Instytut Wymiaru Sprawiedliwości

Standard wolności wypowiedzi na rynku usług cyfrowych w orzecznictwie Europejskiego Trybunału Praw Człowieka i Trybunału Sprawiedliwości Unii Europejskiej

dr hab. Joanna Taczkowska-Olszewska

Prawo prywatne
Warszawa 2023

Spis treści

1. Uwagi wprowadzające

Zarówno państwa-strony europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności[1], jak również państwa członkowskie UE, podpisując traktat z Lizbony, do którego załącznik stanowiła Karta praw podstawowych Unii Europejskiej[2], potwierdziły fundamentalne znaczenie wolności wypowiedzi jako prawa człowieka, a zarazem 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 powierzono sprawowanie kontroli nad przestrzeganiem przez państwa-strony Konwencji (państwa członkowskie UE) standardu wolności wypowiedzi ustanowionego na gruncie Konwencji i umów międzynarodowych.

---

[1] 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 ze zm.) – dalej jako EKPC lub Konwencja.

[2] Wersja skonsolidowana Dz.Urz. UE C 202 z 2016 r., s. 389 – dalej jako KPP. Karta praw podstawowych została włączona na podstawie art. 4 Traktatu o Unii Europejskiej (Traktatu o Unii Europejskiej i Traktatu o funkcjonowaniu Unii Europejskiej Dz.Urz. UE C 115/01 z 2008 r., https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:C2008/115/01&from=PL; dostęp: 20 czerwca 2024 r.) 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 (Dz.Urz. UE C 115/01 z 2008 r.) 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 niezmienność stanowiska Polski, która nigdy z jego postanowień się nie wycofała, nakazuje dokonywanie wykładni art. 51–53 KPP z uwzględnieniem, nie zaś przy pominięciu, treści Protokołu nr 30. W konsekwencji uprawnione jest także stanowisko, zgodnie z którym KPP nie znajduje zastosowania do Polski.

O ile akty prawa międzynarodowego w zakresie, w jakim potwierdzają znaczenie i definiują wolność wypowiedzi, nie uległy od czasu ich sporządzenia i przyjęcia[3] zmianie ani co do 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, kreując nowe zachowania komunikacyjne, charakterystyczne dla internetu. Okoliczności te wpływają także na przedmiot i charakter celów politycznych i gospodarczych realizowanych przez organizacje międzynarodowe, w tym UE i Radę Europy. Monetyzacja informacji i danych, w tym danych osobowych, stała się podstawą rozwoju państw i źródłem ich sukcesu gospodarczego.

Zasadniczą przyczynę zmiany podejścia do metod kształtowania oraz ustalania zakresu wolności wypowiedzi w internecie stanowiło spostrzeżenie, że ograniczona liczba usługodawców świadczących usługi pośrednictwa internetowego[4] uzyskuje rzeczywisty i niekwestionowany wpływ na kształtowanie zachowań komunikacyjnych, w tym zachowań konsumenckich. W treści wniosku Komisji Europejskiej do Parlamentu Europejskiego

[3] Chodzi o te postanowienia aktów prawa międzynarodowego, które gwarantują wolność wypowiedzi, a zatem art. 10 EKPC, art. 11 KPP, art. 19 Międzynarodowego Paktu Praw Obywatelskich i Politycznych przyjętego przez Zgromadzenie Ogólne ONZ z dnia 19 grudnia 1966 r. (Dz.U. z 1977 r. Nr 38, poz. 167) – dalej jako MPPOiP.

[4] Usługi pośrednictwa internetowego zostały zdefiniowane zarówno w akcie o usługach cyfrowych (rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych) (Dz.Urz. UE L 277, s. 1 ze zm.; dalej jako AUC), jak i w akcie o rynkach cyfrowych (rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z 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.Urz. UE L 265, s. 1; dalej jako ARC), a zakresy tych aktów normatywnych się uzupełniają. W akcie o usługach cyfrowych wymieniono w art. 3 lit. g trzy kategorie usług pośrednich, tj.: 1) zwykły przekaz; 2) caching oraz 3) hosting, wskazując, że każda z wymienionych w tym przepisie usług 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. 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 przez odesłanie do art. 2 pkt 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1150 z 20 czerwca 2019 r. w sprawie propagowania sprawiedliwości i przejrzystości dla użytkowników biznesowych korzystających z usług pośrednictwa internetowego (Dz.Urz. UE L 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 (UE) 2015/1535 Parlamentu Europejskiego i Rady z 9 września 2015 r. ustanawiającej procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz.Urz. UE L 241, s. 1); 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.

w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym (ARC)[5] Komisja zauważyła, że podmioty te stanowią kluczowe elementy strukturalne współczesnej gospodarki cyfrowej, pośrednicząc w większości transakcji między użytkownikami końcowymi a użytkownikami biznesowymi. Wiele z tych przedsiębiorstw zajmuje się również kompleksowym śledzeniem i profilowaniem użytkowników końcowych. 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 wejścia[6]. Pełniąc funkcję strażników[7] 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[8], co w niektórych przypadkach skutkuje nieuczciwym postępowaniem

[5] Wniosek KE Rozporządzenie Parlamentu Europejskiego i Rady w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym (akt o rynkach cyfrowych) z 20 grudnia 2020 r., COM(2020) 842 final 2020/0374(COD), https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52020PC0842 (dostęp: 20 czerwca 2024 r.).

[6] 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 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 konsumentów" – Wniosek ROZPORZĄDZENIE 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/ALL/?uri=CELEX:52020PC0842; dostęp: 20 czerwca 2024 r.).

[7] Zgodnie z uzasadnieniem wniosku KE COM(2020) 842 final 2020/0374(COD): „Dostawców podstawowych usług platformowych można uznać za strażników dostępu, jeżeli: (i) wywierają znaczący wpływ na rynek wewnętrzny, (ii) obsługują co najmniej jeden istotny punkt dostępu umożliwiający dotarcie do konsumentów oraz (iii) osiągnęli lub oczekuje się, że osiągną ugruntowaną i trwałą pozycję w zakresie prowadzonej działalności. Taki status 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 rynku". Wskaźniki ilościowe, które znajdują zastosowanie do ustalenia statusu dostawcy usługi pośrednictwa internetowego za strażnika dostępu zostały określone w art. 3 ARC. Zgodnie z tym przepisem domniemuje się, że przedsiębiorstwo jest strażnikiem dostępu, jeśli: a) uzyskało roczny obrót w Unii wynoszący co najmniej 7,5 mld EUR w każdym z ostatnich trzech lat obrotowych; b) 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 UE; c) jeżeli progi ustanowione w lit. b) zostały osiągnięte w każdym z ostatnich trzech lat obrotowych.

[8] Komisja Europejska – na mocy aktu o rynkach cyfrowych (ARC) – wyznaczyła 6 września 2023 r., po raz pierwszy, sześciu strażników dostępu: Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft (zob. *Akt o rynkach cyfrowych: Komisja wyznacza sześciu strażników dostępu*, https://digital-strategy.ec.europa.eu/pl/news/digital-markets-act-commission-designates-six-gatekeepers, dostęp: 20 czerwca 2024 r.).

wobec tych użytkowników biznesowych. Ponadto ma to również niekorzystny wpływ na kontestowalność podstawowych usług platformowych[9].

Celem niniejszego badania jest ustalenie, czy w ogóle, a jeśli tak, to w jaki sposób, klasyczny model wolności wypowiedzi jest realizowany na jednolitym rynku cyfrowym[10], a nadto ustalenie, w jakim zakresie zmiany dotyczące modelu i warunków korzystania z wolności wypowiedzi i jej funkcji w społeczeństwie demokratycznym rzutują na kształt tzw. europejskiego standardu wolności wypowiedzi. Na potrzeby badania przyjęto założenie, że reguły 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[11] pełniące funkcje tzw. strażników dostępu. Próba lustrzanego zastosowania wolnościowej koncepcji swobody wypowiedzi w takim ujęciu, jakie było wypracowane przez Europejski Trybunał Praw Człowieka (ETPC), nie powiodła się, a w konsekwencji konieczne stało się zmodyfikowanie standardu wolności wypowiedzi i jego adaptacja do reguł rynku cyfrowego. Konstrukcja nowego, cyfrowego, standardu wolności wypowiedzi stanowi wypadkową koncepcji zajmowanych przez organizacje międzynarodowe, w tym Radę Europy i Unię Europejską, a także poszczególne państwa, w tym Niemcy, USA i Chiny, w odniesieniu do zarządzania internetem. 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

[9] Podstawowa usługa platformowa oznacza którąkolwiek z następujących usług: 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) wirtualni asystenci; i) usługi przetwarzania w chmurze; j) 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 wymienione w lit. a)–i) (art. 2 pkt 2 ARC).

[10] Jednolity rynek cyfrowy jest definiowany w dokumentach UE jako element (część) rynku wewnętrznego. Pojęcie rynku wewnętrznego zostało wprowadzone do prawa pierwotnego przez Jednolity Akt Europejski (Dz.U. z 2004 r. Nr 90, poz. 854/5). 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 konkurencji uzyskać dostęp do usług online lub je świadczyć" (Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: *Strategia jednolitego rynku cyfrowego dla Europy*, COM (2015) 192 *final*, s. 3, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=COM:2015:192:FIN, dostęp: 22 marca 2024 r.). Strategia budowy jednolitego rynku cyfrowego (JRC) została uruchomiona przez Komisję Europejską w maju 2015 r.

[11] Platforma internetowa oznacza „usługę hostingu, która na żądanie odbiorcy usługi przechowuje i rozpowszechnia publicznie informacje, chyba że takie działanie jest nieznaczną lub wyłącznie poboczną cechą innej usługi lub nieznaczną funkcją głównej usługi, i ze względów obiektywnych i technicznych nie można z niej skorzystać bez takiej innej usługi, a włączenie takiej cechy lub funkcji w taką inną usługę nie jest sposobem na obejście stosowania niniejszego rozporządzenia" (art. 3 lit. i AUC).

zadań, wspólnych zasad, norm, reguł, procedur decyzyjnych oraz programów kształtujących rozwój i sposób korzystania z internetu"[12]. W dokumentach Unii Europejskiej definicja ta jest przytaczana z powołaniem się na „powszechne jej rozumienie"[13]. Przytaczane są także stanowiska wypracowane w czasie Światowego Szczytu Społeczeństwa Informacyjnego, które odbyło się w dwóch fazach. Pierwsza miała miejsce w Genewie w terminie 10–12 grudnia 2003 r., druga miała miejsce w Tunisie i trwała 16–18 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 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[14]. Ujęcie wąskie terminu „zarządzanie internetem" 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 HTML czy SGML. W ujęciu szerokim zarządzanie internetem „wkracza w szeroko rozumiane polityki 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"[15]. Od 2012 r. debata i badania nad internetem odbywają się z udziałem organizacji Internet & Jurisdiction Policy Network, która skupia zainteresowane strony, w tym państwa, podmioty sektora prywatnego, organizacje międzynarodowe w celu koordynowania i ustalania zasad transgranicznego moderowania treści i ograniczeń[16].

W dniu 1 czerwca 2020 r. sekretarz generalny ONZ António Guterres przedstawił, bazując na ustaleniach zawartych w raporcie sporządzonym przez tę organizację, zestaw zalecanych

---

[12] Ł. Morawski, *Unia Europejska wobec procesu zarządzania internetem*, „TEKA of Political Science and International Relations" 2016, nr 3, s. 112.

[13] 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* (Tekst mający znaczenie dla EOG), /* COM/2014/072 final/2 */, pkt 1

[14] Rezolucja Zgromadzenia Ogólnego ONZ 56/183, World Summit on the Information Society, https://www.itu.int/wsis/docs/background/resolutions/56_183_unga_2002.pdf (dostęp: 25 maja 2024 r.).

[15] Ł. Morawski, *Unia*..., s. 112.

[16] Lista członków organizacji nie została ujawniona na stronie internetowej, jednak organizacja wskazuje na ponad 300 członków instytucjonalnych. Organizacja jest wspierana przez sześć organizacji międzynarodowych: Radę Europy, Komisję Europejską, ICANN, OECD, ONZ ECLAC i UNESCO. Kraje partnerskie obejmują Francję (2016), Kanadę (2018) i Niemcy (2019). Prace organizacji zostały przedstawione na Forum Zarządzania Internetem ONZ, stanowiąc przyczynek do zarządzania zasobami sieciowymi.

działań dla społeczności międzynarodowej, aby zapewnić równowagę w erze cyfrowej. Wskazano na następujące potrzeby:

1) osiągnięcie powszechnej łączności do 2030 r.;
2) promowanie cyfrowych dóbr publicznych w celu odblokowania bardziej sprawiedliwego świata;
3) zapewnienie integracji cyfrowej;
4) wzmocnienie budowania potencjału cyfrowego;
5) zapewnienie ochrony praw człowieka w erze cyfrowej;
6) wspieranie globalnej współpracy w zakresie sztucznej inteligencji;
7) promowanie zaufania cyfrowego i bezpieczeństwa;
8) budowanie bardziej efektywnej architektury współpracy cyfrowej[17].

Obecny etap rozwoju internetu nazwano „Epoką cyfrowej współzależności"[18]. Wezwano do dokonania sprawdzenia, w jaki sposób istniejące międzynarodowe porozumienia i standardy dotyczące praw człowieka mają zastosowanie do nowych i powstających technologii cyfrowych. W celu podkreślenia wagi prowadzenia debaty nad ochroną praw człowieka w internecie użyto określenia „cyfrowe prawa człowieka"[19].

Koncepcja zarządzania internetem[20], a w konsekwencji także podejście do regulowania swobody wypowiedzi w internecie, zostały skonkretyzowane w strategii jednolitego rynku cyfrowego[21]. Zauważono, że czynnikiem determinującym rozwój jednolitego rynku cyfrowego jest „ustanowienie zharmonizowanych przepisów dotyczących bezpiecznego, przewi-

---

[17] Panel sekretarza generalnego ds. współpracy cyfrowej na wysokim szczeblu, https://www.un.org/en/sg-digital-cooperation-panel#:~:text=on%20Digital%20Cooperation-,The%20High-level%20Panel%20on%20Digital%20Cooperation%20was%20convened%20by,community%20and%20other%20relevant%20stakeholders. Podstawę dla nakreślenia w/w priorytetów stanowiły dokumenty Content&Juidiction, tj. Data & Jurisdiction Program (https://www.internetjurisdiction.net/uploads/pdfs/Papers/Data-Jurisdiction-Policy-Options-Document.pdf), Content & Jurisdiction Program (https://www.internetjurisdiction.net/uploads/pdfs/Papers/Content-Jurisdiction-Policy-Options-Document.pdf), Domains & Jurisdiction Program (https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Policy-Options-Document.pdf) (dostęp do stron: 20 czerwca 2024 r.).

[18] https://www.un.org/en/pdfs/HLP%20on%20Digital%20Cooperation%20Report%20Executive%20Summary%20-%20ENG.pdf)

[19] High-level Panel Follow-up Roundtable 3A/B - Digital Human Rights1st Session: 12 December 2019, 10am--12pm EST, https://www.un.org/en/pdfs/HLP%20Followup%20Roundtable%203AB%20Digital%20Human%20Rights%20-%201st%20Session%20Summary.pdf (dostęp: 20 czerwca 2024 r.)

[20] Stanowisko organów UE w odniesieniu do zarzadzania internetem zostało zawarte w szczególności w następujących dokumentach: rezolucji Parlamentu Europejskiego z 15 czerwca 2010 r. w sprawie zarządzania Internetem: kolejne działania (2009/2229(INI)) (Dz.Urz. UE C 236E z 2011 r., s. 33, dalej jako rezolucja 2009/2229(INI)), zob. lit. I pkt 1–3; komunikacie KE COM/2014/072, pkt 9; Wspólnym Komunikacie do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń z 7 lutego 2013 r., /* JOIN/2013/01 final */ oraz Wniosku: Dyrektywa Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii /* COM/2013/048 final - 2013/0027 (COD) */ (zob. Ł. Morawski, *Unia*..., s. 112).

[21] Zob. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: *Strategia jednolitego rynku cyfrowego dla Europy*, COM (2015) 192 *final*.

dywalnego i budzącego zaufanie środowiska internetowego"[22]. Aby osiągnąć cel zakładający zapewnienie bezpiecznego, przewidywalnego i godnego zaufania środowiska internetowego, zdefiniowano pojęcie nielegalnych treści i ustalono mechanizmy ich identyfikowania, usuwania i zwalczania, a także wskazano podmioty odpowiedzialne za przeciwdziałanie rozpowszechnieniu nielegalnych treści. Cele, mechanizmy i definicje zostały zawarte w dwóch rozporządzeniach Parlamentu Europejskiego i Rady, tj. akcie o usługach cyfrowych (AUC) oraz akcie o rynkach cyfrowych (ARC) nazywanych „konstytucją internetu"[23] lub „pakietem cyfrowym".

Uchwalenia przez Parlament Europejski pakietu cyfrowego zostało poprzedzone wezwaniem skierowanym w 2015 r. do Komisji Europejskiej, by „dokonała postępów w polityce i ramach prawnych dotyczących zwalczania cyberprzestępczości oraz nielegalnych treści i materiałów w internecie, w tym mowy nienawiści"[24]. Wezwanie do podjęcia aktywności w przedmiocie zwalczania nielegalnych treści stawiało przed Komisją 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 19 stycznia 2016 r. (2015/2147(INI)) odwołano się do klasycznego standardu wolności wypowiedzi wypracowanego na gruncie EKPC, otwierając zarazem drogę do ustanowienia nowego modelu korzystania z wolności wypowiedzi, który, ze względu na specyfikę komunikowania w cyberprzestrzeni, dawał prawodawcy europejskiemu podstawę do dokonywania zmiany wykładni w kierunku standardu bardziej wymagającego, a przez to bardziej restrykcyjnego standardu wolności wypowiedzi[25].

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 [...], a także z zasadami konieczności, proporcjonalności, sprawiedliwości proceduralnej i praworządności" (pkt 88 rezolucji). 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

[22] Art. 1 ust. 1 AUC.

[23] Zob. A. Mikoś, *Konstytucja internetu*, https://informacjapubliczna.org/news/konstytucja-internetu/ (dostęp: 20 czerwca 2024 r.); podobnie S. Cydzik, *Kto i jak ma pilnować wykonania konstytucji internetu*, https://www.rp.pl/internet-i-prawo-autorskie/art40009831-kto-i-jak-ma-pilnowac-wykonania-konstytucji-internetu; *Wchodzi w życie konstytucja internetu. Oto co się zmieni*, https://www.money.pl/gospodarka/wchodzi-w-zycie-konstytucja-internetu-oto-co-sie-zmieni-6996220038113952a.html (dostęp: 20 czerwca 2024 r.).

[24] Rezolucja Parlamentu Europejskiego z 19 stycznia 2016 r. w sprawie „W kierunku aktu o jednolitym rynku cyfrowym" (2015/2147(INI)) (Dz.Urz. UE C 11 z 2018 r., s. 55), pkt 82.

[25] Zob. rezolucja 2015/2147(INI), 3.3.3. Zwalczanie nielegalnych treści w internecie.

społecznej potrzeby) oraz wymóg zachowania proporcjonalności, dodano nowe przesłanki, tj. potrzebę zapewnienia sprawiedliwości proceduralnej oraz wymóg praworządności. Przesłanki te mają mieszany charakter: formalno-materialny i mogą stanowić *de facto* nie tyle zaostrzenie rygorów testu szkodliwości, ile 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 aby 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;
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) współpracować z odnośnymi zainteresowanymi stronami na rzecz promowania kampanii edukacyjnych i podnoszących świadomość (pkt 82 rezolucji).

Realizację zaleceń Parlamentu Europejskiego stanowiło przedłożenie przez Komisję Europejską wniosku w sprawie przyjęcia przez Parlament Europejski dwóch rozporządzeń cyfrowych tworzących tzw. pakiet cyfrowy, tj.: rozporządzenia w sprawie jednolitego rynku usług cyfrowych oraz rozporządzenia w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym (ARC). Rada Europejska w komunikacie z 4 października 2022 r. 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 wewnętrznego [wyróżn. – aut.]"[26].

[26] Zob. https://www.consilium.europa.eu/pl/meetings/ecofin/2022/10/04/ (dostęp: 20 czerwca 2024 r.).

Zapewnienie efektywności rozwiązań zaproponowanych w AUC i ARC było możliwe do osiągnięcia dzięki uprzedniemu uporządkowaniu zasad przetwarzania danych osobowych i stworzeniu nowego rynku gospodarczego, jakim jest rynek danych. Nastąpiło to w dwóch aktach prawnych: 1) rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z 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)[27] oraz rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2018/1807 z 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej[28]. Wskazane akty normatywne pozostają zarazem w funkcjonalnym związku z Aktem w sprawie sztucznej inteligencji przyjętym w pierwszym czytaniu przez Parlament Europejski w dniu 13 marca 2024 r.[29] oraz rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2022/868 z 30 maja 2022 r. w sprawie europejskiego zarządzania danymi i zmieniającym rozporządzenie (UE) 2018/1724 (akt w sprawie zarządzania danymi)[30].

Wskazane 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 aktach prawnych narzędzia, instrumenty i instytucje oddziałują nie tylko na sferę stosunków gospodarczych, ale ingerują w sferę wolności i praw stron tych stosunków, w szczególności w sferę wolności wypowiedzi.

---

[27] Dz.Urz. UE L 119 z 2016 r., s. 1, ze zm. – dalej jako RODO. 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*, https://www.traple.pl/wzajemna-relacja-rodo-i-aktu-w-sprawie-sztucznej-inteligencji-10-najwazniejszych-informacji/ (dostęp: 20 czerwca 2024 r.).

[28] Dz.Urz. UE L 303 z 2018 r., 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".

[29] Akt w sprawie sztucznej inteligencji Rezolucja ustawodawcza Parlamentu Europejskiego z 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 (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_PL.html (dostęp: 22 marca 2024 r.).

[30] Dz.Urz. UE L 152 z 2022 r., s. 1.

2. Standard wolności wypowiedzi – zakres terminu

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, a także 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 wpływały na standard wolności wypowiedzi, dokonując, w efekcie, jego uchylenia bądź zmiany[31].

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 jest dopuszczalne w związku z zastosowaniem sformalizowanego wzorca oceny, ale także sam wzorzec. Przyjąć bowiem można, że dopiero sprzężenie metody dokonywania oceny z jej wynikiem pozwala na wypracowanie standardu wolności wypowiedzi.

[31] J. Taczkowska-Olszewska, *Racjonalizacja wolności prasy – od modelu absolutnego do warunkowego, Europejski i krajowy kontekst wykładni prawa*, „Przegląd Sejmowy" 2018, nr 1(144), s. 115.

Nie jest jednak bez znaczenia, że uzyskanie tego rezultatu wymaga, by zarówno te podmioty, które korzystają z wolności wypowiedzi, jak i organy, które dokonują oceny, 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.

Potwierdzenie przez Trybunał Sprawiedliwości Unii Europejskiej i Europejski Trybunał Praw Człowieka, 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[32]. 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 internetowymi[33]. 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[34]. Przepisy te zawierały 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 Trybunał Sprawiedliwości uzależniał od

[32] Do celów rozporządzenia o usługach cyfrowych przyjęto, że pojęcie „nielegalne treści" powinno w szerokim zakresie odzwierciedlać istniejące przepisy w środowisku pozainternetowym (motyw 12 AUC).

[33] Chodzi o takie akty prawa europejskiego jak: dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z 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.Urz. UE L 178 z 2000 r., s. 1, ze zm. – dalej jako dyrektywa 2000/31/WE) albo akt o usługach cyfrowych i akt o rynkach cyfrowych.

[34] Przepisy te zostały uchylone z dniem 17 lutego 2024 r. w związku z wejściem w życie aktu o usługach cyfrowych. Zgodnie z art. 89 ust. 2 AUC odesłania do art. 12–15 dyrektywy 2000/31/WE odczytuje się jako odesłania odpowiednio do art. 4, 5, 6 i 8 AUC.

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”[35].

2.1. Wolność wypowiedzi w europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności

Gwarancje wolności wypowiedzi zostały potwierdzone w wielu aktach prawa ponadnarodowego, w szczególności w art. 10 EKPCi[36], a także art. 11 KPP oraz w art. 19 MPPOiP i w art. 19 Powszechnej Deklaracji Praw Człowieka[37].

[35] Wyrok TS z 7 sierpnia 2018 r., C-521/17, Coöperatieve Vereniging SNB-REACT U.A. przeciwko Deepakowi Mehcie, ECLI:EU:C:2018:639; podobnie wyrok TS z 11 września 2014 r., C-291/13, Sotiris Papasavvas przeciwko O Fileleftheros Dimosia Etaireia Ltd i in., ECLI:EU:C:2014:2209, a także wyrok TS z 15 września 2016 r., C-484/14, Tobias Mc Fadden przeciwko Sony Music Entertainment Germany GmbH, ECLI:EU:C:2016:689.

[36] Polska ratyfikowała tę Konwencję 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 Konwencji (zob. 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” 2015, t. 17, s. 86). Polska ratyfikowała Protokół nr 15 w drodze ustawy z 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). W uzasadnieniu projektu tej ustawy wskazano, że: „Protokół nr 15 w art. 1 dodaje do preambuły Konwencji nowy ustęp, zawierający odwołanie do zasady subsydiarności mechanizmu ochronnego Konwencji i do doktryny marginesu oceny państwa oraz podkreślający obowiązek państw zapewnienia pełnej skuteczności praw i wolności określonych w Konwencji. (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., Sejm VII kadencji, druk sejmowy nr 3056, https://www.sejm.gov.pl/Sejm7.nsf/PrzebiegProc.xsp?nr=3056, dostęp: 20 czerwca 2024 r.).

[37] 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: 20 czerwca 2024 r.). Powszechna Deklaracja Praw Człowieka zdała się stać na gruncie absolutnych, czyli naturalnych praw człowieka (zob. J. Sobczak, Komentarz do art. 11 KPP [w:] *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, red. A. Wróbel, Warszawa 2020 wraz z cytowaną tam literaturą, a w szczególności: H. Andrzejczak, *Filozoficznoprawne podstawy Powszechnej Deklaracji Praw Człowieka*, „Roczniki Filozoficzne” 1966, t. 14, z. 2, s. 81 i n.; J. Motyka, *50 lat minęło. Powszechna Deklaracja Praw Człowieka i jej credo*, „Prawo i Życie” 1998, nr 39; J. Motyka, *Prawa człowieka. Wprowadzenie. Wybór źródeł*, Lublin 2004, s. 41–44). Jak zauważa J. Sobczak, 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 udzia-

Wolność wypowiedzi stanowi jeden z zasadniczych fundamentów społeczeństwa demokratycznego i jeden z podstawowych warunków jego rozwoju oraz samorealizacji każdej jednostki[38]. 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 społeczeństwo[39].

Zgodnie z orzecznictwem Europejskiego Trybunału Praw Człowieka „art. 10 EKPC gwarantuje każdemu wolność wypowiedzi i informacji i dotyczy nie tylko treści informacji, ale także środków ich rozpowszechniania, a wszelkie ograniczenia tych środków wpływają na prawo do otrzymywania i przekazywania informacji. Jak zauważył ten sąd, 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 ich zdolności do przechowywania i rozpowszechniania dużej ilości danych, przyczyniają się w dużej mierze do zwiększania dostępu ogółu społeczeństwa do aktualnych wiadomości i […] do ułatwiania przekazywania informacji, gdyż możliwość wypowiadania się przez jednostki w Internecie stanowi bezprecedensowe narzędzie umożliwiające korzystanie z wolności wypowiedzi (zob. podobnie wyroki ETPC: z dnia 1 grudnia 2015 r. w sprawie Cengiz i in. przeciwko Turcji, CE:ECHR:2015:1201JUD004822610, § 52; z dnia 23 czerwca 2020 r. w sprawie Vladimir Kharitonov przeciwko Rosji, CE:ECHR:2020:0623JUD001079514, § 33 i przytoczone tam orzecznictwo)”[40]. 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 informacji[41]. Takie udostępnienie online może również dotyczyć innych pokrewnych wol-

łu 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.” (J. Sobczak, Komentarz do art. 11 KPP [w:] *Karta*…, pkt 7).

[38] Zob. wyroki ETPC: z 8 lipca 1986 r., skarga nr 9815/82, Lingens przeciwko Austrii, § 41; z 8 listopada 2022 r., skarga nr 55212/15, Magdalena Bajer i inni przeciwko Polsce; wszystkie powołane w tekście wyroki ETPC dostępne są w bazie HUDOC.

[39] Wyroki ETPC: z 7 grudnia 1976 r., skarga nr 5493/72, Handyside przeciwko Zjednoczonemu Królestwu, § 49; z 8 lipca 1986 r., skarga nr 8815/82, Lingens przeciwko Austrii; z 23 kwietnia 1992 r., skarga nr 11798/85, Castells przeciwko Hiszpanii; z 1 lipca 1997 r., skarga nr 20834/92, Oberschlick przeciwko Austrii.

[40] Wyrok TS z 26.04.2022 r., C-401/19, Rzeczpospolita Polska przeciwko Parlamentowi Europejskiemu i Radzie Unii Europejskiej, ECLI:EU:C:2022:297, pkt 46.

[41] Wyroki ETPC: z 19 lutego 2013 r., skarga nr 40397/12, Neij i Sunde Kolmisoppi przeciwko Szwecji, § 9, 10; z 10 kwietnia 2013 r., skarga nr 36769/08, Ashby Donald i inni przeciwko Francji, § 34; a także opinia rzecznika generalnego N. Jääskinena z 9 grudnia 2010 r. w sprawie L'Oréal i in., C-324/09, ECLI:EU:C:2010:757, pkt 49 i 157.

ności. 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 KPP oraz w art. 10 EKPC[42].

Niemniej jednak art. 10 EKPC 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 ponadto jest uzasadniona realizacją ważnego celu społecznego, jednak tylko wtedy, gdy wkroczenie w wolność wypowiedzi nie narusza istoty tej wolności, a zastosowana sankcja jest proporcjonalna w stosunku do uprawnionego celu[43]. 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"[44].

Artykuł 10 EKPC chroniący swobodę wypowiedzi składa się z dwóch części[45]. 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 EKPC 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 swobody[46]. Dotyczy ona nie tylko treści informacji, ale również środków, za pomocą których są one rozpowszechniane, w tym internetu, ponieważ każde ich ograniczenie narusza prawo do otrzymywania i przekazywania informacji[47]. Podobnie Trybunał wielokrotnie stwierdzał, że art. 10 EKPC gwarantuje nie tylko prawo do przekazywania informacji, ale również prawo społeczeństwa do ich otrzymywania[48].

Ustęp drugi art. 10 EKPC odnosi się do możliwości ingerencji w swobodę wypowiedzi. Każde ograniczenie musi łącznie spełniać trzy warunki: być przewidziane przez prawo,

---

[42] O ile bowiem EKPC nie zawiera takiej wolności jako autonomicznego prawa, o tyle „wolność wypowiedzi artystycznej" jest objęta art. 10 EKPC. Zob. w szczególności wyroki ETPC: z 24 maja 1988 r., skarga nr 10737, Müller i in. przeciwko Szwajcarii, § 27; a także z 8 lipca 1999 r., skarga nr 23168/94, Karataş przeciwko Turcji, § 49.

[43] Wyroki ETPC: z 26 kwietnia 1979 r., skarga nr 6538/74, Sunday Times przeciwko Wielkiej Brytanii, § 62; z 27 maja 2003 r., skarga nr 43425/98, Skałka przeciwko Polsce, § 35.

[44] Wyrok ETPC z 7 grudnia 1976 r., skarga nr 5493/72, Hendyside przeciwko Wielkiej Brytanii.

[45] I.C. Kamiński, *Mowa nienawiści– pojęcie i jego zakres* [w:] *Prawna kwalifikacja mowy nienawiści. Krajowe i europejskie uwarunkowania nadużycia wolności wypowiedzi*, red. J. Taczkowska-Olszewska, Warszawa 2024, s. 90.

[46] Zob. wyrok ETPC z 13 lutego 2003 r., skarga nr 40153/98 i 40160/98, Çetin i inni przeciwko Turcji, § 57.

[47] Zob. wyrok ETPC z 22 maja 1990 r. skarga nr 12726/87, Autronic AG przeciwko Szwajcarii, § 47.

[48] Wyrok ETPC z 26 listopada 1991 r., skarga nr 13585/88, Observer i Guardian przeciwko Wielkiej Brytanii, § 59, oraz z 19 lutego 1998 r., skarga nr 14967/89, Guerra i in. przeciwko Włochom, § 53.

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 sposób[49]. 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 – proporcjonalna"[50].

Do uprawnionej ingerencji w swobodę wypowiedzi zatem może dojść w przypadku spełnienia łącznie kilku przesłanek, które składają się na tzw. test szkodliwości (*harm test*). Dopiero po przeprowadzeniu testu szkodliwości i ustaleniu, że zawarte w nim przesłanki zaistniały, możliwe jest zaakceptowanie ingerencji w wolność wypowiedzi jako działania usprawiedliwionego. Konieczne jest zatem, jak wskazano wcześniej, ustalenie, czy: 1) zastosowane ograniczenie wolności wypowiedzi było przewidziane przez prawo; 2) czy ingerencja była niezbędna (konieczna) w społeczeństwie demokratycznym, a ponadto, czy 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 wystarczające (zob. między innymi wyroki: z 26 listopada 2013 r. Błaja News Sp. Z o.o. przeciwko Polsce, skarga nr 59545/10, § 56; z 18 września 2012 r. Lewandowska-Malec przeciwko Polsce, skarga nr 39660/07, § 58, z 26 kwietnia 1979 r. The Sunday Times przeciwko Zjednoczonemu Królestwu (nr 1), § 62; oraz z 27 maja 2003 r. Skałka przeciwko Polsce, skarga nr 43425/98, § 35)"[51].

Powyższe zasady znajdują zastosowanie także w orzecznictwie Trybunału Sprawiedliwości, co wynika przede wszystkim z treści art. 52 ust. 3 zd. 1 KPP[52]. Wyraźne powołanie

[49] Wyrok ETPC z 26 kwietnia 1979 r., skarga nr 6538/74, Sunday Times przeciwko Wielkiej Brytanii, § 49.
[50] I.C. Kamiński, *Pojęcie*..., s. 203.
[51] Wyrok SN z 21 kwietnia 2021 r., I NSNc 89/20, OSNKN 2021, nr 3, poz. 23.
[52] 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".

się TSUE (wcześniej ETS) na art. 10 EKPC miało miejsce w sprawie ERT[53], 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 EKPC[54]. Trybunał powołał się również na art. 10 i 11 KPP w orzeczeniu w sprawie RTL[55] dotyczącej emitowania reklam w telewizji. Trybunał 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 poglądów[56].

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 odgrywa ważną rolę w poprawie publicznego dostępu do informacji i ogólnie udostępnianiu informacji[57]. 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 prasę[58]. Ze względu na szczególny charakter internetu, jeżeli chodzi o treści osób trzecich, dla celów art. 10 EKPC takie „obowiązki i odpowiedzialność" internetowych portali informacyjnych mogą w pewnym stopniu różnić się od tych spoczywających na wydawcy w rozumieniu tradycyjnym[59]. Jakkolwiek stanowisko to Trybunał wypowiedział, dokonując porównania pomiędzy dystrybucją informacji w internecie a wydawaniem prasy, to jednak znajduje ono zastosowanie nie tylko do wydawania prasy, ale 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

---

[53] Wyrok TS z 18 czerwca 1991 r., C-260/89, Elliniki Radiophonia Tiléorassi AE i Panellinia Omospondia Syllogon Prossopikou przeciwko Dimotiki Etairia Pliroforissis i Sotirios Kouvelas i Nicolaos Avdellas i innym, ECLI:EU:C:1991:254.

[54] T. Jurczyk, *Prawa jednostki w orzecznictwie Europejskiego Trybunału Sprawiedliwości*, Warszawa 2009, s. 189.

[55] Wyrok TS z 23 października 2003 r., C-245/01, RTL Television GmbH przeciwko Niedersächsische Landesmedienanstalt für privaten Rundfunk, ECLI:EU:C:2003:580.

[56] Wyrok TS z 5 października 1994 r., C-23/93, TV10 SA przeciwko Commissariaat voor de Media, ECLI:EU:C:1994:362.

[57] Wyrok ETPC z 18 grudnia 2012 r., skarga nr 3111/10, Ahmet Yildirim przeciwko Turcji, § 48.

[58] Wyrok ETPC z 7 listopada 2017 r., skarga nr 24703/15, Egill Einarsson przeciwko Islandii, § 46.

[59] Wyrok ETPC z 16 czerwca 2015 r., skarga nr 64569/09, Delfi AS przeciwko Estonii, § 113.

specyfiki nowych technologii[60]. 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 człowieka[61].

Z analizy przeprowadzonej przez ETPC dotyczącej ustawodawstwa 20 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 nierozerwalnie związane z prawem dostępu do informacji i komunikacji chronionym przez konstytucje krajowe oraz że obejmuje prawo każdego do uczestnictwa w społeczeństwie informacyjnym oraz obowiązek państw do zagwarantowania obywatelom dostępu do internetu. Na tle ogólnych gwarancji chroniących wolność wypowiedzi można zatem przyjąć, że należy do nich również prawo do nieskrępowanego dostępu do internetu[62].

Trybunał zauważył, że jeśli chodzi o możliwe środki mające na celu ograniczenie nielegalnych treści w internecie, w dokumentach państw UE istniało wiele różnych podejść i instrumentów legislacyjnych, począwszy od zindywidualizowanego 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 zastosowania odpowiednich środków w celu ograniczenia dostępu do stron internetowych zawierających treści zagrażające dobru

---

[60] Wyrok ETPC z 5 maja 2011 r., skarga nr 33014/05, Redakcja Prawoje Dielo i Sztekel przeciwko Ukrainie, § 63.

[61] W decyzji z 10 czerwca 2009 r. (decyzja nr 2009580 DC) Francuska Rada Konstytucyjna wyjaśniła, że wolność wypowiedzi oznacza wolność dostępu do internetu. Wskazano w niej również szereg podstawowych zasad dotyczących ograniczenia tego dostępu. 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, „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. Francuska Rada Konstytucyjna wypowiedziała się 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 kwietnia 2024 r.).

ETPC orzekł, że zawieszenie dostępu jest możliwe tylko wtedy, gdy zostało zarządzone po zakończeniu kontradyktoryjnego postępowania sądowego jako kara 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 z 18 grudnia 2012 r., skarga nr 3111/10, Ahmet Yildirim przeciwko Turcji, § 32). Francuska Rada Konstytucyjna wypowiedziała się we wskazanej decyzji w związku z procedowaną wówczas tzw. ustawą HADOPI (skrót od „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. https://www.hadopi.fr/organisation/presentation, dostęp: 2 kwietnia 2024 r.).

[62] Wyrok ETPC z 18 grudnia 2012 r., skarga nr 3111/10, Ahmet Yildirim przeciwko Turcji, § 32.

małoletnich (Niemcy, Zjednoczone Królestwo, Szwajcaria i Francja). Jeśli chodzi o zwykłą przestępczość, ograniczenia dostępu są różne i mniej dotkliwe w sześciu krajach (Austria, Estonia, Finlandia, Włochy, Litwa, Niderlandy)[63].

Artykuł 10 EKPC jako taki nie zakazuje stosowania uprzednich ograniczeń w zakresie rozpowszechniania wypowiedzi (*ex ante*). Trybunał wskazał[64], że o braku takiego zakazu przesądzają użyte w art. 10 EKPC terminy: „warunki", „ograniczenia", „zapobieganie", „sankcje", co zostało odzwierciedlone w wyroku w sprawie Sunday Sunday Times przeciwko Wielkiej Brytanii[65]. Trybunał 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 tematu"[66]. 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 Brytanii[67], 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 informacji"[68].

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

1) pozostają pod ochroną prawa nawet takie wypowiedzi, których treść lub forma oburza lub wprowadza niepokój[69];

---

[63] Wyrok ETPC z 18 grudnia 2012 r., skarga nr 3111/10, Ahmet Yildirim przeciwko Turcji, § 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 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, Zjednoczone Królestwo), na przykład w przypadkach pornografii dziecięcej lub rasizmu, nawoływania do nienawiści, podżegania do terroryzmu lub zniesławienia" (§ 34 wspomnianego wyroku).

[64] Wyrok ETPC z 18 grudnia 2012 r., skarga nr 3111/10, Ahmet Yildirim przeciwko Turcji, § 47.

[65] Zob. wyrok ETPC z 26 kwietnia 1979 r., skarga nr 6538/74, Sunday Times przeciwko Wielkiej Brytanii oraz wyrok ETPCz z 20 listopada 1989 r., skarga nr 10572/83, Markt intern Verlag GmBH i Klaus Beermann przeciwko Niemcom.

[66] Wyrok ETPC z 18 grudnia 2012 r., skarga nr 3111/10, Ahmet Yildirim przeciwko Turcji, § 47.

[67] Wyrok ETPC z 10 marca 2009 r., skargi nr 3002/03 i 23676/03, Times Newspapers Ltd przeciwko Wielkiej Brytanii, § 27.

[68] Wyrok ETPC z 18 grudnia 2012 r., skarga nr 3111/10, Ahmet Yildirim przeciwko Turcji, § 48.

[69] W sprawie Handyside przeciwko Zjednoczonemu Królestwu ETPC wypowiedział fundamentalne dla ustalenia zakresu standardu wolności wypowiedzi stanowisko, zgodnie z którym: „Wolność słowa jest jednym

2) wolność wypowiedzi stanowi filar demokracji, będąc warunkiem koniecznym systemów demokratycznych[70];
3) jej ograniczenie może następować wyjątkowo – zasadą jest swoboda wypowiedzi, podczas gdy jej ograniczenie jest wyjątkiem od tej zasady i każdorazowo powinno być precyzyjnie uzasadnione[71];
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 uprawnioną[72];
6) państwo ma spełniać funkcje gwaranta wolności wypowiedzi, ale nie jest wykluczone, że spoczywać będą na nim obowiązki pozytywne nawet w stosunkach pomiędzy podmiotami prywatnymi[73];
7) ochrona wolności wypowiedzi obejmuje nie tylko treść, ale także formę jej wyrażenia[74];
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 mieć podstawę faktyczną[75].

---

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" (§ 49–50 wyroku).

[70] Zob. wyrok ETPC z 7 grudnia 1976 r., skarga nr 5493/72, Handyside przeciwko Zjednoczonemu Królestwu, § 49–50.

[71] Zob. wyrok ETPC z 7 grudnia 1976 r., skarga nr 5493/72, Handyside przeciwko Zjednoczonemu Królestwu, § 49–50.

[72] Wyrok ETPC 1 lipca 1997 r., skarga nr 20834/92, Oberschlick przeciwko Austrii, § 29.

[73] 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 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 12 sierpnia 2011 r., skarga nr 28955/06, Palomo Sánchez i inni przeciwko Hiszpanii, § 59).

[74] Zob. wyrok ETPC z 3 kwietnia 2009 r., skarga nr 31276/05, Women on Waves przeciwko Portugalii, § 38; podobnie: wyrok ETPC z 6 maja 2003 r., skarga nr 44306/98, Appleby i inni przeciwko Wielkiej Brytanii, § 39; wyrok ETPC z 30 czerwca 2009 r., skarga nr 32772/02, Verein gegen Tierfabriken Schweiz (VgT) przeciwko Szwajcarii, § 80; zob. również, *mutatis mutandis*, wyrok ETPC z 16 marca 2000 r., skarga nr 23144/93, Özgür Gündem przeciwko Turcji, § 42–46; wyrok ETPC z 29 lutego 2000 r., skarga nr 39293/98, Fuentes Bobo przeciwko. Hiszpanii, § 38.

[75] Zob. wyroki z 19 czerwca 2003 r., skarga nr 49017/99, Pedersen i Baadsgaard przeciwko Danii § 76; z 22 stycznia 2015 r., skarga nr 26671/09, Pinto Pinheiro Marques przeciwko Portugalii, § 43; z 19 lipca 2018 r., skargi nr 64659/11 i 24133/13, Makraduli przeciwko Macedonii, § 62.

2.2. Wolność wypowiedzi w Karcie praw podstawowych Unii Europejskiej

Artykuł 11 KPP odpowiada standardowi z art. 10 EKPC. Prawo zagwarantowane w art. 11 ust. 1 KPP, 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 EKPC.

Struktura i treść art. 11 KPP jest w dużej mierze zbieżna z art. 10 ust. 1 EKPC[76]. 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". Zgodnie z art. 52 ust. 3 KPP te dwa prawa mają zatem takie samo znaczenie lub co najmniej ten sam zakres. Z powyższego wynika, że art. 11 KPP należy interpretować w świetle art. 10 EKPC i związanego z nim orzecznictwa Europejskiego Trybunału Praw Człowieka[77].

Artykuł 52 ust. 3 KPP, nazywany niekiedy klauzulą transferową, reguluje relacje między postanowieniami Karty i (materialnoprawnymi) postanowieniami EKPC oraz zasady wykładni odnośnych postanowień Karty (zd. 1), a także pozwala uznać standard ochronny, gwarantowany postanowieniami Konwencji, za standard minimalny (zd. 2)[78]. Zgodnie z art. 52 ust. 1 KPP 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.

Trybunał Sprawiedliwości 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 prawa[79]. Zasada proporcjonalności wymaga natomiast, by ograniczenia, które mogą

[76] 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 do art. 11 KPP [w:] *Karta*..., pkt 3).

[77] Opinia rzecznika generalnego H. Saugmandsgaarda Øe z 15 lipca 2021 r., C-401/19, Rzeczpospolita Polska przeciwko Parlamentowi Europejskiemu, Radzie Unii Europejskiej, Legalis.

[78] A. Wróbel, Komentarz do art. 52 KPP [w:] *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, red. A. Wróbel, Warszawa 2020, pkt 44.

[79] Wyrok TS z 16 lipca 2020 r., C-311/18, Data Protection Commissioner przeciwko Facebook Ireland Limited i Maximillianowi Schremsowi, ECLI:EU:C:2020:559, pkt 175 – dalej wyrok C-311/18, Facebook Ireland i Schrems.

być zwłaszcza nałożone 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 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 celów[80]. 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 zasadami[81]. Ponadto, aby spełnić wymóg proporcjonalności, uregulowanie prowadzące do ingerencji w prawa podstawowe powinno zawierać jasne i precyzyjne reguły dotyczące zakresu i sposobu 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 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 procesu[82].

Trybunał Sprawiedliwości 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. Wszelkie takie ograniczenia muszą spełniać wymogi zasady proporcjonalności. Wymaga ona, by ograniczenia, które mogą być zwłaszcza nałożone 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 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 celów[83]. W przypadku gdy sprawa

[80] Zob. wyroki TS z 13 marca 2019 r., C-128/17, Rzeczpospolita Polska przeciwko Parlamentowi Europejskiemu i Radzie Unii Europejskiej, ECLI:EU:C:2019:194 – dalej wyrok C-128/17, Polska przeciwko Parlamentowi i Radzie, pkt 94 i przytoczone tam orzecznictwo; z 17 grudnia 2020 r., C-336/19, Centraal Israëlitisch Consistorie van België i in., ECLI:EU:C:2020:1031, pkt 64 i przytoczone tam orzecznictwo – dalej wyrok C-336/19, Centraal Israëlitisch Consistorie van België i in.

[81] Wyrok C-336/19, Centraal Israëlitisch Consistorie van België i in., pkt 65 i przytoczone tam orzecznictwo.

[82] Wyrok C-311/18, Facebook Ireland i Schrems, pkt 176.

[83] Zob. wyroki C-128/17, Polska przeciwko Parlamentowi i Radzie, pkt 94 i przytoczone tam orzecznictwo; C-336/19, Centraal Israëlitisch Consistorie van België i in., pkt 64 i przytoczone tam orzecznictwo.

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, o których mowa, oraz odpowiedniej równowagi między tymi prawami i zasadami[84].

Stanowiska wyrażane przez ETPC i TSUE (ETS) na gruncie, odpowiednio art. 10 EKPC i art. 11 KPP, nie mają 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 „jakość 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 wymogami[85].

Standardy wolności wypowiedzi ustalone na gruncie art. 10 EKPC i art. 11 KPP 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 osiągnięciu tego standardu stają względy technologiczne, związane z przeniesieniem debaty publicznej do internetu, a w konsekwencji potrzebą dostosowania zarówno w aspekcie proceduralnym (formalnym), jak i materialnoprawnym wzorca ochrony do nowych zagrożeń związanych z realizacją wolności wypowiedzi.

[84] Wyrok C-336/19, Centraal Israëlitisch Consistorie van België i in., C-336/19, pkt 65.
[85] I.C. Kamiński, *Pojęcie*..., s. 203.

3. Ingerencja w wolność wypowiedzi na rynku cyfrowym

Organy unijne w warstwie werbalnej stoją na stanowisku, zgodnie z którym: „Internet powinien pozostać jednolitą, otwartą, wolną, niepodzieloną siecią sieci, podlegającą tym samym przepisom i normom, które mają zastosowanie w innych obszarach naszego życia codziennego”[86]. 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 niego”[87]. Komisja Europejska w odniesieniu do zarządzania internetem występowała na rzecz podejścia określanego skrótem COMPACT[88], zgodnie z którym internet jest przestrzenią odpowiedzialności obywatelskiej (*civic responsibilities*), jednym niepodzielnym zasobem (*one unfragmented resource*) zarządzanym w sposób oparty na porozumieniu zainteresowanych stron (*multistakeholder approach*) w celu wspierania demokracji i praw człowieka (*promote democracy and human rights*) w oparciu o solidną architekturę techniczną (*architecture*), która jest źródłem zaufania (*confidence*) i sprzyja przejrzystości zarządzania (*transparent governance*) zarówno bazową infrastrukturą internetu, jak i usługami wykonywanymi przy jej użyciu[89].

Podejście to wskazuje na próbę pogodzenia tendencji wolnościowych z koncepcjami zalecającymi uruchomienie mechanizmów kontrolnych i nadzorczych. Parlament Europejski w rezolucji 2009/2229(INI) w sprawie zarządzania internetem potwierdził, iż „uważa, że Internet jest globalnym publicznym dobrem, i że w związku z tym należy nim zarządzać we wspólnym interesie” (lit. I pkt 1) oraz przyznał, że „Internet ma zasadnicze znaczenie dla praktycznej realizacji wolności słowa” (lit. I pkt 2) 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

[86] Komunikat KE COM/2014/072, pkt 9.
[87] Komunikat KE COM/2014/072, pkt 1.
[88] Podejście COMPACT jest oparte na programie z Tunisu z 2005 r.
[89] Komunikat KE COM/2014/072.

poszanowanie życia prywatnego, ochronę danych, wolność wypowiedzi, słowa i zrzeszania się, wolność prasy, głoszenia poglądów politycznych i udziału w życiu politycznym" (lit. I pkt 3). W opinii Komitetu Regionów internet stanowi „globalną przestrzeń informacji"[90], a dostęp do niego stanowi „niezbywalne prawo obywatelskie"[91].

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"[92]. Już w 2015 r. wyraźnie jednak założono, że model zarządzania internetem, jaki miałby zostać przyjęty w UE, „nie może wykluczać interwencji regulacyjnej, podejmowanej z uwagi na cele leżące w interesie publicznym"[93].

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"[94]. Wskazane cele wykraczają poza sformułowany w art. 10 ust. 2 EKPC katalog materialnoprawnych przesłanek usprawiedliwiających ingerencję. Różnica w sposobie określenia celów ingerencji ma charakter nie tylko ilościowy, ale 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*[95]), co pozwala na duża swobodę interpretacji, a w konsekwencji nie gwarantuje pewności prawa (chodzi o cele ujmowane jako: zapewnienie poszanowania praw człowieka, podstawowych wolności i wartości demokratycznych).

Do czasu przyjęcia przez Parlament Europejski i Radę pakietu rozporządzeń cyfrowych eliminowanie nieodpowiednich treści z internetu następowało w wyniku realizacji dobrowolnie przyjętych przez dostawców usług cyfrowych obowiązków wynikających z akceptowanych przez nich kodeksów etycznych. Zarazem jednak, ze względu na opisany w dyrektywie o handlu elektronicznym[96] mechanizm wyłączenia odpowiedzialności

---

[90] Opinia Komitetu Regionów – Polityka wobec internetu i zarządzanie internetem, pkt 1 (Dz.Urz. UE C 19 z 2015 r., s. 65).

[91] Opinia Komitetu Regionów – Polityka wobec internetu i zarządzanie internetem, pkt 8. W dokumencie zwrócono uwagę, że w niektórych państwach prawo dostępu do internetu zostało uznane za jedno z praw podstawowych. W 2009 r. orzekł tak Trybunał Konstytucyjny Francji. 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 szczeblu Narodów Zjednoczonych.

[92] Komunikat KE COM/2014/072, pkt 9.

[93] Komunikat KE COM/2014/072, pkt 9.

[94] Komunikat KE COM/2014/072, pkt 9.

[95] Wykładni *largissimo sensu* poddawane są także zachowania pewnych podmiotów, w tym prawodawcy; zob. M. Zieliński, *Wykładnia prawa. Zasady – reguły – wskazówki*, Warszawa 2002, s. 59.

[96] Art. 12–15 dyrektywy o handlu elektronicznym. Przepisy te, jak wcześniej zauważono, zostały uchylone na podstawie art. 89 ust. 1 AUC. Zarazem ustawodawca europejski wskazał w art. 89 ust. 2 AUC, że odesłania do

pośredników internetowych za naruszenia prawa spowodowane rozpowszechnieniem nielegalnych treści, pośrednicy nie zawsze na nie reagowali w podobny sposób. W rezultacie te same treści, ale rozpowszechniane na innych platformach albo w innym obszarze geograficznym, spotykały się z odmienną reakcją. O ile mogło to być uzasadnione niejednorodnym podejściem legislatora wynikającym z różnorodnych tradycji prawnych, historycznych lub kulturowych, o tyle ingerencje w wolność wypowiedzi były niezrozumiałe, gdy podejmowały je podmioty prywatne (dostawcy usług pośrednich) na podstawie arbitralnych decyzji, stosując niejasne i niejednorodne kryteria. Powyższe spostrzeżenie stanowiło asumpt do działania w kierunku ujednolicenia zasad postępowania w związku z treściami niedozwolonymi.

3.1. Harmonizacja prawa

Ustawodawstwo krajowe zarówno w obszarze państw UE, jak również, 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)[97], 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

art. 12–15 dyrektywy 2000/31/WE odczytuje się jako odesłania odpowiednio do art. 4, 5, 6 i 8 AUC. Zgodnie z brzmieniem art. 4–6 AUC mechanizm wyłączenia odpowiedzialności pośredników za naruszenia prawa spowodowane rozpowszechnieniem nielegalnych treści, co do zasady, nie zmienił się. Ze względu jednak na nałożone w AUC na pośredników obowiązki związane z zapobieganiem rozpowszechnianiu nielegalnych treści, ustawodawca europejski zezwolił na monitorowanie i filtrowanie treści oraz dokonywanie oceny rozpowszechnianych przez internautów materiałów pod kątem ich zgodności z prawem, a na wypadek, gdyby treści zostały ocenione przez pośredników jako naruszające prawo (nielegalne), zezwolił na ich usuwanie i blokowanie do nich dostępu. Zasadniczego znaczenia dla konstrukcji standardu wolności wypowiedzi nabierają przepisy zawarte w art. 7 i 8 AUC. Konstruują one domniemanie zgodności z prawem takiego działania pośredników, które – o ile jest motywowane potrzebą zwalczania nielegalnych treści – może polegać na ingerowaniu w wolność wypowiedzi internautów bez potrzeby uzyskania nakazu sądowego.

[97] Content & Jurisdiction Program, Operational Approaches Norms, Criteria and Mechanisms, April 2019, s. 7, https://www.internetjurisdiction.net/uploads/pdfs/Papers/Content-Jurisdiction-Program-Operational-Approaches.pdf (dostęp: 20 czerwca 2024 r.).

nieodpowiednich treści w internecie, nie zawsze w pełni respektuje międzynarodowe standardy praw człowieka i gwarancje rzetelnego procesu"[98].

Za główne wyzwanie przy opracowywaniu i wdrażaniu przepisów krajowych, a także wytycznych na poziomie globalnym uznano konieczność pogodzenia konkurujących ze sobą praw, a mianowicie wolności wypowiedzi i zapobiegania jej nadużyciu[99]. W celu ustalenia stopnia międzynarodowej zbieżności normatywnej w odniesieniu do identyfikowania nielegalnych treści w internecie wyodrębniono cztery kategorie stanowisk:

1) istnieje powszechna zgoda co do tego, że treści/zachowania są nielegalne ORAZ istnieje silna zbieżność merytoryczna na całym świecie w zakresie odpowiednich kryteriów progowych (np. materiały przedstawiające niegodziwe traktowanie dzieci w celach seksualnych);
2) istnieje powszechna zgoda co do tego, że treść/zachowanie jest niezgodne z prawem, ALE istnieją znaczne różnice krajowe w kryteriach określających niezgodność z prawem (przykład: zniesławienie);
3) treść/zachowanie NIE JEST powszechnie uważane za nielegalne, ALE stosowanie określonych przepisów krajowych na terytorium lokalnym jest uważane za dopuszczalne przez inne kraje, w szczególności ze względów historycznych (przykład: kryminalizacja negowania Holokaustu);
4) treść/zachowanie NIE JEST powszechnie uważane za niewłaściwe, a niektóre kraje uważają nawet, że nie powinno się zezwalać na delegalizację (przykład: przepisy dyskryminujące lub kryminalizujące określoną orientację seksualną)[100].

Granice między kategoriami wypowiedzi nie są jednak sztywne. Toczą się debaty na temat tego, w jakich obszarach mieszczą się poszczególne rodzaje treści. Brak zgody, w ujęciu globalnym, co do sposobu i zakresu, a także celu uznawania niektórych treści za nielegalne nie sprzyja harmonizacji prawa. Przeciwnie, próba przełamania krajowych lub regionalnych standardów wolności wypowiedzi przez narzucenie regulacji rozbieżnych z tymi, jakie były objęte społecznym konsensusem, może powodować niestabilność systemu i prowadzić, w skrajnych wypadkach, do anarchii. O ile istnieje porozumienie państw i organizacji międzynarodowych w odniesieniu do potrzeby identyfikowania nielegalnych treści oraz zgoda co do ogólnych przesłanek ich bezprawności, o tyle – co wydaje się zrozumiałe i rozsądne – nie ma zgody ani na dokonanie ich jednolitej kwalifikacji, ani na zastosowanie wspólnych rozwiązań dopuszczających stosowanie sankcji, w tym blokowanie lub ograniczanie wolności wypowiedzi w internecie.

W obszarze państw-stron Traktatów Europejskich oraz państw-stron EKPC założono nie tylko istnienie możliwości, ale uznano za niezbędne przyjęcie wspólnych dla całego obszaru

[98] Content & Jurisdiction Program..., s. 8.
[99] Content & Jurisdiction Program..., s. 26.
[100] Content & Jurisdiction Program..., s. 26.

UE i RE definicji terminu „nielegalne treści" oraz wspólnych mechanizmów ich zwalczania w internecie. Komisja i Parlament Europejski zdecydowały się na przyjęcie metody pełnej harmonizacji w dziedzinie usług pośrednictwa internetowego. Komisja Europejska uznała, że aby uniknąć fragmentacji prawnej, konieczne jest przyjęcie aktu prawnego rangi rozporządzenia[101]. 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 Unii[102].

Jako podstawę prawną tej decyzji wskazano art. 114 TFUE[103], który przewiduje ustanowienie środków mających na celu zapewnienie funkcjonowania rynku wewnętrznego[104]. W uzasadnieniu przyjętej metody regulacyjnej wskazano, że służy ona zapewnieniu prawidłowego funkcjonowania rynku wewnętrznego, zwłaszcza 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, 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 przejrzystość"[105]. Pozostawienie możliwości regulowania działalności pośredników internetowych państwom członkowskim oceniono, wskazując, że „działania legislacyjne na szczeblu krajowym [...] utrudniają świadczenie i odbiór usług na terytorium całej Unii i są nieskuteczne"[106]. 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

[101] Wniosek z 15 grudnia 2020 r. Rozporządzenie Parlamentu Europejskiego i Rady w sprawie jednolitego rynku usług cyfrowych (akt o usługach cyfrowych) i zmieniające dyrektywę 2000/31/WE (Tekst mający znaczenie dla EOG) {SEC(2020) 432 final} - {SWD(2020) 348 final} - {SWD(2020) 349 final}, s. 3, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52020PC0825 (dostęp: 20 czerwca 2024 r.) – dalej wniosek KE z 15 grudnia 2020 r.

[102] Wniosek KE z 15 grudnia 2020 r, s. 7.

[103] Wersja skonsolidowana Dz.Urz. UE C 202 z 2016 r., s. 47.

[104] 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".

[105] Wniosek KE z 15 grudnia 2020 r., s. 6.

[106] Wniosek KE z 15 grudnia 2020 r., s. 7.

i konsumentów na całym rynku wewnętrznym. Jest to konieczne do zapewnienia pewności prawa i przejrzystości"[107].

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 TFUE 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 nie mogą, działając samodzielnie, osiągnąć celu, jakim jest zapewnienie wszystkim przedsiębiorstwom kontestowalnych i uczciwych rynków w sektorze cyfrowym w całej Unii[108]. 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 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 rozwiązania zidentyfikowanych problemów dotyczących uczciwości i kontestowalności oraz przeciwdziałania fragmentacji jednolitego rynku podstawowych usług platformowych świadczonych lub oferowanych przez strażników dostępu[109].

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 harmonizacją[110].

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 rozpowszechniania 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) oraz mechanizmu zgłaszania i działania (art. 16 AUC), a także 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).

[107] Wniosek KE z 15 grudnia 2020 r., s. 8.
[108] Wniosek KE z 15 grudnia 2020 r., s. 6.
[109] Wniosek KE z 15 grudnia 2020 r., s. 8.
[110] P. Polański, *Europejskie*..., s. 248.

W motywie 153 AUC ustawodawca europejski deklaruje, że AUC nie narusza praw podstawowych uznanych w Karcie 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 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.

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 jednak z całą pewnością orzec, że ze względu na specyfikę działania internetu i szczególny sposób aktywności oraz zapewniania widoczności w internecie oraz wyższą – jak się wydaje – wrażliwość na ingerencje, wypracowany poza internetem standard wolności wypowiedzi będzie do utrzymania także w internecie.

3.2. Przesłanki ingerencji – redefinicja standardu

Aktywność państw i organizacji międzynarodowych zmierzająca do ustalenia wspólnych standardów reagowania na rozpowszechniane w internecie treści była podejmowana w ramach szerszego pakietu inicjatyw obejmujących zarządzanie internetem, w szczególności politykę zarządzania danymi[111]; zarządzanie zawartością internetu (Content & Jurisdiction Policy Options[112]) oraz politykę rejestrowania domen i dostęp do internetu[113]. W odniesieniu do zarządzania treścią w internecie zauważono potrzebę zagwarantowania wolności wypowiedzi nie tylko na płaszczyźnie materialnoprawnej, w szczególności w zakresie oceny dopuszczalności rozpowszechniania niektórych rodzajów treści, w tym kontrowersyjnych ze względu na ich formę lub wymowę, ale także na płaszczyźnie proceduralnej, wskazując na wymóg zapewnienie tzw. sprawiedliwości proceduralnej[114].

---

[111] Data & Jurisdiction Program: Operational Approaches, Norms, Criteria, Mechanisms, April 2019, https://www.internetjurisdiction.net/uploads/pdfs/Papers/Data-Jurisdiction-Program-Operational-Approaches.pdf (dostęp: 20 czerwca 2024 r.).

[112] Content & Jurisdiction Policy Options: Cross-Border Content Restrictions, s. 5, https://www.internetjurisdiction.net/uploads/pdfs/Papers/Content-Jurisdiction-Policy-Options-Document.pdf (dostęp: 20 czerwca 2024 r.).

[113] Domains & Jurisdiction Program: Operational Approaches, Norms, Criteria, Mechanisms, April 2019, https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Operational-Approaches.pdf (dostęp: 20 czerwca 2024 r.).

[114] Dan Jerker B. Svantesson, *Internet & Jurisdiction Global Status Report 2019*, s. 7, https://www.internetjurisdiction.net/uploads/pdfs/GSR2019/Internet-Jurisdiction-Global-Status-Report-2019_web.pdf (dostęp: 20 czerwca 2024 r.).

Zauważono zatem potrzebę zagwarantowania przejrzystości samego procesu ograniczania wolności wypowiedzi przez jasne kryteria służące wyodrębnieniu kręgu podmiotów i wyposażeniu ich w kompetencje do nakładania ograniczeń, a także ustalenia katalogu dopuszczalnych rodzajów ograniczeń. Szczególnie istotne znaczenie przywiązano do mechanizmów odwoławczych, w tym procedury służącej zakwestionowaniu nałożonych ograniczeń i zapewnieniu skutecznych środków zaskarżania. O ile zatem ustalenie ram klasycznego standardu wolności wypowiedzi realizowanego poza internetem nie wymagało, co do zasady, zapewnienia szczególnych gwarancji „sprawiedliwości proceduralnej", ta była bowiem, jak zasadnie przyjmowano, rezultatem stosowania przepisów prawa formalnego w toku postępowań przed organami wymiaru sprawiedliwości, o tyle wobec przyjęcia ogólnego założenia o dopuszczalności, a nawet potrzebie ingerowania w wolność wypowiedzi przez dostawców usług cyfrowych konieczne stało się przeniesienie uwagi na przejrzystość czynności, w tym ich rodzaj, kolejność i skutki.

Na poziomie zasadniczym utrzymano zatem zasadę, zgodnie z którą każde ograniczenie wolności wypowiedzi przez państwo musi m.in. być dopuszczone przez jasne i przewidywalne prawo, spełniać kryteria konieczności i proporcjonalności"[115]. Równolegle podkreślono, że decyzja o ograniczeniu wolności wypowiedzi powinna być podejmowana przy zachowaniu „wystarczających gwarancji sprawiedliwości proceduralnej"[116], co stanowi, jak zauważono, „złożone wyzwanie na poziomie ponadnarodowym ze względu na brak jasno uzgodnionych ram merytorycznych i proceduralnych"[117]. Przyjęto w konsekwencji, że: „Konieczność i proporcjonalność to kluczowe uzgodnione zasady mające zastosowanie do decyzji o ograniczeniu treści. W tym względzie kwestia zasięgu geograficznego takich ograniczeń stała się kwestią sporną, a kolejnym wyzwaniem stała się szara strefa czysto kontrowersyjnych treści"[118].

Gwarancje proceduralne, których celem jest zapewnienie „sprawiedliwości proceduralnej" osobom, których swoboda wypowiedzi została ograniczona w internecie, powinny przewidywać istnienie co najmniej:

1) formatów (wytycznych pomocnych przy podejmowaniu decyzji o ograniczeniu);
2) świadomości i wiedzy użytkowników odnośnie do kryteriów wprowadzania ograniczenia wolności wypowiedzi;
3) intuicyjnych kanałów zgłaszania naruszeń;
4) starannego połączenia automatycznego wykrywania i weryfikacji przez człowieka umożliwiających szybkie podejmowanie działań przy pełnym uwzględnieniu kontekstu w celu zmniejszenia ryzyka nadmiernego ograniczenia;

---

[115] Dan Jerker B. Svantesson, *Internet*..., s. 75.
[116] Dan Jerker B. Svantesson, *Internet*..., s. 75.
[117] Zob. Dan Jerker B. Svantesson, *Internet*..., s. 49.
[118] Dan Jerker B. Svantesson, *Internet*..., s. 8.

5) prawa do notyfikacji, tj. wyprzedzającego powiadomienia użytkownika o zamiarze zablokowania jego treści;
6) kryteriów uznawania za „szczególne", „nadzwyczajne" okoliczności uzasadniające wprowadzenie ograniczenia;
7) dostępnych, szybkich, jasno udokumentowanych i powszechnych mechanizmów odwoławczych[119].

3.3. Rodzaje nielegalnych treści

Termin „nielegalne treści" jest terminem prawnym zdefiniowanym 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 prawa". Sformułowana w tym przepisie definicja stanowi źródło zasady, zgodnie z którą należy odmówić udzielenia ochrony wypowiedziom sklasyfikowanym jako nielegalne. Zasada ta odzwierciedla zarazem stanowisko ETPC i TSUE wypowiadane na gruncie art. 17 EKPC i art. 53 KPP, kiedy to trybunały odmawiały przyjęcia do rozpoznania skarg na naruszenie wolności wypowiedzi, wskazując na sprzeczność pomiędzy żądaniem oczekiwanej ochrony a konwencyjnymi wartościami, a w konsekwencji uznając je za niedopuszczalne (mechanizm gilotyny)[120]. Zawarta w rozporządzeniach cyfrowych (AUC i ARC) definicja nielegalnych treści i ustanowiony w nich mechanizm ochrony użytkowników internetu (usługobiorców) przed nielegalnymi treściami przesądza o zmianie modelu wolności wypowiedzi w szczególności w ten sposób, że powierza wdrożenie zawartych tam rozwiązań podmiotom prywatnym, legitymizując je w wykonywaniu funkcji państwa[121]. Ustawodawca

[119] Content & Jurisdiction Program..., s. 17.

[120] Terminu tego używa I.C. Kamiński, wskazując, że Trybunał, powołując się na art. 17 EKPC, uruchamia mechanizm gilotyny i wyłącza 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 przepisów (zob. I.C. Kamiński, *Pojęcie*..., s. 89).

[121] Uczeni tacy jak Ost, van de Kerchove (zob. F. Ost, M. van de Kerchove. *De la pyramide au réseau? Pour une théorie dialectique du droit*, Facultés universitaires Saint-Louis Bruxelles, 2002) I E. Weitzenboeck (E. Weitzenboeck,. *Hybrid net: the regulatory framework of ICANN and the DNS*, „International Journal of Law and Information Technology" 2014, nr 22(1), s. 49) podkreślali, że piramidalny model regulacji – charakteryzujący się centralną rolą państwa jako regulatora – został poważnie podważony przez rozwój technologii informacyjnej, globalizację, współzależność gospodarczą. Jak podkreślono – powołując się na wskazanych autorów – „regulacja sieci" lub „regulacja sieciowa" zastąpiła model regulacji ukształtowany na zasadzie piramidy. Państwo przestaje być jedynym źródłem suwerenności (konieczność dzielenia się nią nie tylko z władzami superpaństwowymi, ale także z potężnymi podmiotami prywatnymi); wola ustawodawcy przestaje być przyjmowana jako dogmat (jest akceptowana tylko pod pewnymi warunkami, po złożonym procesie oceny, zarówno wcześniejszej (*ex ante*), jak i późniejszej (*a posteriori*) (zob. Dan Jerker B. Svantesson, *Internet*..., s. 49). Sprawiedliwość, która – jak

europejski nie tylko odmawia ochrony nielegalnym treściom, ale ponadto przyjmuje, że należy przeciwdziałać nielegalnym treściom, a w razie ich rozpowszechnienia konieczne jest ich usuwanie przy założeniu, że co do zasady szkodzą debacie publicznej.

Zasadnicza linia podziału kategorii wypowiedzi jest wytyczana ze względu na zastosowanie kryterium legalności. 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 niejednolity charakter tych wypowiedzi, zmienność kontekstów oraz ich wielowymiarowość, a nawet intuicyjność, znajdują się one na granicy tego, co objęte ochroną i tego, co jest zabronione. Zakwalifikowanie wypowiedzi do kategorii nielegalnych treści uruchamia reakcję silnie ingerującą w wolność wypowiedzi, pozbawiając autora możliwości powoływania się na prawo do realizacji swobody wypowiedzi, a w konsekwencji blokując dalsze rozpowszechnianie „nielegalnej" wypowiedzi.

Rozróżnienie kategorii wypowiedzi przy pomocy przesłanek pozytywnych poprzez zaliczenie wypowiedzi do określonych kategorii (polityczne, komercyjne, reklamowe, prasowe[122]) okazało się w odniesieniu do internetu nieefektywne i mało przydatne. Praktycznego znaczenia, ze względu na specyfikę komunikowania w internecie, charakteryzującego się natychmiastowością, skalowalnością[123], interaktywnością i globalnością, nabrały przesłanki negatywne służące identyfikowaniu niedozwolonych zachowań komunikacyjnych. W klasycznym standardzie akcentowano aspekt pozytywny wolności wypowiedzi (prawo do), a w konsekwencji potrzebę restrykcyjnego ustalania „granicy dopuszczalnych ograniczeń" zgodnie z koncepcją, w myśl której zasadą jest wolność, a ograniczenie stanowi wyjątek od

---

zauważono – w modelu piramidalnym była ujmowana jako gwarant hierarchii wartości, została zastąpiona grą interesów i próbami równoważenia wartości, które są zarówno różne w zależności od systemu prawa, jak i zmienne ze względu na naturalną prawidłowość, jaką cechują się społeczeństwa. Podkreśla się zatem, że zmiana paradygmatu jest w toku, jednak nie są możliwe do przewidzenia jej konsekwencje ani zakres (Dan Jerker B. Svantesson, *Internet*..., s. 51).

[122] I.C. Kamiński, *Ograniczenia swobody wypowiedzi dopuszczalne w Europejskiej Konwencji Praw Człowieka. Analiza krytyczna*, Warszawa 2010, s. 92 i n.

[123] W raporcie Content & Jurisdiction Program, Operational Approaches Norms, Criteria and Mechanisms pojęcie to jest użyte w kontekście różnorodności organizacji oraz, ze względu na ich siłę oddziaływania, intensywności i dotkliwości zarówno rozpowszechnienia nielegalnych treści, jak i ewentualnego ograniczania wypowiedzi. Skalowalność jest także ujmowana jako jedno z kryteriów operacyjnych, jakimi – jak postuluje się w tym opracowaniu – podmioty zaangażowane w zarządzenie internetem powinny się posługiwać przy opracowaniu i wdrażaniu rozwiązań dotyczących eliminowania nielegalnych treści. Oprócz „skalowalności", jako jednego z kryteriów, wskazano ponadto: przejrzystość procedur służących ustalaniu rodzajów treści, w odniesieniu do których składane są wnioski o ograniczenia, oraz normatywna podstawa tych wniosków; wykrywanie, w tym rozróżnienie między zgłoszeniami dokonywanymi przez osoby trzecie a wykrywaniem przez dostawców; proporcjonalne działania, w tym elementy dotyczące terminowości, oceny, ograniczeń proporcjonalnych pod względem geograficznym i typologii działań.

tej zasady. W przypadku internetu nacisk został położony na detekcję nadużyć wolności wypowiedzi. Perspektywa ta jest widoczna w dokumentach dotyczących zarządzania internetem i budowania jednolitego rynku cyfrowego. Organizacje międzynarodowe, tj. zarówno UE, jak i Rada Europy, a także ONZ, podkreślając potrzebę budowania zaufania do internetu, uzależniały osiągnięcie tego celu od wyeliminowania nielegalnych treści. Taka perspektywa stworzyła potrzebę definiowania, typizowania i katalogowania nielegalnych treści. Rozgraniczenie aktów komunikacyjnych ma zatem charakter dychotomiczny i musi uwzględniać linię podziału oddzielającą to, co legalne od tego, co jest nielegalne.

Kluczowe znaczenie dla ustalenia standardu wolności wypowiedzi ma zatem wstępne rozstrzygnięcie[124] przybierające postać swoistego przedsądu. Dopiero bowiem zakwalifikowanie wypowiedzi do kategorii legalnych pozwala na stosowanie wypracowanych na gruncie orzecznictwa ETPC i TSUE zasad oceny. Klasyczny standard wolności wypowiedzi, z całym arsenałem reguł i mechanizmów oceny dopuszczalności ograniczenia wolności wypowiedzi przy zastosowaniu „trójstopniowego testu szkodliwości", jest bowiem odnoszony wyłącznie do tych wypowiedzi, które w ramach przedsądu nie zostały odrzucone jako nielegalne.

Na gruncie UE i RE odwołano się do klauzul generalnych (odpowiednio art. 54 KPP i art. 17 EKPC) zakazujących udzielania ochrony tym aktom, które zmierzają do obejścia przepisów Konwencji lub Karty w celu osiągnięcia skutku stojącego w sprzeczności z konwencyjnymi wartościami. Równolegle sygnalizowana jest potrzeba poszerzenia katalogu europrzestępstw, uzasadniana koniecznością przeciwdziałania przemocy, w tym różnorodnym formom dyskryminacji, a także cyberprzemocy, w szczególności przemocy wobec dzieci i kobiet[125].

Zmiana katalogu europrzestępstw miałaby nastąpić poprzez poszerzenie dziedzin przestępczości wskazanych w art. 83 ust. 1 TFUE i objęcie nim „mowy nienawiści" i „przestępstw z nienawiści"[126]. Realizacja tego postulatu oznaczałaby umożliwienie instytucjom UE wydawanie aktów prawnych ustanawiających normy minimalne odnoszące się do określania znamion typów i kategorii przestępstw z nienawiści i mowy nienawiści, a w konsekwencji dokonywania 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

[124] Na tę okoliczność zwraca uwagę I.C. Kamiński; zob. I.C. Kamiński, *Mowa…*, s. 109.

[125] Wniosek Komisji Europejskiej z 8 marca 2022 r. Dyrektywa PE i Rady w sprawie zwalczania przemocy wobec kobiet i przemocy domowej COM(2022) 105 final, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52022PC0105&from=PL (dostęp: 20 czerwca 2024 r.).

[126] Opinia Europejskiego Komitetu Ekonomiczno-Społecznego z 18 maja 2022 r. „Komunikat Komisji do Parlamentu Europejskiego i Rady «Bardziej inkluzywna i bezpieczna Europa: rozszerzenie wykazu przestępstw UE o nawoływanie do nienawiści i przestępstwa z nienawiści»" (2022/C 323/14), https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:52021DC0777 (dostęp: 20 czerwca 2024 r.), a także: komunikat prasowy Komisji Europejskiej z 19 stycznia 2018 r.: *Zwalczanie nielegalnej mowy nienawiści w internecie – inicjatywa Komisji przynosi stałą poprawę sytuacji, kolejne platformy przystępują do inicjatywy*, https://ec.europa.eu/commission/presscorner/detail/pl/IP_18_261 (dostęp: 20 czerwca 2024 r.).

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 ustalanie granic swobody wypowiedzi[127].

Próba poszerzenia katalogu europrzestępstw stanowi zarazem wtórny skutek realizowanej na gruncie rozporządzeń cyfrowych koncepcji dychotomicznego podziału wypowiedzi na legalne i nielegalne. Skoro istnieją wypowiedzi nielegalne, to – jak się wydaje – konieczne jest ich skatalogowanie, w szczególności wówczas, gdy sankcją za rozpowszechnienie nielegalnej wypowiedzi miałoby być nie tylko jej wyeliminowanie z obiegu publicznego, ale miałoby zostać powiązane z wymierzeniem innej kary lub zastosowaniem środka karnego[128]. Propozycje katalogowania nielegalnych treści poprzez ustalenie i nazwanie rodzajów aktywności komunikacyjnych niemieszczących się w standardzie wolności wypowiedzi zawierają dokumenty opracowywane na szerszym niż UE forum współpracy państw i organizacji międzynarodowych[129]. Rezultatem tego podejścia było wyodrębnienie i opisanie deliktów komunikacyjnych charakterystycznych dla internetu, tj. takich, których popełnie-

[127] Komisja Europejska postuluje poszerzenie dziedzin przestępczości wymienionych w art. 83 ust. 1 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, nawoływanie do nienawiści i przestępstwa z nienawiści można uznać za «dziedzinę przestępczości» w rozumieniu art. 83 ust. 1 TFUE" (Komunikat Komisji do Parlamentu Europejskiego i Rady z 9 grudnia 2021 r., Bardziej inkluzywna i bezpieczna Europa: rozszerzenie wykazu przestępstw UE o nawoływanie do nienawiści i przestępstwa z nienawiści, COM(2021) 777 final, pkt 3.1., https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52021DC0777&from=IT, dostęp: 20 czerwca 2024 r.).

[128] W systemach prawnych państw istnieją różnice w sposobie definiowania i dokonywania oceny wypowiedzi uznawanych za mowę nienawiści. O ile w niektórych państwach tę samą wypowiedź będzie można zaklasyfikować jako mowę nienawiści, o tyle w innych przypadkach może być ona zaklasyfikowana jako dopuszczalna. W szczególności dokonano porównania sposobu, w jaki USA i Niemcy traktują mowę nienawiści. Specjalny Raport ONZ ds. Wolności Słowa wskazał na trzy różne rodzaje wypowiedzi: 1) wypowiedzi, które stanowią przestępstwo w świetle prawa międzynarodowego i mogą być ścigane karnie; 2) wyrażenie, które nie jest, ale może uzasadniać ograniczenie i pozew cywilny; oraz 3) wypowiedzi, które nie powodują sankcji karnych lub cywilnych, ale nadal budzą obawy w zakresie tolerancji (zob. Roczne sprawozdanie Specjalnego Sprawozdawcy Organizacji Narodów Zjednoczonych ds. Promocji i Ochrony Prawa do Wolności Opinii i Wypowiedzi dla Zgromadzenia Ogólnego. (2012). A/67/357, pkt 2; https://undocs.org/en/A/67/357, dostęp: 20 czerwca 2024 r.).

[129] W dokumentach opracowanych przez Internet & Jurisdiction Policy Network, która przedstawia się jako organizacja wspierana, a zarazem angażująca w proces polityczny dotyczący zarządzania internetem 400 kluczowych podmiotów, tj. zarówno organizacji takich jak ONZ, UE, UNESCO, Rada Europy, jak i poszczególnych państw (USA, Chiny, Niemcy, Estonia), a także największych światowych firm internetowych, operatorów technicznych, grup społeczeństwa obywatelskiego, środowisk akademickich i organizacji międzynarodowych z ponad 70 krajów, wskazano na potrzebę podejścia do regulowania internetu wymagającego – jak to określono – „pewnej ręki i beznamiętnego umysłu" – zob. Dan Jerker B. Svantesson, *Internet*..., s. 51.

nie, ze względu na zasięg i intensywność oddziaływania oraz interaktywność komunikacji jest możliwe z wykorzystaniem internetu. W efekcie, ustalenie, że konkretna wypowiedź ze względu na jej treść lub sposób rozpowszechnienia jest nielegalna, może skutkować nie tylko jej wyeliminowaniem (usunięciem) z internetu, ale stanowi podstawę do uruchomienia przeciwko autorowi lub dystrybutorowi takiej wypowiedzi postępowania karnego. Poniżej opisane kategorie wypowiedzi należą do sugerowanego w dokumentach nienormatywnych katalogu nielegalnych treści. Nie ma bowiem ani na płaszczyźnie prawa europejskiego, ani prawa ponadnarodowego z innych obszarów terytorialnych niż Europa, trwałego, uzgodnionego co do metodyki i kryteriów, wzorca klasyfikowania treści ze względu na ich nielegalny charakter.

3.3.1. Ochrona praw dzieci

Zważywszy na treść postanowień Konwencji o ochronie praw dziecka[130], a także art. 17 i 24 MPPOiP proponuje się objąć terminem nielegalnych treści materiały naruszające dobro małoletnich, w szczególności adresowane do dzieci, jeśli mogą negatywnie oddziaływać na ich rozwój psychofizyczny, a także adresowane do osób pełnoletnich, jeśli ze względu na ich zawartość lub formę wykorzystują małoletnich. Artykuł 24 ust. 1 MPPOiP stanowi, że: „Każde dziecko, bez żadnej dyskryminacji ze względu na rasę, kolor skóry, płeć, język, religię, pochodzenie narodowe lub społeczne, sytuację majątkową lub urodzenie, ma prawo do środków ochrony, jakich wymaga status małoletniego, ze strony rodziny, społeczeństwa i Państwa". Deklaracja praw dziecka stwierdza w preambule, że „dziecko, z powodu niedojrzałości fizycznej i umysłowej wymaga szczególnej opieki i troski"[131]. Konwencja o prawach dziecka definiuje dzieci jako osoby poniżej 18. roku życia (art. 1 Konwencji), a w art. 17 Konwencji zobowiązano państwa-strony, by „zachęcały środki masowego przekazu do rozpowszechniania informacji i materiałów, korzystnych dla dziecka w wymiarze społecznym oraz kulturalnym, zgodnie z duchem artykułu 29" (lit. a) oraz „zachęcały do rozwijania odpowiednich kierunków działalności dla ochrony dzieci przed informacjami i materiałami szkodliwymi z punktu widzenia ich dobra, mając na względzie postanowienia artykułów 13 i 18" (lit. e). Przy czym zgodnie z art. 29 ust. 1 lit. a Konwencji jej państwa-strony zobowiązały się do „rozwijania w jak najpełniejszym zakresie osobowości, talentów oraz zdolności umysłowych i fizycznych dziecka", a na podstawie art. 13 do zapewnienia, by dziecko „miało prawo do swobodnej wypowiedzi; prawo to ma zawierać swobodę poszukiwania, otrzymywania i przekazywania informacji oraz idei wszelkiego rodzaju, bez względu na granice, w formie ustnej, pisemnej bądź za po-

[130] Konwencja o prawach dziecka przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 20 listopada 1989 r. (Dz.U. z 1991 r. Nr 120, poz. 526 ze zm.).

[131] Deklaracja Praw Dziecka uchwalona przez Zgromadzenie Ogólne ONZ w dniu 20 listopada 1959 r., http://libr.sejm.gov.pl/tek01/txt/onz/1959.html (dostęp: 20 czerwca 2024 r.).

mocą druku, w formie artystycznej lub z wykorzystaniem każdego innego środka przekazu według wyboru dziecka". Natomiast zgodnie z art. 18 Konwencji: „Państwa-Strony podejmą wszelkie możliwe starania dla pełnego uznania zasady, że oboje rodzice ponoszą wspólną odpowiedzialność za wychowanie i rozwój dziecka". Także w art. 25 Powszechnej Deklaracja Praw Człowieka[132] wskazano, że dzieciństwo ma prawo do szczególnej opieki i pomocy.

W rozporządzeniu o usługach cyfrowych (AUC) w wielu miejscach wskazano, że przez treści nielegalne należy rozumieć treści szkodliwe dla małoletnich, w tym np. udostępnianie obrazów przedstawiających niegodziwe traktowanie dzieci w celach seksualnych (motyw 12). Ochrona małoletnich jest ważnym celem polityki Unii. W myśl motywu 71 AUC: „Platformę internetową można uznać za dostępną dla małoletnich, jeżeli warunki korzystania z jej usług umożliwiają małoletnim korzystanie z usługi, gdy jej usługa jest skierowana do małoletnich lub korzystają z niej w przeważającej mierze małoletni, lub gdy dostawca w inny sposób ma świadomość, że niektórzy odbiorcy jego usługi są małoletni, na przykład dlatego, że w innych celach przetwarza już dane osobowe odbiorców usługi ujawniające ich wiek. Dostawcy platform internetowych, z których korzystają małoletni, powinni wprowadzić odpowiednie i proporcjonalne środki w celu ochrony małoletnich, na przykład poprzez domyślne, w stosownych przypadkach, projektowanie swoich interfejsów internetowych lub ich części z zachowaniem najwyższego poziomu prywatności, bezpieczeństwa i ochrony małoletnich, a także poprzez przyjmowanie norm ochrony małoletnich lub stosowanie kodeksów postępowania służących ochronie małoletnich. Powinni oni uwzględniać najlepsze praktyki i dostępne wytyczne, takie jak te zawarte w komunikacie Komisji pt. „Cyfrowa dekada dla dzieci i młodzieży: nowa europejska strategia na rzecz lepszego internetu dla dzieci" (BIK+)". Dostawcy platform internetowych nie powinni prezentować reklam opartych na profilowaniu z wykorzystaniem danych osobowych odbiorcy usługi, jeżeli wiedzą z wystarczającą pewnością, że odbiorca usługi jest małoletni".

Ustawodawca europejski wymaga od dostawców usług, by dokonywali szacowania i oceny ryzyka systemowego wówczas, gdy istnieje prawdopodobieństwo rozpowszechniania materiałów przedstawiających niegodziwe traktowanie dzieci w celach seksualnych (motyw 80 AUC), a także wówczas, gdy małoletni, realizując prawo do swobody pozyskiwania informacji, mógłby zetknąć się z treściami zagrażającymi lub naruszającymi jego dobro. Wskazano zatem, że: „Przy ocenie rodzajów ryzyka w odniesieniu do praw dziecka dostawcy bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych powinni przeanalizować na przykład, w jakim stopniu projekt i funkcjonowanie danej usługi są łatwo zrozumiałe dla małoletnich, a także w jaki sposób – poprzez świadczoną przez nich usługę – małoletni mogą zetknąć się z treściami, które mogą mieć szkodliwy wpływ na ich zdrowie oraz rozwój

[132] Powszechna Deklaracja Praw Człowieka z 10 grudnia 1948 r., https://libr.sejm.gov.pl/tek01/txt/onz/1948.html (dostęp: 20 czerwca 2024 r.).

fizyczny, psychiczny i moralny. Takie ryzyko może powstać na przykład w związku z projektem interfejsów internetowych, które umyślnie lub nieumyślnie wykorzystują słabe strony i niedoświadczenie małoletnich lub które mogą powodować zachowania nałogowe" (motyw 81 AUC). Ponadto dostawcy bardzo dużych platform internetowych zostali zobowiązani do wdrożenia środków zmniejszających ryzyko, w tym do „podejmowania ukierunkowanych działań w celu ochrony praw dziecka, w tym stosowania narzędzi weryfikacji wieku i kontroli rodzicielskiej, narzędzi mających na celu pomaganie małoletnim sygnalizować niegodziwe traktowanie lub, w stosownych przypadkach, uzyskanie wsparcia" (art. 35 ust. 1 lit, j AUC).

Treści nielegalne w obszarze ochrony praw dziecka będą zatem obejmować w szczególności „materiały przedstawiające wykorzystywanie dzieci lub cokolwiek niewłaściwego z udziałem nieletnich"[133], przez co należy rozumieć: „Treści zawierające materiały o charakterze seksualnym lub z podtekstem seksualnym z udziałem nieletnich, materiały wizualne przedstawiające wykorzystywanie dzieci lub inne treści publikowane z zamiarem wyrządzenia krzywdy i wykorzystania ich wobec dzieci. Może to obejmować prawa do prywatności zdjęć dzieci poniżej 13 roku życia i do 18 roku życia w zależności od jurysdykcji i kontekstu"[134]. Nielegalne jest także rozpowszechnianie materiałów, które mają na celu albo ze względu na swoją treść lub formę mogą wskazywać na „uwodzenie małoletnich"[135]. Uwodzenie online ma miejsce, gdy dana osoba korzysta z mediów społecznościowych, aby celowo pielęgnować emocjonalną więź z dzieckiem w celach seksualnych lub wykorzystywania seksualnego tego dziecka[136].

3.3.2. Ochrona prywatności (prawo do tożsamości) i mowa nienawiści

W ujęciu zaproponowanym przez ETPC i TSUE istnieje bezpośredni związek między ochroną prywatności a sankcjonowaniem treści nielegalnych, w tym mowy nienawiści. Mowa nienawiści jest identyfikowana w orzecznictwie jako bezprawna ingerencja w sferę prywatności, a w szczególności jako naruszenie jednego z aspektów prywatności, tj. prawa do poczucia własnej tożsamości (odrębności). Jest ono odnoszone do stanów świadomości jednostki, która – jak wynika z orzecznictwa ETPC i TSUE – ma prawo do identyfikowania się z grupami mniejszościowymi wyróżnionymi ze względu na płeć, orientację seksualną, rasę lub wyznanie. Okoliczność, że grupy te mają charakter mniejszości, w ocenie trybunałów generuje obowiązek państwa do zapewnienia jednostce niezakłóconego przeżywania jej tożsamości płciowej, religijnej lub rasowej. Obowiązek państwa będzie zatem polegać na zapewnieniu

[133] Content & Jurisdiction Program..., s. 20.
[134] Content & Jurisdiction Program..., s. 20.
[135] W dokumentach organizacji Internet&Juridiction operuje się terminami *„grooming"* lub *„predation"* (Content & Jurisdiction Program..., s. 20).
[136] Content & Jurisdiction Program..., s. 20.

sprawiedliwej równowagi pomiędzy prawem jednostki do odrębności (tożsamości) a prawami i wolnościami ogólnospołecznymi.

Nie ma uzgodnionych na szczeblu międzynarodowym definicji i progu mowy nienawiści. Jeśli nawet należałoby przyznać, że na płaszczyźnie ponadnarodowej wspólne jest stanowisko odnośnie do niedopuszczalności mowy nienawiści i potrzeby jej zwalczania, to jednak brak jest wspólnej koncepcji tego pojęcia, a w konsekwencji nie jest pewne, jakie przejawy aktywności komunikacyjnej (werbalnej i niewerbalnej) miałyby być zwalczane.

Europejski Trybunał Praw Człowieka uczynił znamieniem „mowy nienawiści" nie tyle intensywnie przeżywany przez autora wypowiedzi uzewnętrzniony afekt (nienawiść) wyrażający negatywny stosunek wobec osoby lub grupy społecznej ze względu na wyróżniającą je cechę (rasa, orientacja seksualna, wyznanie, religia), ale dwie inne przesłanki, tj. po pierwsze, związek występujący pomiędzy wypowiedzią a sferą życia prywatnego osoby, której wypowiedź dotyczy, w szczególności prawem tej osoby do niezakłóconego przeżywania poczucia przynależności (tożsamości, odrębności) do grupy mniejszościowej oraz, po drugie, wystąpienie prawdopodobieństwa naruszenia tzw. sprawiedliwej równowagi pomiędzy prawem mniejszości, z którą dana osoba się identyfikuje, a wolnością wypowiadania negatywnych, stygmatyzujących, ujawniających tożsamość tej osoby twierdzeń lub ocen.

Potrzeba zapewnienia ochrony prywatności jest powoływana w orzecznictwie ETPC i TSUE jako jedna z przesłanek materialnoprawnych uzasadniających ograniczenie wolności wypowiedzi. Ochronę prywatności zapewnia art. 8 EKPC oraz art. 7 KPP. Prywatność jest także objęta gwarancjami ochronnymi w innych aktach prawa międzynarodowego, co w szczególności znajduje potwierdzenie w treści art. 17 MPPOiP, który chroni prawo do poszanowania prywatności, rodziny, domu i korespondencji oraz ochrony czci i dobrego imienia. Zgodnie z tym przepisem: „1. Nikt nie może być narażony na samowolną lub bezprawną ingerencję w jego życie prywatne, rodzinne, dom czy korespondencję ani też na bezprawne zamachy na jego cześć i dobre imię. 2. Każdy ma prawo do ochrony prawnej przed tego rodzaju ingerencjami i zamachami". W myśl art. 7 KPP: „Każdy ma prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się". Zgodnie z art. 8 EKPC: „1. Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji. 2. 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".

Gwarancje ochrony prywatności zawarte we wskazanych aktach prawnych dotyczą nie tylko negatywnego aspektu ochrony prywatności polegającego na nieujawnianiu faktów z życia prywatnego, ale także aspektu pozytywnego nakazującego państwom ustanawianie i stosowanie

takich rozwiązań prawnych, które chronią prawa tożsamościowe jednostki[137]. Ochrona prawa do tożsamości wywodzona jest z prawa do autonomii osobistej jednostki[138].

Europejski Trybunał Praw Człowieka zauważa, że jakkolwiek podstawowym celem art. 8 EKPC jest ochrona jednostki przed arbitralnym działaniem ze strony władz krajowych, mogą jednak pojawić się także pozytywne obowiązki wpisane w skuteczne poszanowanie życia prywatnego lub rodzinnego. Te pozytywne obowiązki mogą obejmować przyjmowanie środków mających na celu zabezpieczenie poszanowania życia prywatnego nawet w sferze relacji zachodzących pomiędzy samymi osobami. Nadto, poszanowanie życia prywatnego wymaga, aby każda osoba mogła ustalić szczegóły swojej tożsamości jako indywidualnego człowieka[139]. Artykuł 8 Konwencji, jak podkreśla ETPC, chroni bowiem nie tylko życie „rodzinne", lecz również „prywatne", które obejmuje ważne aspekty tożsamości osobistej[140].

Wskazując na wymiar życia prywatnego jako dobra prawnie chronionego, Trybunał stwierdził, że wówczas, gdy sprawa dotyczy szczególnie ważnego aspektu egzystencji lub tożsamości osoby, państwo w minimalnym zakresie może korzystać z przysługującego mu marginesu uznania. W takim wypadku wzgląd na ochronę zapewnienia jednostce prawa do tożsamości osobistej przeważy nad potrzebą ochrony innych wartości i praw, albowiem tylko wówczas zapewniona zostanie „sprawiedliwa równowaga" pomiędzy prawem jednostki a interesem ogółu społeczeństwa[141]. Ograniczenia doznawać będzie w tym wypadku także swoboda wypowiedzi.

Za niedopuszczalne ETPC i TSUE uznawać będą w konsekwencji nie tylko rozpowszechnienie informacji ujawniających tożsamość, ale także szerzenie opinii, które ze względu na tożsamość jednostki stawiałyby ją w niekorzystnym świetle, narażały na etykietowanie lub napiętnowanie. Prawo do prywatności zagwarantowane w art. 7 KPP i art. 8 EKPC pozostaje bowiem w związku z ochroną przed dyskryminacją zagwarantowaną w art. 21 ust. 1 KPP[142].

---

[137] TSUE rozróżnia rodzaje tożsamości, tj. fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną (zob. wyrok TS z 6 października 2015 r., C-362/14, Maximillian Schrems przeciwko Data Protection Commissioner, ECLI:EU:C:2015:650). Wskazuje się ponadto na tożsamość płciową, odróżniając ją od orientacji seksualnej (wyrok TS z 25 stycznia 2018 r., C-473/16, F przeciwko Bevándorlási és Állampolgársági Hivatal, ECLI:EU:C:2018:36) i transseksualizmu (wyrok TS z 2 grudnia 2014 r., sprawy połączone C-148/13 do C-150/13, A i in. przeciwko Staatssecretaris van Veiligheid en Justitie, ECLI:EU:C:2014:2406).

[138] Wyrok TS z 2 grudnia 2014 r., sprawy połączone C-148/13 do C-150/13, A i in. przeciwko Staatssecretaris van Veiligheid en Justitie, pkt 15. W opinii rzecznika generalnego E. Sharpstona „orzecznictwo ETPC należy rozumieć w ten sposób, że ze względu na pojęcie osobistej autonomii, stanowiące ważną zasadę leżącą u podstaw interpretacji ochrony przyznanej przez art. 8 EKPC, jednostkom przysługuje prawo do określania własnej tożsamości, obejmujące także definiowanie własnej orientacji seksualnej" (opinia rzecznika generalnego przedstawiona 17 lipca 2014 r., sprawy połączone C-148/13 do C-150/13, A i in. przeciwko Staatssecretaris van Veiligheid en Justitie, ECLI:EU:C:2014:2111).

[139] Wyrok ETPC z 29 stycznia 2019 r., skarga nr 62257/15, Mifsud przeciwko Malcie, LEX nr 2611196.

[140] Decyzja ETPC z 15 września 2020 r., skarga nr 22963/16, Słoń przeciwko Polsce, LEX nr 3061542.

[141] Wyrok ETPC z 17 lutego 2022 r., skarga nr 74131/14, Y przeciwko Polsce, LEX nr 3306212.

[142] Opinia rzecznika generalnego przedstawiona 17 lipca 2014 r., sprawy połączone C-148/13 do C-150/13, A i in. przeciwko Staatssecretaris van Veiligheid en Justitie, pkt 38.

Powołanie się w debacie publicznej na aspekt tożsamości jednostki, o ile zostanie on powiązany z wyrażeniem oceny klasyfikującej postawę, zachowanie lub cechy tożsamościowe, a w konsekwencji przynależność do mniejszości rasowej, płciowej, wyznaniowej, stanowi nie tylko podstawę do potwierdzenia ochrony prywatności jednostki, ale ponadto uzasadnia – w ocenie ETPC i TSUE – potrzebę zachowania „sprawiedliwej równowagi pomiędzy konkurującymi interesami jednostki i społeczeństwa"[143].

Termin „mowa nienawiści" powiązano z gwarancją równej ochrony wolności i praw grup mniejszościowych. Mowa nienawiści w dokumentach przygotowanych na potrzeby organów UE, RE i ONZ obejmuje „poważne ataki na osoby ze względu na ich rasę, pochodzenie etniczne, narodowość, religię, tożsamość płciową, orientację seksualną, niepełnosprawność lub stan zdrowia. Może również obejmować kierowanie reklam do osób na podstawie wieku, wagi, statusu imigracyjnego. Przykładem może być agresywna lub dehumanizująca mowa, stwierdzenia o niższości lub wezwania do wykluczenia lub segregacji. Może to również obejmować obrazy, takie jak lincz, lub skoordynowane zachowania mające na celu dyskryminację lub dehumanizację, transmisje na żywo lub publikowanie zarchiwizowanych filmów z wydarzeń na żywo, które nagłaśniają lub podżegają do przestępstw z nienawiści"[144].

W dokumentach Rady Europy, jak zauważają J. Sobczak i K. Kakareko[145], po raz pierwszy zwrócono uwagę na potrzebę przeciwdziałania wypowiedziom motywowanym nienawiścią w rezolucji Komitetu Ministrów 68 (30) z 31 października 1968 r. w sprawie podjęcia środków prawnych zmierzających przeciwko wezwaniom do nienawiści ze względu na przynależność rasową, narodową i religijną. Rada Europy wezwała państwa-strony, aby przyjęły postanowienia Międzynarodowej konwencji w sprawie likwidacji wszelkich form dyskryminacji rasowej[146]. Niewiążącą definicję terminu „mowa nienawiści" zaproponowano w rekomendacji R 97(20) Komitetu Ministrów Rady Europy w sprawie „mowy nienawiści" (fr. *discours de haine*) z 30 października 1997 r.[147] Wskazując na zakres stosowania rekomendacji (fr. *champ d'aplication*), zdefiniowano w niej pojęcie mowy nienawiści jako: „każdą formą wypowiedzi, która rozpowszechnia, podżega, propaguje lub usprawiedliwia nienawiść rasową, ksenofobię, antysemityzm lub inne formy nienawiści oparte na nietolerancji, włączając w to nietolerancję wyrażaną w formie agresywnego nacjonalizmu lub etnocentryzmu, dyskryminacji lub wrogości wobec mniejszości, migrantów, lub osób wywodzących się ze

[143] Wyrok ETPC z 13 lipca 2021 r., skargi nr 40792/10, 30538/14 i 43439/14, Fedotova i inni przeciwko Rosji, LEX nr 3196562.

[144] *Content & Jurisdiction Program…*, s. 25.

[145] J. Sobczak, K. Kakareko, *Przeciwdziałanie mowie nienawiści w międzynarodowych aktach normatywnych* [w:] *Prawna kwalifikacji mowy nienawiści. Krajowe i europejskie uwarunkowania nadużycia wolności wypowiedzi*, red. J. Taczkowska-Olszewska, Warszawa 2024, s. 48.

[146] Międzynarodowa konwencja w sprawie likwidacji wszelkich form dyskryminacji rasowej otwarta do podpisu w Nowym Jorku dnia 7 marca 1966 r. (Dz.U. z 1969 r. Nr 25, poz. 187).

[147] Zob. https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168050116d (dostęp: 20 czerwca 2024 r.).

społeczności migrantów”[148]. Zauważa się, że wyróżnić można wiele form wypowiedzi, które mają charakter dyskryminacyjny, lecz które nie stanowią jednocześnie mowy nienawiści. Mimo że wypowiedzi takie mogą utrwalać lub pogłębiać uprzedzenia i krzywdzące stereotypy, nie zawierają znieważających, poniżających czy stygmatyzujących określeń, które kwalifikowałyby je jako mowę nienawiści[149].

W myśl art. 20 ust. 2 MPPOiP: „Popieranie w jakikolwiek sposób nienawiści narodowej, rasowej lub religijnej, stanowiące podżeganie do dyskryminacji, wrogości lub gwałtu, powinno być ustawowo zakazane”. Zauważono zarazem, że art. 20 MPPOiP stanowi znaczące ograniczenie nie tylko prawa do swobody wypowiedzi, gwarantowanego w art. 19 MPPOiP, lecz również innych praw i wolności przyznanych w tym akcie, w tym przede wszystkim wolności zgromadzeń oraz wolności zrzeszania się[150]. W art. 20 ust. 2 MPPOiP zaleca się, by popieranie nienawiści zostało zakazane w ustawie. Przesłanka zakazania w ustawie dotyczy zarazem „tylko takiego popierania nienawiści narodowej, rasowej lub religijnej, która stanowi jednocześnie nawoływanie do dyskryminacji, wrogości lub przemocy, również precyzuje zakres tej regulacji”[151].

W orzecznictwie ETPC 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 Konwencji”. Autor ten spostrzega, że „mowa nienawiści zaczęła funkcjonować jako jeden z koncepcyjnych fundamentów, służących do kreowania konwencyjnego standardu prawnego […]. Jest stawiana obok tak klasycznych i zakresowo szerokich konstruktów jak wypowiedź polityczna, wypowiedź w sprawach mających ogólne znaczenie, wypowiedź artystyczna i wypowiedź komercyjna”[152].

Trybunał strasburski upatruje swej roli w ustaleniu i ocenie, czy państwo zagwarantowało jednostce „sprawiedliwą równowagę” wówczas, gdy uszczerbku doznać może szczególny aspekt prywatności identyfikowany przez sędziów jako prawo do poczucia osobistej przynależności do mniejszościowej grupy społecznej wyodrębnionej ze względu na jej specyficzną cechę. W zbieżności ze stanowiskiem ETPC pozostaje wykładnia TSUE na gruncie art. 7 KPP[153].

---

[148] Aneks do rekomendacji nr R(97)20, preambuła, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168050116d (dostęp: 20 czerwca 2024 r.) (cyt. za J. Sobczak, K. Kakareko, *Przeciwdziałanie*…, s. 48).

[149] A. Gliszczyńska-Grabias [w:] *Międzynarodowy pakt praw obywatelskich (osobistych) i politycznych. Komentarz*, red. R. Wieruszewski, Warszawa 2012, art. 20, pkt 2.

[150] Zdecydowany sprzeciw USA wobec włączania do paktu zakazu propagandy wojennej znalazł odzwierciedlenie w treści zastrzeżenia, w którym USA stwierdziły, że „art. 20 nie wprowadza ani nie wymaga od USA przyjęcia regulacji prawnych czy podjęcia innych działań, które ograniczyłyby prawo do swobody wypowiedzi i stowarzyszania się, chronione przez Konstytucję i inne przepisy prawne USA” (cyt. za: A. Gliszczyńska-Grabias [w:] *Międzynarodowy*…, art. 20, pkt 2).

[151] A. Gliszczyńska-Grabias [w:] *Międzynarodowy*…, art. 20, pkt 2.

[152] I.C. Kamiński, *Mowa*…, s. 109.

[153] Rzecznik generalny E. Sharpston w opinii do spraw połączonych C-148/13 do C-150/13, A i in. przeciwko Staatssecretaris van Veiligheid en Justitie, zauważyła, że na gruncie wykładni dokonywanej przez ETPC,

Ochrona prywatności w ujęciu sędziów TSUE obejmuje prawo do poczucia przynależności do szczególnej grupy społecznej. Uznanie za szczególną grupę społeczną następuje, jeśli: „członkowie takiej grupy mają jakąś wspólną nieusuwalną cechę wrodzoną lub przeszłość lub charakteryzują się jakimś wspólnym rysem lub przekonaniem na tyle istotnym z punktu widzenia tożsamości lub sumienia, że nie należy nikogo zmuszać do wyrzeczenia się go, oraz [...] grupa ta posiada odrębną tożsamość w danym państwie, ponieważ jest postrzegana przez otaczające społeczeństwo jako inna. W zależności od sytuacji w kraju pochodzenia szczególna grupa społeczna może oznaczać grupę, u podstaw której leży wspólna cecha orientacji seksualnej. Orientacji seksualnej nie należy rozumieć jako obejmującej czyny uznawane za przestępcze w świetle prawa krajowego państw członkowskich"[154]. Definiowanie szczególnej grupy społecznej następuje w oparciu o treść dyrektywy Parlamentu Europejskiego i Rady 2011/95/UE[155]. Zgodnie z motywem 30 tej dyrektywy: „Definiując szczególną grupę społeczną, należy zwrócić należytą uwagę na aspekty związane z płcią wnioskodawcy, jeżeli mają one związek z uzasadnioną obawą wnioskodawcy przed prześladowaniem, w tym na tożsamość płciową i orientację seksualną, które to aspekty mogą być powiązane z określoną tradycją prawną i zwyczajami, prowadzącymi na przykład do okaleczania narządów płciowych, przymusowej sterylizacji czy przymusowej aborcji".

Państwo, w myśl zapatrywań TSUE i ETPC, powinno zapewnić jednostce realizację prawa do tożsamości w sposób niezakłócony, tj. wolny od niepokojenia jednostki ze względu na jej przynależność lub orientację. Jednostka nie powinna być zatem, w ujęciu orzecznictwa, niepokojona przez inne osoby, w tym organy publiczne, ze względu na jej identyfikację tożsamościową. Pozytywne obowiązki państwa, w ujęciu ETPC i TSUE, obejmują nie tylko działania o charakterze następczym, ale także *ex ante*, bowiem tylko w ten sposób zapewniona może zostać „sprawiedliwa równowaga" pomiędzy prawem jednostki do ochrony jej tożsamości a innymi wartościami ogólnospołecznymi.

Takie podejście powoduje, że ochrona wolności wypowiedzi, w ujęciu ETPC i TSUE, musi ustąpić potrzebie ochrony prywatności wówczas, gdy jednostka skarży się, że jest niepokojona, napiętnowana albo nierówno traktowana (dyskryminowana) ze względu na jej tożsamość. Naruszenie prawa do tożsamości może zaistnieć zarówno wówczas, gdy naruszyciel swoje działania kieruje wobec indywidualnie obranej osoby, jak i wtedy, gdy stanowi ono atak na

„pojęcie «życia prywatnego» jest szerokie i jako takie nie poddaje się wyczerpującej definicji. Obejmuje ono integralność fizyczną i psychiczną osoby, w tym elementy takie jak orientacja seksualna i życie seksualne, które mieszczą się w sferze osobistej, chronionej przez art. 8 EKPC (wyrok ETPC z dnia 12 czerwca 2003 r. w sprawie Van Kück przeciwko Niemcom, nr 35968/97, Recueil des arrêts et décisions, 2003VII, § 69 i przytoczone tam orzecznictwo)" (pkt 38 opinii).

[154] Wyrok TS z 25 stycznia 2018 r., C-473/16, F przeciwko Bevándorlási és Állampolgársági Hivatal, pkt 11.

[155] Dyrektywa Parlamentu Europejskiego i Rady 2011/95/UE z 13 grudnia 2011 r. w sprawie norm dotyczących kwalifikowania obywateli państw trzecich lub bezpaństwowców jako beneficjentów ochrony międzynarodowej, jednolitego statusu uchodźców lub osób kwalifikujących się do otrzymania ochrony uzupełniającej oraz zakresu udzielanej ochrony (Dz.Urz. UE L 337 z 2011 r., s. 9).

całą grupę, o ile jest to „szczególna grupa społeczna". W takim bowiem wypadku działanie to może zostać zakwalifikowane jako naruszenie „sprawiedliwej równowagi" pomiędzy wartościami ogólnospołecznymi a prawami mniejszości[156].

Zmodyfikowane podejście normatywne stanowi prawną podstawę i uzasadnienie zmiany stanowiska ETPC. I.C. Kamiński zauważa, że w 2022 r. Komitet Ministrów Rady Europy przyjął nową rekomendację w sprawie zwalczania mowy nienawiści, która posługuje się już inną perspektywą normatywną[157]. Podczas gdy pierwsza rekomendacja R 97/20 koncentrowała się na swobodzie wypowiedzi[158], druga[159] akcentuje potrzebę budowania równowagi różnych gwarancji Konwencji, a więc uwzględnienia prawa do życia prywatnego (art. 8 EKPC), które obejmuje ochroną tożsamość jednostki, oraz zakazu dyskryminacji (art. 14 EKPC). I.C. Kamiński zwraca uwagę, że zgodnie z przyjętą przez ETPC aktualną wykładnią, z art. 8 i 14 EKPC wynika pozytywny obowiązek państwa do zabezpieczenia jednostki przed mową nienawiści oraz stworzenia adekwatnego reagowania na taką mowę[160]. Ochrona prywatności,

[156] ETPC w sprawie Fedotova i inni przeciwko Rosji analizował co prawda sytuację konkretnych skarżących żyjących w związku jednopłciowym, faktycznie jednak udzielona odpowiedź dotyczyła całej grupy mniejszościowej. Trybunał, odpowiadając na pytanie, czy Rosja wywiązała się z pozytywnego obowiązku zapewnienia prawa skarżących do poszanowania ich życia prywatnego i rodzinnego, zwłaszcza poprzez zapewnienie ram prawnych pozwalających im na uznanie i ochronę ich jednopłciowego związku w prawie krajowym, uznał, że doszło do naruszenia art. 8 EKPC. Skarżące wskazywały, że „bez formalnego uznania związki jednopłciowe nie mogą brać udziału w programach mieszkaniowych lub pomocowych, nie mogą odwiedzać swych partnerów w szpitalu, są pozbawione gwarancji w postępowaniu karnym (prawo do odmowy złożenia zeznań na szkodę partnera), oraz praw do dziedziczenia majątku po zmarłym partnerze. Sytuacja ta stwarza konflikt pomiędzy rzeczywistością społeczną skarżących, które żyją w stałym związku opartym na wzajemnym uczuciu, a prawem, które odmawia ochrony najbardziej podstawowych «potrzeb» pojawiających się w kontekście par jednopłciowych. Taki konflikt może skutkować poważnymi codziennymi utrudnieniami dla par jednopłciowych". Trybunał uznał, że „zachodzi […] poważna różnica pomiędzy uwzględnieniem powszechnego poparcia za rozszerzeniem zakresu gwarancji konwencyjnych a sytuacją, w której takie poparcie zostaje przywołane, aby odmówić dostępu znacznej części ludności do podstawowego prawa do poszanowania życia prywatnego i rodzinnego. Byłoby to niezgodne z wartościami leżącymi u podstaw Konwencji jako instrumentu europejskiego porządku publicznego, gdyby wykonywanie praw konwencyjnych przez grupę mniejszościową uzależnić od akceptacji większości".

[157] I.C. Kamiński, *Mowa*..., s. 90.

[158] Jak wskazuje I.C. Kamiński" „Rekomendacja posługuje się szeroką definicją nowy nienawiści. Przez mowę nienawiści rozumiane są wszelkie postacie wypowiedzi, które szerzą, nawołują, promują lub usprawiedliwiają (*spread*, *incite*, *promote or justify*) nienawiść rasową, ksenofobię, antysemityzm lub inne formy nienawiści opartej na nietolerancji, włączając nietolerancję mającą postać «agresywnego nacjonalizmu» lub etnocentryzmu, dyskryminacji i wrogości wobec mniejszości, imigrantów bądź osób o imigracyjnym pochodzeniu. Szczególna odpowiedzialność spoczywa przy tym na instytucjach władzy publicznej, tak ogólnokrajowych, jak i samorządowych" (I.C. Kamiński, *Pojęcie*..., s. .88–89).

[159] Rekomendacja Rec (2022)16 z 20 maja 2022 r. w sprawie zwalczania mowy nienawiści, https://rm.coe.int/prems-083822-gbr-2018-recommendation-on-combating-hate-speech-memorand/1680a710c9 (dostęp: 20 czerwca 2024 r.).

[160] Autor ten podkreśla, że na gruncie nowej rekomendacji państwa nie muszą co prawda wprowadzić trybu ścigania z oskarżenia publicznego wypowiedzi naruszających prywatność (prawa tożsamościowe), ale twórcy rekomendacji sygnalizują, że państwo nie decydując się na kryminalizację, powinno „zabronić" wypowiedzi na mocy prawa cywilnego lub administracyjnego (pkt 62 rekomendacji). Dodatkowo, państwa powinny zapewnić, że w każdym przypadku, gdy na mocy prawa krajowego mowa nienawiści stanowi przestępstwo, a jednocześnie zachodzi wystarczające podejrzenie, iż czyn został popełniony, przeprowadzone będzie skuteczne postępowanie wyjaśniające (pozytywny obowiązek proceduralny). I.C. Kamiński zauważa, że: „Analiza strasburskiego orzecznictwa uzasadnia wniosek, że tradycyjne standardy, związane z kwalifikacją wypowiedzi jako twierdzenia

w poszerzonym, tożsamościowym kształcie, uzyskała prymat nad potrzebą zapewnienia swobody wypowiedzi nawet wówczas, gdy wypowiedź dotyczy istotnych kwestii społecznych budzących powszechne zainteresowanie[161].

Wypowiedzi naruszające prywatność jednostki w rozumieniu zaproponowanym przez ETPC i TSUE będą, jak należy sądzić, mogły być kwalifikowane jako „nielegalne treści" w ujęciu AUC, a w konsekwencji ich usuwanie lub blokowanie będzie nie tylko usprawiedliwione, ale stanie się konieczne ze względu na ciążące na państwie obowiązki pozytywne. Do naruszeń prywatności uzasadniających kwalifikowanie wypowiedzi jako nielegalnej proponuje się także zaliczyć wypowiedzi, które ujawniają dane osobowe jednostki, w szczególności dane wrażliwe.

Na gruncie EKPC postuluje się zastosowanie zarówno następczych środków ochrony, jak i usprawiedliwiona oraz konieczna jest uprzednia reakcja prawa (*ex ante*) skierowana na przeciwdziałanie aktom mowy nienawiści. Można uznać, że „mowa nienawiści staje się, obok wypowiedzi politycznej oraz w sprawach o ogólnym znaczeniu, wypowiedzi artystycznej oraz wypowiedzi komercyjnej, jednym z kluczowych typów wypowiedzi, które organizują sposób badania przez Trybunał ingerencji w wolność wypowiedzi kwestionowanej w skardze"[162].

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.

Zmiana paradygmatu ochrony wolności wypowiedzi dotyczy zatem zarówno zmian w strukturze i hierarchii wartości prawnie chronionych, jak i w sposobie ich definiowania, a także dotyczy identyfikowania funkcji i zadań państwa. Państwo w miejsce negatywnych obowiązków polegających na powstrzymaniu się przed działaniem i pełnieniu roli gwaranta staje się zobowiązane do pełnienia funkcji monitorujących i interwencyjnych, w tym także w sferze stosunków prywatnoprawnych[163].

---

lub opinii, tracą znaczenie w kontekście wypowiedzi, które są identyfikowane jako mowa nienawiści. Analogicznie dzieje się także 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. Konstrukcja mowy nienawiści pełni więc funkcję klasyfikacyjną czy też identyfikacyjną – 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" (I.C. Kamiński, *Pojęcie*..., s. 108–109).

[161] I.C. Kamiński, *Pojęcie*..., s. 98.

[162] I.C. Kamiński, *Mowa*..., s. 109.

[163] Zgodnie z wyrażonym przez ETPC stanowiskiem, mimo iż podstawowym przedmiotem art. 8 Konwencji jest ochrona jednostek przed arbitralną ingerencją ze strony organów władzy publicznej, artykuł ten może także nakładać na państwo pewne pozytywne obowiązki w postaci zapewnienia skutecznego poszanowania praw chronionych przez art. 8. Obowiązki te mogą obejmować przyjęcie środków mających na celu zabezpieczenie poszanowania dla życia prywatnego lub rodzinnego nawet w sferach relacji pomiędzy samymi osobami prywatnym (wyrok ETPC z 13 lipca 2021 r., skargi nr 40792/10, 30538/14 i 43439/14, Fedotova i inni przeciwko Rosji).

Uzasadnienia zmiany stanowiska ETPC należy poszukiwać nie tyle w nowym podejściu Trybunału do oceny zjawisk społecznych, ile w sposobie ich definiowania w zaleceniach i rekomendacjach Rady Europy.

3.3.3. Dezinformacja

W klasyfikacji zaproponowanej przez organizację „Internet & Jurisdiction" w ramach programu CONTENT & JURISDICTION[164], realizowanego na potrzeby zarówno organów UE, jak i Rady Europy, a także ONZ i UNESCO oraz 400 innych kooperujących z tą organizacją państw i podmiotów[165], przyjęto, że dezinformacja i inne rodzaje „treści nielegalnych" mogą występować w różnej postaci. Działanie identyfikowane jako dezinformacja obejmuje zatem zarówno rozpowszechnianie fake newsów (fałszywych wiadomości), jak i jest kojarzone z podszywaniem się pod inne osoby, tworzeniem fałszywych kont, a także przekazywaniem wprowadzających w błąd informacji o substancjach medycznych oraz wprowadzaniem nieprawdziwych metadanych w celu uzyskiwania wadliwych wyników wyszukiwania, a nadto dotyczy zachowań polegających na projekcji rzeczywistości z użyciem środków audiowizualnych i hologramów (projekcje holograficzne 3d) w sposób łudząco przypominający osoby, zdarzenia i okoliczności.

Dezinformacja (*disinformation*, *fake news*) obejmuje rozpowszechnianie przez osoby fizyczne lub boty fałszywych bądź niedokładnych informacji w celu uzyskania korzyści politycznych, ideologicznych lub ekonomicznych. W skrajnych wypadkach jej celem jest uzyskanie wpływu na wyniki wyborów i zakłócenie procesów demokratycznych. Dezinformacja może przybierać formę samoistnych postów quasi-informacyjnych opartych częściowo na faktach, w tym na tzw. tweetowaniu, publikowaniu materiałów przypominających artykuły prasowe albo umieszczaniu zmasowanych komentarzy. Tego typu treści, tj. zawierające nieprawdziwe informacje i dane, nie są zazwyczaj identyfikowane jako naruszenie prawa. Rozpowszechnienie nieprawdziwej informacji nie stanowi bowiem, co do zasady, występku ani nie daje podstawy do zgłoszenia roszczeń na gruncie prawa cywilnego. Zarazem ocena prawdziwości może dotyczyć tylko tych wypowiedzi, które zawierają twierdzenia o faktach[166]. Wypowiedzi zawierające twierdzenia należy wyraźnie odróżnić od opinii i satyry.

[164] Content & Jurisdiction Program..., s. 21.

[165] Internet & Jurisdiction Policy Network jest organizacją z udziałem wielu zainteresowanych stron, która – jak wskazano na stronie podmiotowej tej organizacji – „wspiera interoperacyjność prawną w cyberprzestrzeni. Jej zainteresowane strony współpracują ze sobą, aby zachować transgraniczny charakter Internetu, chronić prawa człowieka, zwalczać nadużycia i umożliwić globalną gospodarkę cyfrową. Od 2012 roku Internet & Jurisdiction Policy Network zaangażowała ponad 400 kluczowych podmiotów z sześciu grup interesariuszy na całym świecie" (https://www.internetjurisdiction.net/about/mission, dostęp: 20 czerwca 2024 r.).

[166] Potrzeba odróżnienia twierdzeń o faktach od sądów wartościujących stała się jednym ze stałych elementów prowadzonych postępowań sądowych w sprawach, których przedmiotem było ustalenie granic wolności wypowiedzi. ETPC wielokrotnie wskazywał, że wypowiedzi mogą przybierać postać zracjonalizowanych twierdzeń

Nie jest zatem co do zasady dopuszczalne, by opinia (sąd wartościujący) mógł zostać uznany za dezinformację (fałszywą wiadomość). Zważywszy jednak, że opinia, jak się oczekuje[167], powinna opierać się na faktach (podstawa faktyczna), przestaje być oczywiste, czy rzeczywiście wypowiedzi przybierające postać opinii nigdy nie stanowią dezinformacji. O ile więc satyra oraz sąd wartościujący, generalnie, nie będą kwalifikowane jako dezinformacja, o tyle działanie polegające na rozgłoszeniu nieprawdziwych twierdzeń o faktach proponuje się uznawać za treści szkodliwe (nielegalne treści)[168].

Przedmiotem dezinformacji mogą być różne kwestie, jednakże zawsze okoliczność ich rozgłoszenia wywołuje negatywne skutki w sferze świadomości odbiorców, motywując ich do podejmowanie szkodliwych decyzji i wadliwych wyborów. Przedmiotem ochrony jest zatem nie tyle prawdziwość informacji, ile raczej bezpieczeństwo informacyjne i utrzymanie jego stanu na poziomie, który nie zagraża innym dziedzinom, jak w szczególności bezpieczeństwo publiczne i bezpieczeństwo państwa (wewnętrzne i zewnętrzne)[169].

Bezpieczeństwo informacyjne nie jest terminem prawnym, jednakże termin ten uzyskał autonomię na gruncie nauki o bezpieczeństwie[170], a także stał się nośnikiem koncepcji i rozwiązań o charakterze normatywnym. Pojęcie bezpieczeństwa informacyjnego powinno być bowiem ujmowane w znaczeniu materialnoprawnym i proceduralnym. W znaczeniu materialnoprawnym bezpieczeństwo informacyjne może być definiowane jako dobro prawne, które wymaga indywidualnej, tj. odrębnej w stosunku do innych dóbr prawnie chronionych,

---

odnoszących się do faktów, a także mogą mieć charakter niezracjonalizowanych, subiektywnych opinii (ocen). 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 art. 10 Konwencji. Konsekwencją powyższego ustalenia jest zastosowanie bardziej rygorystycznych wymagań w stosunku do autorów wypowiedzi o faktach, bowiem prawdziwości faktów 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 faktach (wyroki ETPC z 19 maja 2005 r., skarga nr 48176/99, Turhan przeciwko Turcji; z 27 lutego 2001 r., skarga nr 26958/95, Jerusalem przeciwko Austrii; z 6 maja 2003 r., skarga nr 48898/99, Perna przeciwko Włochom; z 12 lipca 2001 r., skarga nr 29032/95, Feldek przeciwko Słowacji).

[167] ETPC 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 uzasadnione podstawy. 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 słowa (wyrok ETPC z 12 lipca 2001 r., skarga nr 29032/95, Feldek przeciwko Słowacji).

[168] Content & Jurisdiction Program..., s. 22.

[169] Z. Nowakowski, M. Pomykała, J. Rajchel, *Pojęcie bezpieczeństwa i porządku publicznego* [w:] *Administracja bezpieczeństwa i porządku publicznego ze szczególnym uwzględnieniem aspektów prawno-organizacyjnych Policji*, red. K. Rajchel, Warszawa 2009, s. 48; cyt. za: D. Kamuda, M. Policeusz, *Cyberprzestępstwa a zagrożenie bezpieczeństwa RP – zagadnienia wybrane* [w:] *Przestępczość XXI wieku. Zapobieganie i zwalczanie. Problemy technologiczno-informatyczne*, red. E.W. Pływaczewski, W. Filipkowski, Z. Rak, Warszawa 2015, s. 593.

[170] W naukach o bezpieczeństwie wskazuje się na potrzebę wyodrębnienia bezpieczeństwa informacyjnego jako dziedziny bezpieczeństwa państwa (zob. K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2008, s. 19 i n.).

ochrony prawnej. W znaczeniu proceduralnym pojęcie bezpieczeństwa informacyjnego stanowić będzie dyrektywę działania, a w konsekwencji normę kompetencyjną upoważniającą określone rodzaje organów państwa do podejmowania czynności kształtujących sytuację prawną innych podmiotów w sferze ich praw i obowiązków w zakresie utrzymania lub osiągnięcia stanu bezpieczeństwa, a także przeciwdziałania zagrożeniom[171]. Autonomizacja informacji jako wartości prawnie chronionej oraz dostrzeżenie potrzeby stosowania nowych instrumentów ochrony prawnej informacji stały się możliwe na skutek ustalenia, że informacja stanowi zasób strategiczny[172], którego ochrona leży w interesie państwa, a jego naruszenie zagraża bezpieczeństwu. K. Liedel zauważa, że „bezpieczeństwo informacyjne wraz z bezpieczeństwem ekonomicznym i energetycznym stają się priorytetowymi aspektami bezpieczeństwa"[173].

Zważywszy na skutki naruszenia bezpieczeństwa informacyjnego, w szczególności związane z dezinformacją i rozpowszechnieniem fałszywych wiadomości, istnieje ryzyko naruszenia wielu wartości i dóbr prawnie chronionych, takich jak np. dobre imię, godność, ale także zdrowie, bezpieczeństwo, środowisko przyrodnicze, integralność państwa, porządek publiczny. W rezultacie spośród form dezinformacji wyróżniono np. dezinformację medyczną (*medical misinformation*)[174]. Fałszywe wiadomości medyczne to treści rozpowszechniające nieprawdziwe lub wprowadzające w błąd informacje, które mogą mieć szkodliwy wpływ na zdrowie i bezpieczeństwo osób. Ten rodzaj dezinformacji zidentyfikowano w czasie pandemii COVID-19, w sposób arbitralny i stanowczy rozstrzygając, że „przykładem może być promowanie fałszywych leków na choroby i porady antyszczepionkowe. Może to być motywowane celem uzyskania korzyści finansowych lub po prostu z niewiedzy, a nie z zamiarem wyrządzenia krzywdy"[175].

Zidentyfikowanie *„medical misinformation"* jako jednego z typów fałszywych wiadomości sygnalizuje, z jednej strony, związek występujący pomiędzy rozpowszechnieniem fałszywej wiadomości a naruszeniem dobra w postaci życia i zdrowia, z drugiej jednak strony – wskazuje na ryzyko nadużyć w zakresie klasyfikowania wiadomości jako nielegalnej. Dezinformacja wystąpi bowiem także wówczas – czego jednak organizacja Internet & Jurisdiction nie dostrzega – kiedy ustalenie rzekomej nielegalnej, wprowadzającej w błąd treści następuje w warunkach braku dostatecznych dowodów na potwierdzenie nieprawdziwości informacji,

[171] J. Taczkowska-Olszewska, *Bezpieczeństwo informacyjne jako kategoria prawna. Ujęcie teoretyczne [w:] Bezpieczeństwo informacyjne. Aspekty prawno-administracyjna*, red. W. Kitler, J. Taczkowska-Olszewska, Warszawa 2017, s. 49.

[172] Bezsporne wydaje się obecnie na gruncie nauki o bezpieczeństwie, że „informacja jest strategicznym zasobem państwa współdecydującym o bezpieczeństwie narodowym" (B. Lent, *Bezpieczeństwo w telekomunikacji i teleinformatyce*, Warszawa 2007, s. 14).

[173] K. Liedel, *Cyberbezpieczeństwo – wyzwania przyszłości. Działania społeczności międzynarodowej* [w:] *Bezpieczeństwo w XXI wieku. Asymetryczny świat*, red L. Liedel, P. Piasecka, T.R. Aleksandrowicz, Warszawa 2011, s. 437.

[174] Content & Jurisdiction Program..., s. 22.

[175] Content & Jurisdiction Program..., s. 22.

a pomimo to zostaje ona usunięta z przestrzeni dyskusji (forum publicznej debaty). Istnieje zatem poważne ryzyko ograniczenia debaty publicznej jako następstwa nadużycia uprawnień przez podmioty moderujące debatę, w tym organy publiczne, w zakresie, w jakim podmioty te korzystają z przyznanych im kompetencji do dokonywania wiążącej wykładni terminu „nielegalne treści".

Inną formą dezinformacji jest podszywanie się pod inne osoby [fałszywe konta/profile/strony – *impersonation* (*fake accounts/profiles/pages*)] polegające na kopiowaniu układu użytkownika, używaniu podobnej nazwy użytkownika lub podszywaniu się pod inną osobę w profilach, na stronach, w komentarzach, e-mailach lub filmach[176]. W zależności od zamiaru sprawcy możliwe jest kwalifikowanie tego działania zarówno jako fałszywego oskarżenia lub wprowadzenia w błąd, jak i jako znamienia innego rodzaju czynu, w szczególności oszustwa. Stąd czynność tworzenia fałszywego konta albo podszywania się pod inną osobę może być opisywana nie tylko jako samodzielna czynność sprawcza objęta sankcją, ale będzie także rozpatrywana jako czyn pozostający w zbiegu z innymi występkami bądź stanowiący znamię szczególnego typu przestępstwa. Podszywanie się pod inne konta może obejmować działanie botów lub innych aplikacji; oznacza *de facto* przejmowanie kont użytkowników w celu nadania generowanym informacjom oczekiwanego poziomu wiarygodności (*fraudulent accounts*)[177]. Działanie to może polegać na przejmowaniu zarówno kanału komunikacji (np. kanał YouTube), jak i umieszczaniu postów w miejsce znanej, identyfikowanej przez opinię publiczną, osoby fizycznej (np. Facebook lub platforma „X")[178].

Szczególną postacią podszywania jest „głębokie kłamstwo" (*deepfakes*) polegające na synchronizacji obrazu i dźwięku z użyciem wizerunków i głosu znanych postaci i prezentowanie ich zachowań, w tym wypowiedzi, jako rzeczywistych, podczas gdy zachowania te nigdy nie miały miejsca, a prezentacja stanowi cyfrowo wygenerowaną projekcję łudząco przypominającą rzeczywiste zdarzenia i postacie. W niektórych państwach rozpowszechnianie *deepfakes* uznano za poważne zagrożenie, angażując w ich zwalczanie *ex officio* organy porządku i bezpieczeństwa publicznego[179]. *Deepfake* odnosi się do szerokiego zakresu generowanych lub manipulowanych w mediach cyfrowych obrazów, filmów, dźwięku lub tekstu; zbiorczo

[176] Content & Jurisdiction Program..., s. 21.
[177] Content & Jurisdiction Program..., s. 26.
[178] Content & Jurisdiction Program..., s. 21.
[179] W USA w zwalczanie deepfake'ów zaangażowano FBI, która wydała komunikat adresowany do użytkowników internetu, opisując istotę tego występku. FBI wskazuje, że treści syntetyczne mogą być uważane za chronione zgodnie z Pierwszą Poprawką; jednak FBI może zbadać, kiedy związane z nimi fakty i raporty wskazują potencjalne naruszenia federalnych ustaw karnych. Aplikacje mobilne, „deepfake-as-a-service" i inne publicznie dostępne narzędzia coraz częściej ułatwiają złośliwym podmiotom manipulowanie istniejącymi lub tworzenie nowych obrazów lub filmów. Narzędzia te, często swobodnie spotykane online, są wykorzystywane do tworzenia wysoce realistycznych i konfigurowalnych treści deepfake dla ofiar docelowych lub do atakowania wtórnych, powiązanych z nimi ofiar (zob. *Malicious Actors Manipulating Photos and Videos to Create Explicit Content and Sextortion Schemes*, https://www.ic3.gov/Media/Y2023/PSA230605, dostęp: 20 czerwca 2024 r.).

określanych jako „treści syntetyczne" lub „mediatetyczne"[180] tworzone przy użyciu sztucznej inteligencji i procesów uczenia maszynowego. *Deepfakes* może przedstawiać zmianę lub podszywanie się pod tożsamość danej osoby, aby wyglądało to tak, jakby robiła lub mówiła rzeczy, których nigdy nie zrobiła[181].

Jako odrębnie klasyfikowaną formę dezinformacji wskazuje się także wyciek poufnych lub tajnych informacji (*leaked confidential* lub *secret information*[182]). Ocena bezprawnego charakteru działania sprawcy jest uzasadniana rozmiarem szkody, jaka może powstać w związku z uzyskaniem dostępu do informacji przez osoby nieuprawnione[183], w szczególności wówczas, gdy naruszona albo zagrożona zostaje jedna z dziedzin bezpieczeństwa (państwa, publiczne, wewnętrzne, zewnętrzne, energetyczne i inne). Jednakże za wyjątek stanowiący wyłom w tym systemie uchodzą informacje ujawnione przez sygnalistów działających w interesie publicznym. Zarówno na gruncie rozporządzeń cyfrowych[184], jak i aktów nienormatywnych UE[185], a także na gruncie konwencji Narodów Zjednoczonych szczególną ochroną objęte zostały

[180] *Malicious*...

[181] Zostało to opisane jako „audio i wideo, które wyglądają i brzmią jak prawdziwa osoba, mówiące coś, czego ta osoba nigdy nie powiedziała", – Content & Jurisdiction Program..., s. 21.

[182] Content & Jurisdiction Program..., s. 24.

[183] Niejawny charakter informacji wynika z jej cech materialnych, a nie z tego, czy została jej nadana klauzula tajności (zastrzeżone, poufne, tajne, ściśle tajne). Informacja jest bowiem niejawna z uwagi na zagrożenia wynikające z jej treści, a nie w wyniku klasyfikacji (zob. A. Ziółkowska, D. Fleszer, O. Sitarz [w:] *Ochrona informacji niejawnych. Komentarz*, red. A. Ziółkowska, Warszawa 2024, art. 5, pkt 2). Informacje niejawne podzielono ze względu na stopień ich ważności (niezbędności utrzymania w tajemnicy). Wartościami mogącymi ograniczać prawo dostępu do informacji są: bezpieczeństwo państwa, porządek publiczny, ważny interes gospodarczy państwa, ochrona praw i wolności innych osób. Zgodnie z definicjami klauzul tajności ochronie określonej przepisami ustawy o ochronie informacji niejawnych podlegają tylko takie informacje, których ujawnienie przyniosłoby szkodę dla bezpieczeństwa lub interesów państwa (A. Ziółkowska, D. Fleszer, O. Sitarz [w:] *Ochrona*..., art. 5, pkt 2).

[184] Na gruncie AUC szczególny status mają tzw. zaufane podmioty sygnalizujące (zaufani sygnaliści). Celem działania sygnalistów jest powiadamianie o istniejących, a także prawdopodobnych naruszeniach polegających na rozpowszechnianiu nielegalnych treści oraz treści szkodliwych (zob. G. Bar [w:] *Akt o usługach cyfrowych. Komentarz*, red. D. Lubasz, M. Namysłowska, Warszawa 2024, art. 22, pkt. 10). Status zaufanego podmiotu sygnalizującego na podstawie AUC 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. Status zaufanego podmiotu sygnalizującego, jak wskazano w motywie 61, należy przyznawać wyłącznie podmiotom, a nie osobom, które to podmioty wykazały m.in., że posiadają szczególną wiedzę ekspercką i kompetencje w zakresie zwalczania nielegalnych treści oraz że działają w sposób dokładny, obiektywny i z zachowaniem należytej staranności. Podmioty takie mogą mieć charakter publiczny, mogą być to także organizacje pozarządowe i podmioty prywatne lub mieszane. Dostawcy platform internetowych zostali zobowiązani w art. 22 ust. 1 AUC do wprowadzenia niezbędnych środków technicznych i organizacyjnych w celu zapewnienia priorytetowego traktowania zgłoszeń dokonywanych przez zaufane podmioty sygnalizujące, działające w wyznaczonych dziedzinach, w których dysponują wiedzą ekspercką.

[185] W rezolucji Parlamentu Europejskiego z 24 października 2017 r. w sprawie uzasadnionych środków ochrony sygnalistów działających w interesie publicznym podczas ujawniania poufnych informacji posiadanych przez przedsiębiorstwa i organy publiczne (2016/2224(INI)) (https://www.europarl.europa.eu/doceo/document/TA-8-2017-0402_PL.html, dostęp: 20 czerwca 2024 r.) wskazano, że „sygnaliści i członkowie ich rodzin, jak również osoby, które pomagają im i których życie lub bezpieczeństwo jest zagrożone, muszą być uprawnione do właściwej i skutecznej ochrony ich integralności fizycznej, moralnej i społecznej oraz źródła utrzymania

osoby zgłaszające naruszenia prawa. W art. 33 konwencji przeciwko korupcji[186] zalecono, aby państwa zapewniły ochronę osobom, które zgłaszają w dobrej wierze i na uzasadnionych podstawach właściwym organom wszelkie fakty dotyczące przestępstw objętych konwencją. Artykuł 32 tej konwencji zapewnia ochronę świadkom, biegłym i ofiarom.

Do kategorii dezinformacji zaliczane jest także działanie polegające na tworzeniu fałszywych metadanych stanowiących opisy zawartości oferowanych treści po to, by uzyskać wynik wyszukiwania korzystny dla autora treści i wysokie jej pozycjonowanie, pomimo że oferowane treści pozostają w luźnym związku z wyszukiwaną frazą. Wprowadzające w błąd metadane (tytuł, opis, znaczniki, adnotacje i miniatury) zawierają wprowadzające w błąd tytuły, opisy, tagi, adnotacje służące oszukiwaniu algorytmów w wyszukiwarkach, prowadząc do zawartości niereprezentatywnej dla wyszukiwanej frazy[187].

3.3.4. Zniesławienie

Wypowiedzi zniesławiające (*defamatory personal content*), a także skoordynowana aktywność komunikacyjna nakierowana na zniesławienie (*coordinated/organized attempts at defamation*) mogą być kwalifikowane jako nielegalne treści, co jednak nie oznacza, że istnieje zasada, zgodnie z którą za nielegalne należałoby uznawać wypowiedzi ingerujące w dobre imię, godność lub cześć jednostki albo naruszające jej renomę. Platformy na ogół nie ograniczają tego typu treści, chyba że przekraczają one próg mowy nienawiści lub podżegania[188]. Platformy ograniczają treści rzekomo zniesławiające tylko wtedy, gdy są one skoordynowane z zamiarem wyrządzenia szkody. Przyjmuje się bowiem, że prawa jednostek do ochrony przed bezprawnymi atakami na ich honor i reputację muszą być zrównoważone z prawami mówców do wyrażania opinii bez ingerencji oraz prawem dostępu do informacji. Wypowiedzi lub opinie polityczne, krytyka osób pełniących funkcje publiczne działających w ramach ich obowiązków lub wypowiedzi leżące w interesie publicznym, nawet jeśli zostaną uznane za zniesławiające, będą objęte ochroną, jako mieszczące się w standardzie wolności wypowiedzi.

Rozstrzygająca dla zakresu udzielonej ochrony jest decyzja klasyfikująca daną wypowiedź pod kątem stwierdzenia, czy wypowiedź może być oceniana na gruncie konwencyjnego standardu wolności wypowiedzi (art. 10 EKPC, art. 11 KPP, art. 19 MPPOiP) czy przeciwnie,

poprzez zastosowanie możliwie najwyższego stopnia poufność" (pkt 42), a także, że „sygnaliści nie powinni być przedmiotem postępowania karnego, cywilnego, sankcji administracyjnych lub dyscyplinarnych z tytułu dokonanych zgłoszeń" (pkt 48). Zarazem zaleca się przyjęcie mechanizmów wyłączających odpowiedzialność sygnalistów nawet wówczas, gdy przekazane przez nich informacje nie okazały się prawdziwe. Podkreślono, że „osoba nie powinna być pozbawiana ochrony wyłącznie z tego powodu, że błędnie oceniła fakty lub stwierdzone zagrożenie dla interesu publicznego nie wystąpiło" (pkt 50).

[186] Konwencja Narodów Zjednoczonych przeciwko korupcji, przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 31 października 2003 r. (Dz.U. z 2007 r. Nr 84, poz. 563).

[187] Content & Jurisdiction Program..., s. 25.

[188] Content & Jurisdiction Program..., s. 21.

nie mieści się w tym standardzie, a w konsekwencji nie tylko nie zostanie uznana za dopuszczalną, ale zostanie uznana za nielegalną i jako taka zostanie usunięta z obiegu publicznego, a autor wypowiedzi poniesie odpowiedzialność prawną za jej rozpowszechnienie.

Wytyczenie linii podziału wypowiedzi na legalne (objęte ochroną konwencyjną) i nielegalne (wyłączone z tej ochrony) następuje przez wykorzystanie konstrukcji mowy nienawiści. W mechanizmie tym tkwi zarazem jej normatywny charakter. Konstrukcja mowy nienawiści jest bowiem wykorzystywana nie tylko na płaszczyźnie materialnoprawnej, ale przede wszystkim procesowej, służąc podejmowaniu decyzji klasyfikacyjnej. I.C. Kamiński zwraca uwagę, że „decyzja klasyfikacyjna" jest kluczowa[189] dla ustalenia zakresu ochrony wypowiedzi. Zarazem decyzja ta nigdy nie będzie w pełni obiektywna, bo zawsze należy do sędziów, których stanowiska i perspektywy mogą się od siebie różnić[190].

O ile zatem mowa nienawiści jako wypowiedź nielegalna zostanie usunięta z internetu, o tyle nie każda wypowiedź nieprawdziwa (dezinformacja), choćby naruszała dobra osobiste osoby, której dotyczy, zostanie usunięta, nawet jeśli zawarte w niej dane ingerowałyby w prywatność osoby, której dotyczą. Nawet bowiem wówczas, gdy nieprawdziwa wypowiedź zawiera dane osobowe, co jest jednoznaczne z ingerencją w prywatność, ETPC i TSUE uznawać będą za konieczne jej usunięcie z internetu tylko wówczas, gdy na przeszkodzie temu działaniu nie stanie potrzeba ochrony innej wartości, w tym prawa społeczeństwa do informacji. W wytycznych Europejskiej Rady Ochrony Danych Osobowych[191] wskazano, że „w zależności od okoliczności sprawy, administratorzy stron internetowych a także pośrednicy internetowi, w tym dostawcy wyszukiwarek internetowych mogą odmówić usunięcia z listy wyników wyszukiwania treści w przypadku, gdy są w stanie wykazać, że ich ujęcie w wynikach wyszukiwania jest bezwzględnie konieczne do ochrony prawa internautów do wolności wypowiedzi"[192].

---

[189] I.C. Kamiński, *Mowa*..., s. 89.

[190] I.C. Kamiński, *Mowa*..., s. 89.

[191] Wytyczne 5/2019 w sprawie kryteriów dotyczących prawa do bycia zapomnianym w sprawach dotyczących wyszukiwarek internetowych na podstawie RODO (część 1), Wersja 2.0 Przyjęte 7 lipca 2020 r., ; s. 15–16, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201905_rtbfsearchengines_afterpublicconsultation_pl.pdf (dostęp: 20 czerwca 2024 r.).

[192] Europejska Rada Ochrony Danych Osobowych wypowiedziała się w ten sposób na tle dwóch orzeczeń TSUE, tj.: wyroku z 24 września 2019 r., C-136/17, GC i in. przeciwko Commission nationale de l'informatique et des libertés (CNIL), ECLI:EU:C:2019:773, pkt 35 oraz wyroku z 13 maja 2014 r., C-131/12, Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mariowi Costesze Gonzálezowi (wyrok Google 2), ECLI:EU:C:2014:317, a także wyroku ETPC z 28 czerwca 2018 r., skargi nr 60798/10 i 65599/10, M.L. i W.W. przeciwko Niemcom, HUDOC. Rada zauważyła, że w przypadku spełnienia warunków określonych w art. 17 ust. 1 RODO administrator ma, co prawda, obowiązek bez zbędnej zwłoki usunąć dane osobowe. Prawo to nie jest jednak prawem bezwzględnym. Wyłączenia ujęte w art. 17 ust. 3 RODO wskazują przypadki, w których obowiązek ten nie ma zastosowania. Jedną z okoliczności uzasadniających uchylenie się od obowiązku usunięcia danych jest potrzeba zachowania równowagi między ochroną praw zainteresowanych stron a wolnością wypowiedzi, w tym swobodnego dostępu do informacji. Jak TSUE wyjaśnił w wyroku w sprawie Google 2, art. 17 ust. 3 lit. a) RODO stanowi wyraz tego, iż „prawo do ochrony danych osobowych nie stanowi prawa bezwzględnego, lecz należy (...) je postrzegać w kontekście jego funkcji społecznej i wyważyć względem

O ile zatem postuluje się, jak wskazano wcześniej, usuwanie mowy nienawiści, a także sankcjonowanie rozpowszechniania fałszywych informacji (dezinformacji), to jednak postulat ten nie obejmuje co do zasady usuwania treści zniesławiających jednostkę. Naruszenie dobrego imienia, czci lub godności jednostki wypowiedzią wprowadzającą w błąd nie stanowi tym bardziej uzasadnionej podstawy do zastosowania środków ochrony *ex ante*, w szczególności polegających na blokowaniu dostępu do treści. Zastosowanie tych środków nie jest co prawda wyłączone, ale nie zawsze będzie uznane za niezbędne[193].

Objęcie terminem „nielegalne treści" wypowiedzi o charakterze zniesławiającym wymagać będzie zatem zindywidualizowanej oceny uwzględniającej okoliczności, w tym stopień szkodliwości danej wypowiedzi[194]. Dla oceny stopnia szkodliwości zniesławienia istotne znaczenie będzie mieć zarówno rozmiar naruszenia, jak i zastosowany przez sprawcę naruszenia

innych praw podstawowych w myśl zasady proporcjonalności" (sprawa C-136/17, pkt 57). Trybunał stwierdza, że „w przypadku gdy do operatora wyszukiwarki skierowano żądanie usunięcia linku do strony internetowej, na której są opublikowane dane osobowe należące do szczególnych kategorii danych (...) operator ten musi, na podstawie wszystkich istotnych elementów danego przypadku i uwzględniając powagę ingerencji w ustanowione w art. 7 i 8 karty prawa podstawowe do poszanowania życia prywatnego i ochrony danych osobowych przysługujące osobie, której dane dotyczą, sprawdzić, czy z uwagi na względy związane z ważnym interesem publicznym (...) umieszczenie takiego linku na wyświetlanej liście wyników wyszukiwania mającego za punkt wyjścia imię i nazwisko osoby, której dane dotyczą, jest ściśle niezbędne do ochrony prawa do wolności informacji przysługującego internautom potencjalnie zainteresowanym uzyskaniem, dzięki takiemu wyszukiwaniu, dostępu do tej strony internetowej, która to wolność jest chroniona na podstawie art. 11 KPP" (sprawa C-136/17, pkt 69) (zob. Wytyczne 5/2019 w sprawie kryteriów dotyczących prawa do bycia zapomnianym w sprawach dotyczących wyszukiwarek internetowych na podstawie RODO, przyjęte 7 lipca 2020 r., https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_pl; dostęp: 20 czerwca 2024 r.). Podobne stanowisko zajął rzecznik generalny UE M. Szpunar (zob. opinia rzecznika generalnego M. Szpunara przedstawiona w dniu 10 stycznia 2019 r., Dokument 62017CC0136, https://eur-lex.europa.eu/legal-content/pl/TXT/?uri=CELEX:62017CC0136, dostęp: 20 czerwca 2024 r.).

[193] Na gruncie aktualnego stanowiska, „jeżeli wydawca portalu internetowego lub strony internetowej nie chce odpowiadać za komentarze anonimowych internautów, które naruszają prawa innych osób, musi wdrożyć odpowiednie środki zapobiegawcze i zaradcze. Do środków takich należy możliwość sprawnego raportowania zniesławiających treści oraz niezwłoczne ich usuwanie przez administratora strony. W świetle spójnego orzecznictwa Trybunału, takie działanie zwalnia portal internetowy z odpowiedzialności za naruszenie dóbr osobistych, nawet jeżeli indywidualne dochodzenie roszczeń od anonimowych internautów przez osobę zainteresowaną będzie utrudnione (Høiness przeciwko Norwegii – wyrok ETPC z dnia 19 marca 2019 r., skarga nr 43624/14" (K. Warecka, *Strasburg: Portal nie odpowiada za komentarze internauty, jeżeli zostały niezwłocznie usunięte*, https://www.prawo.pl/prawo/komentarze-w-internecie-naruszajace-prawa-innych-osob-portal,388384.html, dostęp: 18czerwca 2024 r.).

[194] Zważywszy na szeroką definicję terminu „nielegalne treści" zawartą w art. 3 lit. h AUC, a także wykładnię zaproponowaną w motywie 12 AUC, nie można oczywiście zaprzeczyć, że zniesławienie stwierdzone prawomocnym orzeczeniem sądu stanowi wypowiedź, która ma charakter nielegalny. W motywie 12 AUC zaproponowano, by termin „nielegalne treści" 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". Uzyskanie prawomocnego rozstrzygnięcia odnośnie do zniesławienia może zatem stanowić podstawę domagania się usunięcia nieprawdziwej informacji z internetu. Podejrzenie zniesławienia zanim zapadnie prawomocne orzeczenie, w przeciwieństwie do innych treści nielegalnych, nie będzie jednak stanowiło skutecznej podstawy domagania się zablokowania dostępu do treści lub jej usunięcia.

mechanizm rozgłaszania treści zniesławiających (bombardowanie Google, *Googlewashing*, *coordinated/organized harm*) oraz charakter informacji zawartych w wypowiedzi (*sexual objectification*), a także intencje sprawcy (pornografia z zemsty)[195].

„Bombardowanie Google, Googlewashing oznacza działanie polegające na stosowaniu sugestywnych odesłań z użyciem hiperłączy (linków) oraz technik polegających na autouzupełnianiu wyników wyszukiwania przez przekierowanie na zniesławiające treści. Technika ta może polegać także na masowym linkowaniu (czyli dodawaniu linków do danej strony na innych stronach) przy pomocy odpowiednio przygotowanego anchor textu (tekstu, na który klika się, by przejść na inną stronę), będącego słowem kluczowym, pod jakim pozycjoner chce wysoko wypozycjonować stronę[196].

Na rozmiar zniesławienia i charakter zastosowanych środków ochrony może wpływać rodzaj zamieszczonych treści, w szczególności chodzi o treści, które uprzedmiotawiają przez zmanipulowane zdjęcia i dodane do nich opisy o charakterze jednoznacznie seksualnym. Fotografie są często wykorzystywane bez zgody osób na nich przedstawionych i manipulowane tak, aby pojawiały się w scenach pornograficznych lub były wykorzystywane w memach[197]. Działanie to przybiera formę nieautoryzowanego rozpowszechniania intymnych zdjęć (pornografia z zemsty). Sprawca uzyskuje zdjęcia lub filmy z wcześniejszego związku lub włamuje się do komputera, na konta w mediach społecznościowych lub telefon ofiary. Zwykle odbywa się to z zamiarem nękania, poniżania czy zranienia osoby.

Zniesławienie popełnione z wykorzystaniem nietypowych środków i treści może być kwalifikowane także jako inny typ przestępstwa. Skrajna forma działań nakierowanych na nękanie przez rozpowszechnienie nieprawdziwych informacji lub zmienionych (zmanipulowanych) obrazów, które są celowo wymierzone w osoby prywatne z zamiarem ich poniżenia lub zawstydzenia, jest nazywana „płomieniowaniem" (*flaming*). Wskazuje się, że powyższe okoliczności nie będą stanowić, co do zasady, znamienia bezprawności w stosunku do osób publicznych, od których oczekuje się, że będą tolerować wyższy poziom odporności na krytykę, o ile treści te nie zawierają mowy nienawiści ani wiarygodnych gróźb[198].

Opisane czynności mogą przybierać postać skoordynowanych, zorganizowanych działań (*coordinated/organized harm*). Ich celem jest sabotowanie aktywności komunikacyjnej ofiary lub wtargnięcie do wielu przestrzeni internetowych w celu jej nękania. Każda platforma ma przyjęte na własny użytek opisy zachowań uznawanych za niepożądane. Jednakże reakcja ze strony administratora dotyczy tylko tej części zmasowanej aktywności sprawcy naruszeń,

[195] Content & Jurisdiction Program..., s. 21.

[196] Przykładami Google bombingu było umieszczenie strony Andrzeja Leppera pod słowem kluczowym „kretyn" na górze wyników wyszukiwania oraz strony Radia Maryja pod frazą „siedziba szatana" (zob. *Google bombing lub Googlewashing*, https://www.i-slownik.pl/1909,google-bombing-googlewashing/, dostęp: 20 czerwca 2024 r.).

[197] Content & Jurisdiction Program..., s. 21.

[198] Content & Jurisdiction Program..., s. 23.

której skutki ujawniły się na platformie, którą on moderuje. W efekcie, jeżeli dochodzi do reakcji ze strony administratora, to reakcja ta obejmuje tylko nękanie, które ma miejsce na stronach konkretnego administratora i nie dotyczy innych miejsc w sieci[199].

3.3.5. Przemoc, nakłanianie, nękanie

Z reakcją prawa spotykają się popełnione w internecie za pomocą słowa, dźwięku lub obrazu czyny znamionowane jako przemoc, nakłanianie do przestępstwa, a także nękanie. Wypowiedzi stanowiące znamię czynu zabronionego oraz wypowiedzi, które ze względu na swoją treść lub formę odpowiadają opisowi czynu zabronionego (nękanie, groźba karalna, zniesławienie, znieważenie), są objęte zakresem definicji „nielegalne treści" zawartej w art. 3 lit. h AUC[200].

Nie dokonując szczegółowej analizy ani zamkniętego wyliczenia wypowiedzi, które ze względu na ich treść, formę lub zachowanie komunikacyjne autora wypowiedzi znamionują przemoc, nakłanianie do przestępstwa lub nękanie, należy wskazać na opisy niektórych zachowań wymienionych w dokumentach opracowanych na potrzeby organów europejskich, wobec których postuluje się przyjęcie jednolitej polityki reagowania (zbliżanie stanowisk, harmonizacja). Wskazuje się zatem, że wypowiedzi, które należy kwalifikować jako karygodne, przybierają postać nękania (*harassment*), cyberstalkingu, nieautoryzowanego posługiwanie się cudzym nazwiskiem rodowym (*deadnamin*), uporczywego naruszania prywatności (*doxing*), szantażu, wymuszenia (*blackmail/extortion*), organizowania przemocy (*content to organize violence* lub *support violent organizations*), epatowania treściami drastycznymi (*violent/graphic content*), a także podżegania do samookaleczenia lub samobójstwa (*abetting self-harm or suicide*).

Przemoc na gruncie doktryny prawa karnego to zarówno użycie siły fizycznej bezpośrednio wobec osoby, jak i przemoc, która może być skierowana na rzecz i stanowić środek do zmuszenia w ten sposób osoby do określonego zachowania. Zachowanie się sprawcy polegające na stosowaniu przemocy może przybrać postać przymusu fizycznego (*vis absoluta*), a także przymusu psychicznego (*vis compulsiva*). Przemocą są wszelkie jej przejawy, które „powodują lub mogą prowadzić do psychologicznej szkody lub cierpienia", „wszelkie akty przemocy psychologicznej", a także przemoc, która może obejmować „przemoc psychologiczną i może powodować uraz psychiczny, cierpienie moralne bądź emocjonalne"[201]. Z kolei

[199] Content & Jurisdiction Program..., s. 23.

[200] Prawodawca europejski definiuje treści nielegalne w art. 3 lit. h AUC 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".

[201] Uchwała SN z 31 marca 2021 r., I KZP 7/20, OSNK 2021, nr 6, poz. 23.

przestępstwem z użyciem przemocy jest każde przestępstwo, które faktycznie popełniono z użyciem przewagi fizycznej lub psychicznej.

Na gruncie polskiego prawa karnego przez nękanie należy rozumieć wielokrotne prześladowanie wyrażające się w podejmowaniu różnych naprzykrzających się czynności, których celem jest udręczenie, utrapienie, dokuczenie lub niepokojenie pokrzywdzonego lub osoby najbliższej[202]. Aby wyczerpać znamiona tego czynu, sprawca może podejmować działania legalne, np. wysyłać listy, wiadomości tekstowe, czy nachodzić w miejscach pracy. Zachowania mogą przybrać również postać zachowań nielegalnych, jak w szczególności rozpowszechnianie nieprawdziwych lub przykrych informacji godzących w cześć lub dobre imię. O uporczywym zachowaniu świadczyć będzie z jednej strony szczególne nastawienie psychiczne, wyrażające się w nieustępliwości nękania, tj. trwaniu w swego rodzaju uporze, mimo próśb i upomnień pochodzących od pokrzywdzonego lub innych osób o zaprzestanie przedmiotowych zachowań, z drugiej strony – dłuższy upływ czasu, przez który sprawca je podejmuje[203]. Zarazem dla odpowiedzialności karnej za uporczywe nękanie nie ma znaczenia cel działania sprawcy, który sam w sobie nie musi być społecznie naganny[204].

Skutkiem działania sprawcy jest ugodzenie w sferę prywatności, prowadzące do zakłócenia spokoju i poczucia bezpieczeństwa ofiary. Wypowiedź (werbalna, niewerbalna) stanowi zazwyczaj widoczny przejaw działania sprawcy, a zarazem w odniesieniu do niektórych rodzajów występków (np. groźba karalna, nękania) stanowi element czynności sprawczej czynu. Na gruncie prawa karnego zarówno nękanie, jak i stosowanie przemocy, a także nakłanianie mogą następować z użyciem wypowiedzi, w tym słowa, dźwięku lub obrazu. Wypowiedź przybierająca formę kwalifikowaną, tj. odpowiadającą opisowi znamienia występku opisanego w przepisach prawa karnego, przesądza o jej skategoryzowaniu jako „treści nielegalnej", a w konsekwencji wymagającej usunięcia z przestrzeni debaty publicznej.

W dokumentach UE i RE odnoszących się do granic wolności wypowiedzi wskazuje się, że naruszenie standardu tej wolności następuje zawsze wtedy, gdy wypowiedź stanowi nakłanianie do przemocy. Nie jest jednak jasne, czy nawoływanie do przemocy należy uznawać za konieczne znamię mowy nienawiści, czy też stanowi odrębną kategorię nielegalnych treści. Cechą mowy nienawiści jest to, jak wynika z analizy orzecznictwa ETPC przeprowadzonej przez J. Sobczaka i K. Kakareko, „iż towarzyszy jej zamiar podżegania lub można racjonalnie oczekiwać, iż przyniesie skutek w postaci podżeganie innych osób do popełnienia czynu z udziałem przemocy, zastraszania, wrogości lub dyskryminacji osób, w które jest wymie-

[202] Wyrok Sądu Okręgowego w Warszawie z 18 lipca 2019 r., IX Ka 640/19, LEX nr 2747784. Uporczywe nękanie sankcjonuje art. 190a § 1 ustawy z 6 lipca 1997 r. – Kodeks karny (tekst jedn. Dz.U. z 2024 r. poz. 17). Zgodnie z tym przepisem: „Kto przez uporczywe nękanie innej osoby lub osoby dla niej najbliższej wzbudza u niej uzasadnione okolicznościami poczucie zagrożenia, poniżenia lub udręczenia lub istotnie narusza jej prywatność, podlega karze pozbawienia wolności od 6 miesięcy do lat 8".

[203] Wyrok Sądu Okręgowego w Warszawie z 18 lipca 2019 r., IX Ka 640/19.

[204] Wyrok SN z 2 grudnia 2020 r., III KK 266/20, OSNKW 2021, nr 1, poz. 3.

rzona. Wskazano, że element podżegania pociąga za sobą istnienie wyraźnego zamiaru spowodowania czynów z udziałem przemocy" [205]. Zarazem podżeganie do nienawiści niekoniecznie przy tym sprowadza się do wzywania do dokonania czynów z wykorzystaniem przemocy lub innych czynów zagrożonych karą[206].

Europejska Komisja przeciw Rasizmowi i Nietolerancji (*European Commission against Racism and Intolerance*, ECRI) zaleca, aby prawo kryminalizowało następujące czyny, gdy są one popełniane umyślnie:

1) publiczne nakłanianie do przemocy, nienawiści czy dyskryminacji;
2) publiczne znieważanie i zniesławianie;
3) groźby kierowane w stosunku do osoby bądź grupy osób z powodu ich rasy, koloru skóry, języka, religii, narodowości czy pochodzenia narodowego lub etnicznego;
4) publiczne wyrażanie w rasistowskim celu ideologii wywyższania się bądź takiej, która deprecjonuje, czy oczernia grupę osób z powodu ich rasy, koloru skóry, języka, religii, narodowości, pochodzenia narodowego czy etnicznego;
5) publiczne zaprzeczanie, bagatelizowanie, usprawiedliwianie czy rozgrzeszanie w celu rasistowskim ze zbrodni ludobójstwa, zbrodni przeciwko ludzkości czy zbrodni wojennych[207].

Rekomendacja Rec (2022)16 z 20 maja 2022 r. w sprawie zwalczania mowy nienawiści[208] wskazuje w § 11, że sankcjonowanymi w prawie krajowym państw członkowskich przejawami mowy nienawiści powinny być:

1) publiczne nawoływanie do ludobójstwa, zbrodni przeciwko ludzkości lub zbrodni wojennych;
2) publiczne nawoływanie do nienawiści, przemocy lub dyskryminacji;
3) groźby rasistowskie, ksenofobiczne, seksistowskie i związane z niechęcią wobec osób LGBTI;
4) publiczne zniewagi na tle rasistowskim, ksenofobicznym, seksistowskim i związane z niechęcią wobec osób LGBTI, na warunkach określonych specjalnie dla zniewag internetowych w Protokole dodatkowym do Konwencji Rady Europy o cyberprzestępczości dotyczącym penalizacji czynów o charakterze rasistowskim lub ksenofobicznym popełnionych przy użyciu systemów komputerowych, sporządzonym w Strasburgu 28 stycznia 2003 r.[209];

---

[205] J. Sobczak, K. Kakareko, *Przeciwdziałanie*..., s. 45.

[206] J. Sobczak, K. Kakareko, *Przeciwdziałanie*..., s. 47.

[207] Zalecenie nr 12 dotyczące ogólnej polityki ECRI w sprawie zwalczania rasizmu i dyskryminacji rasowej w sporcie (przyjęte w dniu 19 grudnia 2008 r.), dostępne na https://www.gov.pl/web/dyplomacja/ecri (dostęp: 20 czerwca 2024 r.).

[208] Zob. https://rm.coe.int/prems-083822-gbr-2018-recommendation-on-combating-hate-speech-memorand/1680a710c9 (dostęp: 20 czerwca 2024 r.).

[209] Dz.U. z 2015 r. poz. 730.

5) publiczne zaprzeczanie, trywializowanie i aprobowanie ludobójstwa, zbrodni przeciwko ludzkości lub zbrodni wojennych;
6) celowe rozpowszechnianie materiałów zawierających przejawy mowy nienawiści, wymienionych w pkt 1–5, w tym idei opartych na wyższości rasowej lub nienawiści[210].

Nękanie jest opisywane jako rozpowszechnianie przy wielu okazjach treści w celu wywołania u danej osoby stresu, upokorzenia, niepokoju lub strachu przed przemocą[211]. Treści mogą zawierać ukierunkowane przekleństwa, rażąco obraźliwe komentarze lub groźby obrażeń fizycznych, a nawet śmierci (*harassment*). W odniesieniu do cyberstalkingu karygodność zachowania odnosi się do czynności polegającej na powtarzalnym rozsyłaniu wiadomości, w szczególności e-maili lub wiadomości tekstowych z pogróżkami bądź zawierających obsceniczne treści, a także *flaming* (ukierunkowane obelgi słowne online), nękanie poprzez drwiny lub wysyłanie gróźb w niechcianych wiadomościach.

Deadnaming jako forma nękania polega na używaniu lub ujawnianiu nazwiska rodowego osoby transpłciowej w celu jej wyśmiania ze względu na tożsamość oraz wywołania tzw. stresu emocjonalnego[212]. *Doxing* oznacza wyszukiwanie i publikowanie prywatnych lub prowadzących do łatwej identyfikacji informacji o konkretnej osobie, często przez przełamywanie zabezpieczeń, używanie haseł w sposób nieuprawniony. „Dox" to slangowa wersja słowa „dokumenty". Wywoływanie strachu, stresu i paniki jest celem doxingu, nawet jeśli sprawcy myślą, że ujawnienie dokumentu samo w sobie nie stanowi czynu bezprawnego[213].

Nadużyciem wolności wypowiedzi jest także wiadomość wysyłana z zamiarem wymuszenia na adresacie niekorzystnego dla niego zachowania (szantaż). Chodzi o przesyłanie prywatnych wiadomości, w których zawarta zostaje groźba ujawnienia kłopotliwych informacji lub zdjęć ofiary zebranych nielegalnie lub za zgodą ofiary[214].

Za nielegalne mogą zostać uznane także treści krytyczne wobec religii (bluźnierstwo/apostazja), jednakże tylko wówczas, gdy autor nawołuje do nienawiści religijnej i podżega do dyskryminacji, wrogości lub przemocy wobec jej wyznawców[215].

Treści drastyczne i brutalne, jeśli są sensacyjne, a ich brutalność nie jest uzasadniona albo gloryfikują przemoc, będą uznawane za niezasługujące na ochronę. Treści, które podżegają do działalności przestępczej, są uważane za zagrażające bezpieczeństwu publicznemu[216]. Podobnie ocenione zostaną wypowiedzi mające na celu organizowanie przemocy lub wspieranie organizacji stosujących przemoc, w tym treści, które zawierają wiarygodne groźby wyrządzenia poważnej krzywdy fizycznej (przemoc zorganizowana, morderstwo, handel

[210] Zob. J. Sobczak, K. Kakareko, *Przeciwdziałanie*..., s. 69.
[211] Content & Jurisdiction Program..., s. 22.
[212] Content & Jurisdiction Program..., s. 23.
[213] Content & Jurisdiction Program..., s. 23.
[214] Content & Jurisdiction Program..., s. 25.
[215] Content & Jurisdiction Program..., s. 22.
[216] Content & Jurisdiction Program..., s. 23.

ludźmi) konkretnej osobie lub określonej grupie osób lub wyrażają poparcie lub pochwałę dla grup, liderów lub osób zaangażowanych w te działania (*content to organize violence or support violent organizations*). Podobna ocena dotyczy treści podżegających do samookaleczenia lub samobójstwa. Są one uznawane za promujące szkodliwe zachowania, takie jak okaleczanie, zaburzenia odżywiania lub nadużywanie narkotyków. W podobny sposób zostaną ocenione treści, które identyfikują ofiary lub osoby, które przeżyły samookaleczenie lub samobójstwo (*abetting self-harm or suicide*)[217].

3.4. Rola Komisji Europejskiej

W AUC wskazano, że przyjęte w UE rozwiązania prawne zawarte w tym akcie i akcie o rynkach cyfrowych stanowią pełną harmonizację prawa. Celem harmonizacji jest zapewnienie bezpiecznego, przewidywalnego i budzącego zaufanie środowiska internetowego, przeciwdziałanie rozpowszechnianiu nielegalnych treści w internecie oraz zagrożeniom społecznym, jakie może stwarzać rozpowszechnianie dezinformacji (art. 1 AUC). W rezultacie – o ile nie jest to wyraźnie przewidziane w AUC – państwa członkowskie nie powinny przyjmować lub utrzymywać w mocy dodatkowych wymogów krajowych w odniesieniu do spraw objętych zakresem rozporządzeń cyfrowych (AUC i ARC), ponieważ miałoby 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 funkcję regulatora, korzystając z szerokich uprawnień do wydawania aktów delegowanych, co miałoby stanowić reakcję na zmieniające się uwarunkowania funkcjonowania rynków cyfrowych i pojawiające się nowe zagrożenia, jak również korzysta z szerokich uprawnień kontrolnych i nadzorczych. W celu wykonywania tych uprawnień KE może, a niekiedy ma obowiązek korzystać z wyników ustaleń dokonanych przez specjalnie do tego utworzony organ, tj. Europejską Radę ds. Usług Cyfrowych. Rada została określona w AUC jako niezależna grupa doradcza na poziomie unijnym (art. 61 ust. 1 AUC) której zadaniem jest udzielanie wsparcia i pomocy Komisji. Rada 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 będą zarazem wykonywać zadania punktów kontaktowych, a państwa członkowskie są zobowiązane do zapewnienia im

[217] Content & Jurisdiction Program..., s. 24.

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 135 AUC). Wyposażenie w wiedzę ekspercką powinno zapewniać Komisji i Radzie Obserwatorium Gospodarki Platform Internetowych utworzone na mocy decyzji Komisji z 26 kwietnia 2018 r. (motyw 137 ACU). Komisji Europejskiej zostały powierzone zadania w zakresie wdrażania i zapewniania skuteczności i elastyczności rozwiązań przyjętych w rozporządzeniach cyfrowych, w tym przez wydawanie aktów delegowanych (motyw 152 AUC), a także kontroli, nadzoru oraz egzekwowania i monitorowania wykonania przepisów na szczeblu UE. Komitet Regionów poparł wniosek, by monitorowanie egzekwowania przepisów rozporządzeń cyfrowych (AUC i ARC) powierzyć KE[218]. Przykładem powierzenia KE poważnych instrumentów kontrolnych jest nadanie jej uprawnienia dostępu do baz danych i algorytmów dowolnego organu publicznego, podmiotu, agencji, osoby fizycznej lub osoby prawnej (motyw 141 AUC)[219].

Komisja jest zatem – na gruncie rozwiązań przyjętych w AUC i ARC – organem centralnym wyposażonym w funkcje normodawcze, kontrolne, 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 tej kompetencji 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 dotyczących 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 kompetencji niezastrzeżonych dla KE (kompetencje dzielone), „Komisja powinna oceniać, czy w danym przypadku uważa za

[218] Opinia Europejskiego Komitetu Regionów – Akt o usługach cyfrowych i akt o rynkach cyfrowych, (Dz.Urz. UE C 440 z 2021 r., s. 67), pkt 16.

[219] G. Bar, R. Skibicki, *Wyzwania prawne związane z wykorzystaniem sztucznej inteligencji w usługach cyfrowych*, „Prawo Nowych Technologii" 2021, nr 1, s. 40.

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".

Ponadto w art. 56 ust. 5 AUC państwa członkowskie zobowiązano do „ścisłej 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, posiadały 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 potwierdzono istnienie kompetencji państw członkowskich, to jednak ich wykonywanie także zostało poddane kontroli organów europejskich, w tym Komisji Europejskiej. Nie jest bez znaczenie, że ograniczenia te mogą wynikać także z zastosowanej przez KE i PE metody regulacyjnej, tj. harmonizacji pełnej. Nawet zatem, 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.

3.5. Rola strażników dostępu

Niezależnie od różnorodności podejść do sposobu, metod i zakresu definiowania nieodpowiednich (nielegalnych) treści, skutek faktyczny polegający na usunięciu, zablokowaniu dostępu do treści albo jej ograniczeniu w internecie powstaje nie tyle ze względu na zastosowanie

sądowego nakazu wprowadzenia takiego ograniczenia, ile ze względu na arbitralne decyzje podejmowane przez podmioty prywatne, w szczególności pośredników internetowych, na podstawie przyjętych u nich regulaminów i polityk. Dostawcy usług opracowują bowiem coraz bardziej szczegółowe – i często aktualizowane – warunki korzystania z usługi i wytyczne dla społeczności, określające zasady mające zastosowanie do ich przestrzeni internetowych. Niektóre z tych zasad są specyficzne dla konkretnej społeczności, której usługa ma służyć, ale niektóre są bardziej ogólne. Biorąc pod uwagę znaczącą rolę, jaką odgrywają główni operatorzy w ekosystemie, globalne stosowanie tych norm bezpośrednio wpływało na to, jakie treści są uznawane za legalne, a jakie nie w cyberprzestrzeni jako całości[220].

O ile w przestrzeni pozawirtualnej kluczowymi kwestiami dotyczącymi wolności wypowiedzi była możliwość stosowania ograniczonych terytorialnie przepisów krajowych oraz odpowiednie procedury wydawania przez organy publiczne nakazów i sposób, w jaki adresaci tych nakazów powinni na nie reagować, o tyle w internecie zasadnicze znaczenie dla wyznaczania granic swobody wypowiedzi uzyskały decyzje prywatnych podmiotów podejmowane w oparciu o ustanawiane przez te podmioty własne, cechujące się dużym stopniem arbitralności i uznania, zasady oceny. Mechanizmy, za pomocą których podmioty prywatne ograniczają treści zgodnie z ich własnymi przepisami, stały się zagadnieniem wymagającym nowego podejścia regulacyjnego do wolności wypowiedzi oraz wytyczania jej granic.

Terminu „strażnicy dostępu" Komisja Europejska użyła w treści wniosku do Parlamentu Europejskiego z 12 grudnia 2020 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym (akt o rynkach cyfrowych ARC). 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 zatem rynek „potencjalnie konkurencyjny"[221]. 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"[222]. 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 wejść[223]. Warunkiem kontestowalności rynku są niskie koszty utopione[224].

---

[220] Zob. Opinia Europejskiego Komitetu Regionów...

[221] Zob. https://encyklopedia.pwn.pl/haslo/rynek-kontestowalny;3970469.html (dostęp: 20 czerwca 2024 r.).

[222] Zob. https://encyklopedia.pwn.pl/haslo/rynek-potencjalnie-konkurencyjny;3970477.html (dostęp: 20 czerwca 2024 r.).

[223] N.G. Mankiw, M.P. Taylor, *Mikroekonomia*, Warszawa 2022, s. 528, cyt. za: https://pl.wikipedia.org/wiki/Rynek_kontestowalny#cite_note-2 (dostęp: 20 czerwca 2024 r.).

[224] N.G. Mankiw, M.P. Taylor, *Mikroekonomia*..., s. 740, cyt. za: https://pl.wikipedia.org/wiki/Koszty_utopione#cite_note-1 (dostęp: 20 czerwca 2024 r.).

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 wejścia[225].

Istotne stało się zatem nie tylko ustalenie przesłanek dopuszczalności ograniczenia wolności wypowiedzi, ale rozstrzygnięcie, w jakim zakresie podmioty prywatne, a także jakie spośród nich i kiedy, mogą legalnie wkraczać (ingerować) w sferę wolności wypowiedzi obywateli. Nadto istotne stało się ustalenie, czy działania podmiotów prywatnych polegające na ograniczeniu wolności wypowiedzi użytkowników internetu (usługobiorców) należy definiować jako podejmowane w interesie publicznym, a jeśli tak, czy działania te mogą korzystać z domniemania zgodności z prawem oraz w odniesieniu do jakich kategorii wypowiedzi.

Strażnikami dostępu zostały nazwane podmioty świadczące podstawowe usługi platformowe, jeżeli podmioty te:

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 działalności[226].

Wszystkie wskazane 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) internetowe serwisy społecznościowe;
4) usługi platformy udostępniania wideo;
5) usługi łączności interpersonalnej niewykorzystujące numerów;
6) systemy operacyjne;
7) usługi przetwarzania 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

[225] Zob. Opinia Europejskiego Komitetu Regionów...
[226] Art. 3 ust. 1 lit. a–c ARC.

związane co najmniej z jedną z pozostałych podstawowych usług platformowych wymienionych powyżej[227].

Strażnikiem dostępu są podmioty, które „obsługują co najmniej jeden istotny punkt dostępu"[228]. 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).

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). Środki, jakie strażnik dostępu wdraża, aby zapewnić przestrzeganie obowiązków polegających na przeciwdziałaniu nielegalnym treściom, muszą skutecznie przyczyniać się do osiągnięcia celów rozporządzenia[229] i celu, w jakim ustanowiono dany obowiązek (art. 8 ust. 1 ARC). Przepisy art. 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 ARC), zmienić lub ograniczyć obowiązki nałożone na strażnika, a także zwolnić strażnika z realizacji obowiązków wskazanych w decyzji o wyznaczeniu (art. 10 ust. 1 ARC). Zwolnienia można udzielić wyłącznie ze względów zdrowia publicznego lub bezpieczeństwa publicznego (art. 10 ust. 3 ARC).

Strażnicy dostępu są adresatami norm zawartych w rozporządzeniach cyfrowych, w szczególności w akcie o rynkach cyfrowych (ARC), a zarazem stali się stronami prowadzonego z organami UE dialogu regulacyjnego oraz – w konsekwencji – kooperantami Komisji Europejskiej w sprawach dotyczących zwalczania nielegalnych treści. O ile zatem definiowanie terminu „nielegalne treści" należy do wyłącznych kompetencji organów UE, w tym Komisji

[227] Art. 2 pkt 2 ARC.

[228] Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym (akt o rynkach cyfrowych), COM/2020/842 final, s. 2 https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020PC0842 (dostęp: 20 czerwca 2024 r.).

[229] 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 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).

Europejskiej, o tyle realizacja celów związanych z wykrywaniem i usuwaniem nielegalnych treści oraz stosowaniem środków przeciwdziałania rozpowszechnieniu nielegalnych treści, w tym środków *ex ante*, została powierzona strażnikom dostępu. W pewnym uproszczeniu można przyjąć, że strażnicy dostępu wykonują na rzecz organów UE usługę, której przedmiotem jest monitorowanie wolności wypowiedzi w internecie i reagowanie na nielegalne treści w zamian za możliwość uchylenia się przez strażników dostępu od odpowiedzialności za naruszenia prawa spowodowane rozpowszechnieniem w Internecie materiałów ze względu na ich formę lub treść (art. 4–6 AUC w zw. z art. 7 AUC).

4. Zakończenie

Realizowany w państwach członkowskich UE po przyjęciu pakietu cyfrowego (AUC i ARC) model zarządzania internetem[230] dokonuje zmiany zasad reagowania na nadużycia wolności wypowiedzi przez legitymizowanie środków prewencyjnych (*ex ante*), a także przez uzupełnienie przesłanek legalizujących ingerencję w wolność wypowiedzi. Unia Europejska przyjęła koncepcję „współzarządzania" internetem w ramach dialogu regulacyjnego prowadzonego z podmiotami prywatnymi, w szczególności dostawcami usług pośrednich, w tym strażnikami dostępu. Przyjęty model skłonił UE do zaakceptowania aktywności kontrolnej (monitoring, filtrowanie) realizowanej przez podmioty prywatne i przesądził o udzieleniu 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). Wykorzystanie tych instrumentów w celu stworzenia „bezpiecznego, przewidywalnego i budzącego zaufanie środowiska internetowego" (art. 1 ust. 1 AUC) zostało przewidziane w pakiecie cyfrowym. Zawarte tam rozwiązania stanowią realizację postulatów wypowiadanych w judykatach ETPC i TSUE w reakcji na zmieniający się model komunikowania oraz poszerzenie wpływu, jaki na procesy komunikacji mają dostawcy usług pośrednich, w szczególności strażnicy dostępu.

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 polegających na przyjęciu domniemania szkodliwości niektórych kategorii wypowiedzi i potrzebie ich eliminowania z debaty publicznej.

[230] Komunikat KE COM/2014/072, pkt 5.

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) legitymowanie ograniczenia wolności wypowiedzi *ex ante*;
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 *versus* 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) modyfikacja przesłanek legalizujących ingerencję w wolność wypowiedzi zarówno przez poszerzenie ich katalogu, jak i zmianę o charakterze jakościowym.

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

Bibliografia

Andrzejczak H., *Filozoficznoprawne podstawy Powszechnej Deklaracji Praw Człowieka*, „Roczniki Filozoficzne" 1966, t. 14, z. 2.

Bar G. [w:] *Akt o usługach cyfrowych. Komentarz*, red. D. Lubasz, M. Namysłowska, Warszawa 2024.

Bar G., Skibicki R., *Wyzwania prawne związane z wykorzystaniem sztucznej inteligencji w usługach cyfrowych*, „Prawo Nowych Technologii" 2021, nr 1.

Cydzik S., *Kto i jak ma pilnować wykonania konstytucji internetu*, https://www.rp.pl/internet-i-prawo-autorskie/art40009831-kto-i-jak-ma-pilnowac-wykonania-konstytucji-internetu (dostęp: 20 czerwca 2024 r.).

Dan Jerker B. Svantesson, *Internet & Jurisdiction Global Status Report 2019*, https://www.internetjurisdiction.net/uploads/pdfs/GSR2019/Internet-Jurisdiction-Global-Status-Report-2019_web.pdf (dostęp: 20 czerwca 2024 r.).

Gliszczyńska-Grabias A. [w:] *Międzynarodowy pakt praw obywatelskich (osobistych) i politycznych. Komentarz*, red. R. Wieruszewski, Warszawa 2012.

Jurczyk T., *Prawa jednostki w orzecznictwie Europejskiego Trybunału Sprawiedliwości*, Warszawa 2009.

Kamiński I.C., *Mowa nienawiści – pojęcie i jego zakres* [w:] *Prawna kwalifikacja mowy nienawiści. Krajowe i europejskie uwarunkowania nadużycia wolności wypowiedzi*, red. J. Taczkowska-Olszewska, Warszawa 2024.

Kamiński I.C., *Ograniczenia swobody wypowiedzi dopuszczalne w Europejskiej Konwencji Praw Człowieka. Analiza krytyczna*, Warszawa 2010.

Kamuda D., Policeusz M. , *Cyberprzestępstwa a zagrożenie bezpieczeństwa RP – zagadnienia wybrane* [w:] *Przestępczość XXI wieku. Zapobieganie i zwalczanie. Problemy technologiczno-informatyczne*, red. E.W. Pływaczewski, W. Filipkowski, Z. Rak ,Warszawa 2015.

Konarski X., *Wzajemna relacja RODO i Aktu w sprawie sztucznej inteligencji – 10 najważniejszych informacji*, https://www.traple.pl/wzajemna-relacja-rodo-i-aktu-w-sprawie-sztucznej-inteligencji-10-najwazniejszych-informacji/ (dostęp: 20 czerwca 2024 r.).

Kotuła Z., *Protokół 15 do europejskiej konwencji praw człowieka: doktryna marginesu swobody uznania i zasada subsydiarności w kontekście reformy ETPCz*, „Studenckie Prace Prawnicze, Administratywistyczne i Ekonomiczne" 2015, t. 17.

Lent B., *Bezpieczeństwo w telekomunikacji i teleinformatyce*, Warszawa 2007.

Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2008.

Liedel K., *Cyberbezpieczeństwo – wyzwania przyszłości. Działania społeczności międzynarodowej* [w:] *Bezpieczeństwo w XXI wieku. Asymetryczny świat*, red L. Liedel, P. Piasecka, T.R. Aleksandrowicz, Warszawa 2011.

Malicious Actors Manipulating Photos and Videos to Create Explicit Content and Sextortion Schemes, https://www.ic3.gov/Media/Y2023/PSA230605 (dostęp: 20 czerwca 2024 r.).

Małobęcka-Szwast I. [w:] *Rynek cyfrowy. Akt o usługach cyfrowych. Akt o rynkach cyfrowych. Rozporządzenie platform-to-business. Komentarz*, red. M. Grochowski, Warszawa 2024.

Mankiw N.G., Taylor M.P. M.P., *Mikroekonomia*, Warszawa 2022.

Mikoś A., *Konstytucja internetu*, https://informacjapubliczna.org/news/konstytucja-internetu/ (dostęp: 20 czerwca 2024 r.).

Morawski Ł., *Unia Europejska wobec procesu zarządzania internetem*, „TEKA of Political Science and International Relations" 2016, nr 3.

Motyka J., *50 lat minęło. Powszechna Deklaracja Praw Człowieka i jej credo*, „Prawo i Życie" 1998, nr 39.

Motyka J., *Prawa człowieka. Wprowadzenie. Wybór źródeł*, Lublin 2004.

Nowakowski Z., Pomykała M., Rajchel J., *Pojęcie bezpieczeństwa i porządku publicznego* [w:] *Administracja bezpieczeństwa i porządku publicznego ze szczególnym uwzględnieniem aspektów prawno-organizacyjnych Policji*, red. K. Rajchel, Warszawa 2009.

Ost F., van de Kerchove M., *De la pyramide au réseau? Pour une théorie dialectique du droit*, Facultés universitaires Saint-Louis Bruxelles, 2002.

Polański P., *Europejskie prawo handlu elektronicznego. Mechanizmy regulacji usług społeczeństwa informacyjnego*, Warszawa 2014.

Sobczak J. [w:] *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, red. A. Wróbel, Warszawa 2020.

Sobczak J., Kakareko K., *Przeciwdziałanie mowie nienawiści w międzynarodowych aktach normatywnych* [w:] *Prawna kwalifikacja mowy nienawiści. Krajowe i europejskie uwarunkowania nadużycia wolności wypowiedzi*, red. J. Taczkowska-Olszewska, Warszawa 2024.

Taczkowska-Olszewska J., *Bezpieczeństwo informacyjne jako kategoria prawna. Ujęcie teoretyczne* [w:] *Bezpieczeństwo informacyjne. Aspekty prawno-administracyjna*, red. W. Kitler, J. Taczkowska-Olszewska, Warszawa 2017.

Taczkowska-Olszewska J., *Racjonalizacja wolności prasy – od modelu absolutnego do warunkowego, Europejski i krajowy kontekst wykładni prawa*, „Przegląd Sejmowy" 2018, nr 1(144).

Warecka K., *Strasburg: Portal nie odpowiada za komentarze internauty, jeżeli zostały niezwłocznie usunięte*, https://www.prawo.pl/prawo/komentarze-w-internecie-naruszajace-prawa-innych-osob-portal,388384.html (dostęp: 20 czerwca 2024 r.).

Wchodzi w życie konstytucja internetu. Oto co się zmieni, https://www.money.pl/gospodarka/wchodzi-w-zycie-konstytucja-internetu-oto-co-sie-zmieni-6996220038113952a.html (dostęp: 20 czerwca 2024 r.).

Weitzenboeck E., *Hybrid net: the regulatory framework of ICANN and the DNS*, „International Journal of Law and Information Technology" 2014, nr 22(1).

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

Zieliński M., *Wykładnia prawa. Zasady – reguły – wskazówki*, Warszawa 2002.