC, co ujmowano jako jej absolutyzowanie, że zasadą jest wolność wypowiedzi, a jej ograniczenie jest wyjątkiem od tej zasady.

W ramach przeprowadzonych badań potwierdziły się także dwie pozostałe hipotezy. Poczynione ustalenia doprowadziły do wniosku, zgodnie z którym kształt wolności wypowiedzi (standard) zależy od sposobu definiowania terminu „nielegalne treści”, a następnie klasyfikowania wypowiedzi, w szczególności przy zastosowaniu klauzuli przepadku (art. 17 EKPC) do tych kategorii wypowiedzi, które zostały uznane za nielegalne. Za prawdziwe Autorka przyjmuje także założenie o nieadekwatności oraz niewystarczalności wzorców oceny, tak normatywnych, jak i orzecznich, które znajdowały zastosowanie do wypowiedzi rozpowszechnionych poza internetem wobec potrzeby zastosowania tych wzorców w realiach jednolitego rynku cyfrowego. Jeśli wzorce te nadal znajdują zastosowanie, czego dowodzi orzecznictwo sądów europejskich i krajowych, to jednak następuje to dopiero na etapie postępowania sądowego, co wobec podejmowanych często przez pośredników internetowych *ad hoc* czynności o charakterze prewencyjnym, może być spóźnione, a w konsekwencji nieskuteczne.

Bibliografia

- Andrzejczak H., *Filozoficzne podstawy Powszechnej Deklaracji Praw Człowieka*, „Roczniki Filozoficzne” 1966, nr 14.
- Bach-Golecka D., *Otwarta metoda koordynacji*, [w:] *Źródła prawa. Teoria i praktyka*, red. T. Giaro, Warszawa 2016.
- Bar G., Skibicki R., *Wyzwania prawne związane z wykorzystaniem sztucznej inteligencji w usługach cyfrowych*, „Prawo Nowych Technologii” 2021, nr 1.
- Baran M., *Europeizacja prawa administracyjnego*, t. 3, red. R. Hauser, Z. Niewiadomski, A. Wróbel, Warszawa 2014 (System Prawa Administracyjnego).
- Barcz J., *Akty delegowane i akty wykonawcze – pojęcie i kryteria rozróżnienia*, „Europejski Przegląd Sądowy” 2012, nr 3.
- Barta J. (red.), *Prawo autorskie*, t. 13, Warszawa 2003 (System Prawa Prywatnego).
- Bieńkowski D., *Mechanizmy zaawansowanych rekomendacji w systemach portali internetowych*, *Praca inżynierska*, Politechnika Warszawska 2012.
- Bodnar A., Gliszczyńska-Grabias A., Wieruszewski R., Wyrzykowski M., *Mowa nienawiści a wolność słowa. Aspekty prawne i społeczne*, Warszawa 2010.
- Bychawska-Siniarska D., *Ochrona prawa do wolności wyrażania opinii na mocy Europejskiej Konwencji Praw Człowieka*, Strasburg 2018.
- Celińska-Grzegorzczak C., *Sądowa kontrola administracji publicznej*, t. 10, red. R. Hauser, Z. Niewiadomski, A. Wróbel, Warszawa 2016 (System Prawa Administracyjnego).
- Cempura A., Kasolik A., *Metodyka sporządzania umów gospodarczych*, Warszawa 2016.
- Chałubińska-Jentkiewicz K., Taczowska-Olszewska J., *Świadczenie usług drogą elektroniczną. Komentarz*, Warszawa 2019.
- Chentosz T., Wawrzyniak M., *Artykuł 7, [w:] Ustawa o partnerstwie publiczno-prywatnym. Komentarz*, red. nauk. M. Grabiec, Warszawa 2019.
- Chomiczewski W., *Zasady wyłączeń odpowiedzialności dostawców usług pośrednich w projekcie rozporządzenia Akt o usługach cyfrowych (cz. I)*, „Prawo Nowych Technologii” 2021, nr 2.

- Chomiczewski W., *Zasady wyłączeń odpowiedzialności dostawców usług pośrednich w projekcie rozporządzenia Akt o usługach cyfrowych (cz. II)*, „Prawo Nowych Technologii” 2022, nr 1.
- Chrobot M., *Google dogadało się z Unią. Konkurencja będzie miała fory w wyszukiwarce*, „Komputer Świat” 2013.
- Ciżyńska-Pałosz A., *Wpływ Europejskiego Trybunału Praw Człowieka na porządek prawny państw-stron Europejskiej Konwencji Praw Człowieka, a koncepcja marginesu oceny. Analiza ze szczególnym uwzględnieniem wyroku Europejskiego Trybunału Praw Człowieka w sprawie Hirst przeciwko Zjednoczonemu Królestwu*, „Przegląd Prawno-Ekonomiczny” 2020, nr 1.
- Czopek J., *Hasło: Internet*, [w:] *Leksykon terminów medialnych*, red. K. Wolny-Zmorzyski, Toruń 2024.
- Ćwiąkalski Z., *Komentarz do art. 256 Kodeksu Karnego*, [w:] G. Bogdan, *Kodeks karny. Część szczególna. Komentarz do art. 117–277 k.k.*, t. 2, red. A. Zoll, Kraków 1999.
- Dąbrowska-Kardas M., *Analiza dyrektywalna przepisów części ogólnej kodeksu karnego*, Warszawa 2012.
- Dąbrowska P., *Koncepcja „nowego rządu” w prawie Unii Europejskiej a Konstytucja dla Europy*, [w:] *Konstytucja dla Europy. Przyszły fundament Unii Europejskiej*, red. S. Dudzik, Kraków 2005.
- Drózd M., *Etyka mediów. W obronie wartości*, Kraków 2019.
- Dubisz S., *Uniwersalny słownik języka polskiego*, Warszawa 2003.
- Dziekan-Łanucha A., *Od personalizacji do profilowania. Opis konsekwencji korzystania z wyszukiwarki internetowej Google*, „Studia Socialia Cracoviensia” 2016, nr 1.
- Etoa S., *La terminologie des „droits fondamentaux” dans la jurisprudence du Conseil constitutionnel*, „Cahiers de la recherche sur les droits fondamentaux” 2011, nr 9.
- Frankiewicz A., *Regulacja wolności wypowiedzi w polskim porządku prawnym*, [w:] *Prawa i wolności obywatelskie w Konstytucji RP*, red. B. Banaszak, A. Preisner, Warszawa 2002.
- Gardocki L., *Zagadnienia teorii kryminalizacji*, Warszawa 1990.
- Garlicki L., *Polskie prawo konstytucyjne. Zarys wykładu*, Warszawa 2007.
- Garlicki L., *Zakres zobowiązań państwa w świetle orzecznictwa Europejskiego Trybunału Praw Człowieka*, [w:] *Stosowanie prawa międzynarodowego i wspólnotowego w wewnętrznym porządku prawnym Francji i Polski*, red. M. Granat, Warszawa 2007.
- Gliszczyńska-Grabias A., *Międzynarodowy pakt praw obywatelskich (osobistych) i politycznych. Komentarz*, red. nauk. R. Wieruszewski, Warszawa 2012.
- Gliściński K., *Gwarancje ex ante praw użytkowników na tle wyroku Trybunału Sprawiedliwości z 26.04.2022 r., C-401/19, Rzeczpospolita Polska przeciwko Parlamentowi Europejskiemu i Radzie Unii Europejskiej*, „Europejski Przegląd Sądowy” 2023, nr 3.
- Gluzik R., *Wolność słowa a mowa nienawiści. Analiza karnoprawna*, Warszawa 2021.

- Goździaszek Ł., *Prawo do bycia zapomnianym w wyszukiwarce internetowej. Glosa do wyroku TS z dnia 13 maja 2014 r., C-131/12*, „Europejski Przegląd Sądowy” 2015, nr 2.
- Góral U., *Artykuł 70, [w:] Akt o usługach cyfrowych. Komentarz*, red. D. Lubasz, M. Namysłowska, Warszawa 2024.
- Górski M., *Test prawideł kanonu artystycznego. Glosa do wyroku sądu apelacyjnego z dnia 18 lutego 2016 r., 15/02687*, „Europejski Przegląd Sądowy” 2019, nr 3.
- Grzelak A., *Artykuł 3, [w:] Traktat o funkcjonowaniu Unii Europejskiej. Komentarz. Tom I (art. 1–89)*, red. D. Miąsik, N. Półtorak, A. Wróbel, Warszawa 2012.
- Grzelak A., *Komentarz do art. 6 TFUE, [w:] Traktat o Unii Europejskiej. Komentarz*, red. R. Grzeszczak, D. Kornobis-Romanowska, Warszawa 2023.
- Gumularz M., *Zapłata danymi osobowymi – co musisz wiedzieć o nowej dyrektywie o dostarczaniu treści cyfrowych i usług cyfrowych*, LEX/el. 2019.
- Hajdys D., *Formalnoprawne możliwości współpracy sektora publicznego i prywatnego w ramach modelu partnerstwa publiczno-prywatnego*, „Finanse Komunalne” 2009, nr 9.
- Hambura S., Muszyński M., *Karta Praw Podstawowych z komentarzem*, Bielsko-Biała 2001.
- Hańderek A., *Naruszenie praw autorskich i praw pokrewnych w związku z funkcjonowaniem wyszukiwarek internetowych*, Warszawa 2024.
- Hottelier M., McGregor E., *La liberté d'expression: regards croisés sur ses sources, son contenu et ses fonctions*, „Cahiers de la recherche sur les droits fondamentaux” 2010, nr 8.
- Izdebski H., *Fundamenty współczesnych państw*, Warszawa 2007.
- Jaskiernia A., *Media masowe w demokratycznych procesach wyborczych. Standardy europejskie i uwarunkowania ich realizacji*, Warszawa 2008.
- Jerker D., Svantesson B., *Global status report 2019*, Internet & Jurisdiction Policy Network 2019.
- Jurczyk T., *Prawa jednostki w orzecznictwie Europejskiego Trybunału Sprawiedliwości*, Warszawa 2009.
- Kamiński I.C., *„Mowa nienawiści” w orzecznictwie Europejskiego Trybunału Praw Człowieka*, Centrum Badań Polityki Europejskiej 2023.
- Kamiński I.C., *Europejski Trybunał Praw Człowieka w roku 2014: czy to jeszcze ten sam trybunał?* „Polski Rocznik Praw Człowieka i Prawa Humanitarnego” 2015, nr 6.
- Kamiński I.C., *Fałszywe wiadomości (fake news) oraz dezinformacja a Europejska Konwencja Praw Człowieka*, „Przegląd Prawa Publicznego” 2023, nr 11.
- Kamiński I.C., *Mowa nienawiści – pojęcie i jego zakres, [w:] Prawna kwalifikacja mowy nienawiści – krajowe i europejskie uwarunkowania normatywne, społeczne i obyczajowe nadużycia wolności wypowiedzi*, red. J. Taczowska-Olszewska, Warszawa 2023.
- Kamiński I.C., *Ograniczenia swobody wypowiedzi dopuszczalne w Europejskiej Konwencji Praw Człowieka. Analiza krytyczna*, Warszawa 2010.

- Kamiński I.C., *Pojęcie „mowy nienawiści” w orzecznictwie Europejskiego Trybunału Praw Człowieka*, [w:] *Kwalifikacja prawna mowy nienawiści – krajowe i europejskie uwarunkowania normatywne, społeczne i obyczajowe nadużycia wolności wypowiedzi*, red. J. Taczowska-Olszewska, Warszawa 2024.
- Kamiński I.C., *Swoboda wypowiedzi w orzeczeniach Europejskiego Trybunału Praw człowieka w Strasburgu*, Kraków 2002.
- Kapelańska-Pręgowska J., *Koncepcja tzw. marginesu oceny w orzecznictwie ETPC*, „Państwo i Prawo” 2007, nr 12.
- Kocot W.J., *Europeizacja materialnego prawa prywatnego – stan obecny i perspektywy*, „Prawo i Życie” 2020, nr 2.
- Koenig-Witkowska M., Łazowski A., Ostrihansky R., *Prawo instytucjonalne Unii Europejskiej*, Warszawa 2007.
- Kolarz S., *Reforma Europejskiego Trybunału Praw Człowieka*, „Biuletyn Polski Instytut Praw Międzynarodowych” 2021, nr 155.
- Konarski X., *Unijny Akt o Usługach Cyfrowych – cele uchwalenia, zakres stosowania oraz najważniejsze obowiązki dostawców usług pośrednich*, „Prawo Nowych Technologii” 2022, nr 3.
- Konarski X., *Wzajemna relacja RODO i Aktu w sprawie sztucznej inteligencji – 10 najważniejszych informacji*, *Traple* 2023.
- Koncewicz T.T., *Zasada jurysdykcji powierzonej Trybunału Sprawiedliwości Wspólnot Europejskich*, Warszawa 2009.
- Kotuła Z., *Protokół 15 do europejskiej konwencji praw człowieka: doktryna marginesu swobody uznania i zasada subsydiarności w kontekście reformy ETPC*, „Studenckie Prace Prawnicze, Administratywistyczne i Ekonomiczne”, Wrocław 2015.
- Koubi G., *Droits de l’homme et droits de la personne: réflexion sur l’imprudence d’une distinction*, „International Journal of Psychology” 2000, t. 6, nr 15.
- Kowalik-Bańczyk K., Dąbrowska-Kłosińska P., *Komentarz do art. 14 TFUE*, [w:] *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz. Tom II (art. 90-222)*, red. M. Szwarc-Kuczer, A. Wróbel, Warszawa 2012.
- Kratochvíl J., *The Inflation of the Margin of Appreciation by the European Court of Human Rights*, „Netherlands Quarterly of Human Rights” 2011, nr 29/3.
- Kulesza J., *Prawo do anonimowej wypowiedzi a prywatna cenzura Internetu w Polsce*, „Prawo i Życie” 2012, nr 6.
- Kunc-Urbańczyk K., *Wprowadzenie*, [w:] *Prawo sztucznej inteligencji i nowych technologii 2*, red. B. Fischer, A. Pązik, M. Świerczyński, Warszawa 2022.
- Lang W., Wróblewski J., Zawadzki S., *Teoria państwa i prawa*, Warszawa 1979.
- Leszczyński L. (red.), *Wykładnia prawa Unii Europejskiej*, t. 3, Warszawa 2019 (System Prawa Unii Europejskiej).
- Levinet M., *La clause d’interdiction de l’abus de droit de l’article 17 de la CEDH. Un instrument légitime de l’ordre public européen?*, *Confluence des droits_La revue* 2023.

- Lewoszewski M., *Wybrane obowiązki dostawców usług cyfrowych na gruncie ustawy o cyberbezpieczeństwie*, „Informacja w Administracji Publicznej” 2019, nr 1.
- Lis W., Wiśniewski P., Husak Z., *Prawo prasowe. Komentarz*, Warszawa 2012.
- Lubasz D., *Artykuł 1, [w:] Akt o usługach cyfrowych. Komentarz*, red. D. Lubasz, M. Namysłowska, Warszawa 2024.
- Łopatka A., *Prawoznawstwo*, Warszawa 2006.
- Łukaszczuk A., *Mowa nienawiści w stosunku do mniejszości rasowych, narodowych i etnicznych jako granica wolności wypowiedzi. Uwagi na tle wybranych orzeczeń Europejskiego Trybunału Praw Człowieka*, „Przegląd Prawa Konstytucyjnego” 2021, nr 5.
- Macierzyńska-Franaszczyk E., *Treści cyfrowe – ujęcie definicyjne w unijnych i krajowych regulacjach prawnych*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny” 2018, nr 6.
- Małobęcka-Szwast I., *Komentarz do art. 6 ARC, [w:] Rynek cyfrowy. Akt o usługach cyfrowych. Akt o rynkach cyfrowych. Rozporządzenie platform-to-business. Komentarz*, red. M. Grochowski, Warszawa 2024.
- Mankiw G.N., Taylor N.P., *Mikroekonomia*, Warszawa 2022.
- Marek A., *Kodeks karny. Komentarz*, Lex.
- Markiewicz R., *Prawo autorskie na jednolitym rynku cyfrowym. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790*, Warszawa 2021.
- Markiewicz R., *Prawo pokrewne wydawców prasy*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej” 2019, nr 4.
- Mik C., *Europejskie prawo wspólnotowe. Zagadnienia teorii i praktyki*, Warszawa 2000.
- Mincewicz W., *Metadane – cichy zabójca prywatności*, „Studia Politologiczne” 2019, nr 54.
- Morawski L., *Zasady wykładni prawa*, Toruń 2010.
- Morawski L., *Unia Europejska wobec procesu zarządzania internetem*, „Teki Komisji Politologii i Stosunków Międzynarodowych” 2016, t. 11, nr 3.
- Motyka K., *50 lat minęło. Powszechna Deklaracja Praw Człowieka i jej credo*, „Prawo i Życie” 1998, nr 39.
- Motyka K., *Prawa człowieka. Wprowadzenie, wybór źródeł*, Lublin 2004.
- Mozgawa M., *Komentarz do art. 256 Kodeksu Karnego*, Lex.
- Niesiołowski J., *Polityka prawa, [w:] Leksykon współczesnej teorii i filozofii prawa*, red. J. Zajadło, Warszawa 2007.
- Nowińska E., *Wolność wypowiedzi prasowej*, Warszawa 2007.
- Ochocki T., *Czy Google Analytics jest zgodne z RODO? – decyzja CNIL*, odo24.pl 2022.
- Oczkowski T., *[w:] Kodeks karny. Komentarz*, red. nauk. V. Konarska-Wrzošek, Warszawa 2023.
- Ogrodowczyk A., Borkowska M., Murawska-Najmiec E., Twardowska K., *Fake news – dezinformacja online, próby przeciwdziałania tym zjawiskom z perspektywy instytucji międzynarodowych oraz wybranych państw UE, w tym Polski*, Warszawa 2018.

- Oniszczyk J., *Prawo, jego tworzenie i systematyka. Wybrane zagadnienia*, Warszawa 1999.
- Orliński W., *Internet. Czas się bać*, Warszawa 2013.
- Orzeszyna K., *Recenzja monografii A. Wiśniewskiego, Margines oceny w orzecznictwie Europejskiego Trybunału Praw Człowieka*, „Roczniki Nauk Prawnych KUL” 2010, nr 1.
- Pariser E., *Filter bubble: what the Internet is hiding from you*, Nowy Jork 2011.
- Piech M., *Pośrednicy internetowi w prawie Unii Europejskiej. Rola i obowiązki wobec treści użytkowników*, Warszawa 2019.
- Piech M., *Wylączenie odpowiedzialności dostawców usług pośrednich na gruncie Aktu o Usługach Cyfrowych*, „Prawo Nowych Technologii” 2022, nr 3.
- Piskorz A., *Nadchodzi koniec anonimowości w sieci? To nowy pomysł Francji*, justgeek.it 2022.
- Polański M., *Europejskie prawo handlu elektronicznego. Mechanizmy regulacji usług społeczeństwa informacyjnego*, Warszawa 2014.
- Polański M., *Odpowiedzialność prawna za treści rozpowszechniane w Internecie*, Warszawa 2012.
- Radoniewicz F., *Komentarz do art. 2, [w:] Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa 2019.
- Rodak B., *Naruszenie dobrego imienia osoby poprzez sportretowanie jej w powieści a prawo do poszanowania życia prywatnego. Glosa do decyzji ETPC z dnia 11 marca 2014 r., 47318/07, LEX/el. 2014.*
- Roulhac C., *Les droits de l'homme sans la loi?*, „La Revue des droits de l'homme” 2014, nr 5.
- Sajó A., *Freedom of expression*, Warszawa 2004.
- Sarnecki P., *Uwaga 5 do art. 54, [w:] Konstytucja Rzeczypospolitej Polskiej, Komentarz*, t. 3, red. L. Garlicki, Warszawa 2003.
- Scheuring K., *System źródeł prawa pochodnego UE oraz sposoby jego tworzenia po wejściu w życie Traktatu z Lizbony*, „Studia Lubuskie” 2015, nr 11.
- Seweryn R., *Technologie informacyjne i komunikacyjne – wprowadzenie w problematykę*, [w:] *Technologie informacyjne i komunikacyjne na rynku turystycznym*, red. J. Berbeka, K. Borodako, Warszawa 2017.
- Skorupka J., *Istnienie stron procesowych*, [w:] T. Grzegorzczak, *System Prawa Karnego Procesowego. Dopuszczalność procesu*, t. 4, red. nauk. M. Jeż-Ludwichowska, A. Lach, Warszawa 2015.
- Skrzydło J., *Wolność słowa w orzecznictwie Sądu Najwyższego Stanów Zjednoczonych i Europejskiego Trybunału Praw Człowieka. Analiza porównawcza*, Toruń 2013.
- Skrzydło W., *Konstytucja Rzeczypospolitej Polskiej*, Warszawa 2007.
- Sobczak J., *Prawo prasowe. Komentarz*, Warszawa 2008.
- Sobczak J., *Hasło: cenzura*, [w:] *Leksykon terminów medialnych*, red. K. Wolny-Zmorzyński, Toruń 2024.

- Sobczak J., *Komentarz do art. 11 KPP*, [w:] *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, red. A. Wróbel, Warszawa 2020.
- Sobczak J., *Komentarz do art. 8*, [w:] *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz. Tom I (art. 1–89)*, red. D. Miąsik, N. Półtorak, A. Wróbel, Warszawa 2012.
- Sobczak J., *Prawo Prasowe. Komentarz*, Warszawa 2008.
- Sobczak J., *Swoboda wypowiedzi w orzecznictwie Trybunału Praw Człowieka w Strasburgu*, cz. II, „*Ius Novum*” 2007, nr 4.
- Sobczak J., *U podstaw liberalnej koncepcji prasy*, [w:] *Czy istnieje IV władza? Wolność prasy w teorii i praktyce*, red. T. Gardocka, J. Sobczak, Warszawa 2010.
- Sobczak K., *UE: Powstają przepisy mające zwalczać nielegalne treści w internecie*, prawo.pl 2022.
- Spielmann A., *Europejski Trybunał Praw Człowieka i Podstawowych Wolności*, [w:] *Au diapason des droits de l'homme: écrits choisis (1975–2003)*, Bruksela 2006.
- Symonides J., *Powszechna Deklaracja Praw Człowieka (po 60 latach od jej przyjęcia)*, „*Prawo i Życie*” 2008, nr 12.
- Szczerski K., *Skępowani serdecznym uściskiem – społeczna gospodarka rynkowa o wysokiej konkurencyjności. Europejskie konteksty gospodarki społecznej*, Ośrodek Myśli Politycznej.
- Szpor G., *Jawność i jej ograniczenia. Idee i pojęcia*, t. 1, Warszawa 2016.
- Szwarc-Kuczer M., *Bezpośrednia skuteczność przepisów prawa wspólnotowego – wprowadzenie i wyrok ETS z 5.02.1963 r. w sprawie 26/62 NV Algemene Transport – ex Expeditie Onderneming van Gend an Loos przeciwko holenderskiej administracji celnej*, „*Europejski Przegląd Sądowy*” 2006, nr 12.
- Szymanek J., *Konstytucyjna zasada wolności słowa w radiofonii i telewizji*, „*Państwo i Prawo*” 2007, nr 8.
- Szymielewicz K., Iwańska K., *Śledzenie i profilowanie w internecie*, Fundacja Panoptikon 2019.
- Śledzińska-Simon A., *Decyzja ramowa w sprawie zwalczania pewnych form i przejawów rasizmu i ksenofobii jako trudny kompromis wobec mowy nienawiści w Unii Europejskiej*, [w:] *Mowa nienawiści a wolność słowa. Aspekty prawne i społeczne*, red. R. Wieruszewski, Warszawa 2010.
- Ślęzak P., *Ograniczenia swobody wypowiedzi*, [w:] *Prawo mediów*, red. P. Ślęzak, Warszawa 2020.
- Taczkowska J., *Autoryzacja wypowiedzi*, Warszawa 2008.
- Taczkowska-Olszewska J., Chałubińska-Jentkiewicz K., *Ustawa o świadczeniu usług drogą elektroniczną. Komentarz*, Warszawa 2019.
- Taczkowska-Olszewska J., *Cyberprzestrzeń jako przestrzeń przetwarzania i wymiany informacji w systemach teleinformatycznych*, [w:] Taczkowska-Olszewska J., Chałubińska-Jentkiewicz K., Nowikowska M., *Retencja, migracja i przepływy danych w cyberprzestrzeni. Ochrona danych osobowych w systemie bezpieczeństwa państwa*, Warszawa 2019.

- Taczkowska-Olszewska J., *Funkcjonariusz publiczny vs. Osoba pełniąca funkcje publiczne*, [w:] Taczkowska-Olszewska J., Brzostek A., Walczuk K., *Status prawny funkcjonariusza publicznego. Ochrona-obowiązki-odpowiedzialność*, Warszawa 2020.
- Taczkowska-Olszewska J., *Komentarz do art. 17*, [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa 2019.
- Taczkowska-Olszewska J., *Racjonalizacja wolności prasy. Od modelu absolutnego do warunkowego. Europejski i krajowy kontekst wykładni prawa*, „Przegląd Sejmowy” 2018, nr 1.
- Tylec G., *Ograniczenia mowy nienawiści w świetle regulacji prawnych obejmujących jednolity rynek usług cyfrowych*, [w:] *Kwalifikacja prawna mowy nienawiści – krajowe i europejskie uwarunkowania normatywne, społeczne i obyczajowe nadużycia wolności wypowiedzi*, red. J. Taczkowska-Olszewska, Warszawa 2023.
- Urbańczyk M., *Liberalna doktryna wolności słowa a swoboda wypowiedzi historycznej*, Poznań 2009.
- Van Drooghenbroeck S., *Czy artykuł 17 Europejskiej Konwencji Praw Człowieka jest niezbędny?*, „Revue trimestrielle des droits de l’homme” 2001.
- Wacławczyk J., *Swoboda wypowiedzi politycznej w USA do roku 1918*, Toruń 2011.
- Wacławczyk J., *Idea wolności słowa Johna Milтона*, Toruń 2008.
- Wacławczyk W., *Swoboda wypowiedzi jako fundamentalna zasada społeczeństwa demokratycznego. Kilka uwag o standardach Rady Europy i orzecznictwie Europejskiego Trybunału Praw Człowieka*, „Orzecznictwo Sądów Apelacyjnych” 2005, nr 12.
- Warecka K., *Strasburg: sankcja karna za obrazę homoseksualistów nie narusza wolności słowa. Vejdeland i inni przeciwko Szwecji – wyrok ETPC z dnia 9 lutego 2012 r., skarga nr 1813/07, LEX/el. 2014.*
- Wątor W., *Prawo do bycia zapomnianym a swoboda wypowiedzi. Glosa do wyroku ETPC z dnia 28 czerwca 2018 r.*, „Europejski Przegląd Sądowy” 2019, nr 5.
- Węgrzyn Ł., *Mechanizmy kontraktowe ograniczające uzależnienie się od dostawcy usług chmurowych dostarczanych w modelu SaaS (Software as a Service)*, „Monitor Prawniczy” 2020, nr 20.
- Wiczanowska H., *Oddziaływanie doktryny marginesu uznania na rozstrzyganie konfliktu pomiędzy wolnością wypowiedzi a wolnością sumienia i wyznania w praktyce orzeczniczej Europejskiego Trybunału Praw Człowieka*, „Przegląd Europejski” 2020, nr 2.
- Wilk L., *Odpowiedzialność karna w Prawie prasowym*, [w:] *Prawo mediów*, red. P. Ślęzak, Warszawa 2020.
- Winczorek P., *Komentarz do Konstytucji Rzeczypospolitej Polskiej*, Warszawa 2000.
- Winczorek P., *Nauka o państwie*, Warszawa 2011.
- Wiśniewski A., *Margines oceny w orzecznictwie Europejskiego Trybunału Praw Człowieka*, Gdańsk 2008.

- Wiśniewski A., *Znaczenie wolności słowa w państwie demokratycznym*, „Gdańskie Studia Prawnicze” 2000, t. 7.
- Wiśniewski L., *Prawo a wolność człowieka – pojęcie i konstrukcja prawna*, [w:] *Podstawowe prawa jednostki i ich sądowa ochrona*, red. nauk. L. Wiśniewski, Warszawa 1997.
- Wiśniewski L., *Zakres ochrony prawnej wolności człowieka i warunki jej dopuszczalnych ograniczeń w praktyce*, [w:] *Wolności i prawa jednostki oraz ich gwarancje w praktyce*, red. L. Wiśniewski, Warszawa 2006.
- Wojtyczek K., *Granice ingerencji ustawodawczej w sferę praw człowieka w Konstytucji RP*, Warszawa 1999.
- Wróbel A. (red.), *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, Warszawa 2020.
- Wróbel A., Rec.: Bresselink L., Pennings F., Prechal S. (red.), *The Eclipse of the Legality Principle in the European Union*, „Europejski Przegląd Sądowy” 2011, nr 11.
- Zawadzka Z., *Tymczasowe zwielokrotnianie utworu*, [w:] *Prawo własności intelektualnej. Teoria i praktyka*, red. J. Sieńczyło-Chlabicz, Warszawa 2021.
- Zieliński M., *Wykładnia prawa. Zasady. Reguły. Wskazówki*, Warszawa 2002.
- Zoll A., *Komentarz do art. 256 Kodeksu karnego*, Lex.
- Żaczekiewicz-Zborska K., *TSUE: Wolność słowa i prawo do informacji w sieci – zapewnione w dyrektywie*, prawo.pl 2022.

