INSTYTUT WYMIARU SPRAWIEDLIWOŚCI

dr Konrad Buczkowski

Prawnokarna problematyka ochrony danych osobowych

Warszawa 2015

Spis treści

Wprowadzenie

Postęp technologiczny umożliwia coraz łatwiejszy i coraz szerszy dostęp do danych osobowych o bardzo różnym charakterze: od bardzo podstawowych, jak imię i nazwisko, miejsce zamieszkania, data urodzenia, imiona rodziców, numery identyfikacyjne, do takich, które identyfikują osobę poprzez jej zainteresowania, rodzaj zakupów przez nią dokonywanych, krąg posiadanych znajomych, wyznanie czy orientację seksualną. Na pozyskanie tych danych zainteresowani w wielu przypadkach sami wyrażają zgodę, bowiem możliwość skorzystania przez nich z szeregu usług uzależniona jest od udzielenia zezwolenia na dostęp do określonych informacji o osobie. W przypadku części danych pozyskiwane mogą być one w sposób nielegalny (np. programy szpiegujące) lub naruszający obowiązujące przepisy w zakresie dozwolonego wykorzystywania danych osobowych.

Nieuprawnione posłużenie się danymi osobowymi innej osoby stanowi naruszenie, uznanego w Karcie Praw Podstawowych Unii Europejskiej [1], jednego z podstawowych praw człowieka.

Art. 8 Karty przyznaje każdemu prawo do ochrony danych, które go dotyczą. Dane te muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Każdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania. Ponadto przestrzeganie tych zasad podlega kontroli niezależnego organu, w tym do skutecznego środka prawnego przed sądem (art. 47 Karty).

Uszczegółowienie tej zasady – na poziomie wspólnotowym – wprowadzają przepisy Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[2].

---

[1] Karta Praw Podstawowych Unii Europejskiej (2010/C 83/02), Dz. Urz. UE Nr C83/389 z 30.3.2010 r.

[2] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz. Urz WE Nr L 281/31 z 23.11.1995 z późn. zm.; Dz. Urz. UE Polskie wydanie specjalne, rozdz. 13, t. 15, str. 355, z późn. zm.).

Na marginesie należy wspomnieć o trwających pracach nad nową dyrektywą w zakresie ochrony danych osobowych. Ma ona realizować trzy podstawowe cele: 1) opracowanie ogólnoeuropejskiej

W preambule Dyrektywy stwierdza się, że „systemy przetwarzania danych są tworzone po to, aby służyły człowiekowi; muszą one, niezależnie od obywatelstwa czy miejsca stałego zamieszkania osób fizycznych, szanować ich podstawowe prawa i wolności, szczególnie prawo do prywatności, oraz przyczyniać się do postępu gospodarczego i społecznego, rozwoju handlu oraz dobrobytu jednostek."

Dyrektywa ta wprowadza minimalne standardy dla państw członkowskich, zobowiązujące je do przyjęcia na poziomie krajowym rozwiązań umożliwiających osobom fizycznym dochodzenie roszczeń[3].

Art. 24 Dyrektywy zobowiązuje Państwa Członkowskie do wprowadzenia odpowiednich środków w celu zapewnienia pełnej realizacji przepisów dyrektywy oraz w szczególności do określenia sankcji, jakie należy nałożyć w przypadku naruszenia przepisów przyjętych zgodnie z dyrektywą.

W następstwie postanowień Dyrektywy wykształciły się w Unii Europejskiej trzy systemy ochrony danych osobowych:

- administracyjny – z udziałem krajowego organu ochrony danych osobowych,
- cywilnoprawny – w ramach postępowania o ochronę dóbr osobistych,
- prawnokarny – w oparciu o przepisy prawa karnego[4].

W dużej grupie państw UE system sankcji oparto na rożnego rodzaju karach pieniężnych – nakładanych przez krajowy organ ochrony danych osobowych – występujących bądź samodzielnie, jako jedyne sankcje przewidziane przez krajowe

regulacji w zakresie ochrony danych osobowych, obowiązujących we wszystkich krajach Unii Europejskiej („one continent – one law"), 2) zgłaszanie przez przedsiębiorców baz danych tylko do jednego organu powołanego do nadzoru nad przestrzeganiem przepisu, brak konieczności zgłoszeń do takich organów we wszystkich państwach, w których przedsiębiorca prowadzi działalność („one-shop-stop"), 3) te same prawa dla wszystkich przedsiębiorców, niezależnie od formy ich utworzenia („The same rules for all companies – regardless of their establishment"). Dyrektywa powinna zacząć obowiązywać od roku 2017 lub 2018. Zob. http://europa.eu/rapid/press-release_MEMO-14-186_en.htm

[3] Zob. D. Głowacka, Dostęp do mechanizmów ochrony danych osobowych w krajach UE – wnioski z raportu Agencji Praw Podstawowych Unii Europejskiej, dodatek do Monitora Prawniczego, 2014, nr 9.

[4] Ibidem.

regulacje w zakresie ochrony danych osobowych (m.in. Czechy, Słowacja, Finlandia, Malta), bądź też w towarzystwie przepisów karnych (m.in. Holandia i Portugalia)[5].

Na tym tle system przyjęty przez ustawodawcę polskiego jest wyjątkowy, gdyż został oparty wyłącznie na sankcjach o charakterze karnym, przewidzianych w przepisach pozakodeksowych, tj. art. 49 – 54a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (dalej: u.o.d.o.)[6].

Ustawa o ochronie danych osobowych określa zasady postępowania przy przetwarzaniu *danych osobowych* oraz prawa osób fizycznych, których *dane osobowe* są lub mogą być przetwarzane w zbiorach *danych (art. 2 ust. 1* u.o.d.o.*)*.

Ustawę stosuje się do przetwarzania danych osobowych: 1) w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych; 2) w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych *(art. 2 ust. 2* u.o.d.o.*)*. W odniesieniu do zbiorów *danych osobowych* sporządzanych doraźnie, wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką w szkołach wyższych, a po ich wykorzystaniu niezwłocznie usuwanych albo poddanych anonimizacji, mają zastosowanie jedynie przepisy rozdziału 5 ustawy – zabezpieczenie danych osobowych *(art. 2 ust. 3* u.o.d.o.*)*.

System ten w literaturze uważany jest za mało efektywne narzędzie służące ochronie danych osobowych. Podkreśla się, że „iluzoryczność ochrony wynika m.in. z konstrukcji przestępstw stypizowanych w art. 53 i 54 ustawy jako typów wyłącznie umyślnych, czy też z ograniczenia stosowania art. 49 ust. 1 i 2 u.o.d.o. do działania na zbiorze danych osobowych. Jednocześnie uznanie zachowań, takich jak niezgłoszenie zbioru danych osobowych do rejestracji czy naruszenie obowiązków informacyjnych względem osób, których dane dotyczą, wydaje się z perspektywy zawartości bezprawia takiego zachowania oraz jego społecznej szkodliwości

[5] Za: P. Barta, P. Litwiński, *Ustawa o ochronie danych osobowych. Komentarz. Wyd. 3*, Warszawa 2015, s. 513 i 514. Odnośnie do poszczególnych państw zob.: Czechy - ustawa z 4.4.2000 r. o ochronie danych osobowych i o zmianie niektórych innych ustaw, Słowacja - ustawa 428/2002 o ochronie danych osobowych, Finlandia - ustawa 523/1999 o ochronie danych osobowych, Malta - ustawa XXVI z 2001 r. o ochronie danych osobowych, Portugalia - ustawa z 26.10.1998 r. o ochronie danych osobowych, Holandia - ustawa z 3.7.2000 r. o ochronie danych osobowych.

[6] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. 2015, poz. 2135 ze zm.).

nieuzasadnioną kryminalizacją zachowań, które nie powinny być uznane za przestępcze.”[7]

Niniejsze opracowanie podejmuje zatem – od strony analizy postępowań przygotowawczych i spraw zakończonych wydaniem prawomocnego orzeczenia sądowego – próby określenia, czy przepisy karne ustawy o ochronie danych osobowych są wystarczające do prawidłowej ochrony dóbr osobistych obywateli przed ich nieuprawnionym wykorzystaniem.

[7] Zob. P. Barta, P. Litwiński, *op. cit.*

1. Przepisy karne ustawy o ochronie danych osobowych

1.1. Uwagi wstępne

Przepisy karne ustawy o ochronie danych osobowych, od wejścia w życie większości jej postanowień z dniem 30 kwietnia 1998 r., ulegały niewielu korektom. I tak:

- art. 50 ustawy uchylony został przez art. 1 pkt 12 ustawy z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych oraz niektórych innych ustaw[8] - z dniem 7 marca 2011 r.

- art. 54a dodany został przez art. 1 pkt 13 ustawy z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych oraz niektórych innych ustaw - z dniem 7 marca 2011 r.[9]

Pozostałe przepisy karne nie uległy zmianie od czasu wejścia ich życie.

W stosunku do nich – na podstawie art. 116 k.k. – zastosowanie znajdują przepisy części ogólnej kodeksu karnego. Oznacza to, że stosować się do nich będzie m.in. przepisy dotyczące środków karnych (art. 39 k.k.), środków związanych z poddaniem sprawcy próbie czy odpowiedzialności współsprawcy przestępstwa, jak również

[8] Dz.U. Nr 229, poz.1497.

[9] Uzasadnieniem wykreślenia art. 50 u.o.d.o. z ustawy było stwierdzenie, że przedmiot regulacji objęty tym przepisem mieści się w art. 49 u.o.d.o. odnoszącym się do bezprawnego przetwarzania danych, gdyż przechowywanie stanowi jeden z elementów szeroko ujmowanego przetwarzania danych. Natomiast art. 54a stanowi *novum* w tej ustawie, nie był bowiem przewidziany w pierwotnym brzmieniu projektu nowelizacji ustawy. Jak zauważył P. Fajgielski, komentując wprowadzone w przepisach prawnokarnych ustawy zmiany: „Przyjęte rozwiązanie prawne jest odmienne od przewidzianego w pierwotnym projekcie ustawy mechanizmu kar pieniężnych za utrudnianie bądź uniemożliwianie kontroli, które to kary nakładać miał Generalny Inspektor. Bez wątpienia odpowiedzialność karna jest surowsza niż zakładana wcześniej odpowiedzialność administracyjna. Z drugiej jednak strony można twierdzić, że wyroków wydanych na podstawie wskazanego przepisu będzie zdecydowanie mniej, niż byłoby decyzji o ukaraniu wydanych przez organ ochrony danych. Ponadto, sytuacja, w której GIODO mógłby karać za utrudnianie kontroli pociągałaby za sobą poważne wątpliwości co do bezstronności organu, a przepisy przyznające organowi ochrony danych uprawnienia do nakładania kar mogłyby w praktyce być podstawą do wymuszania określonych zachowań osób reprezentujących administratora danych w trakcie kontroli, działań nie zawsze mających wystarczające podstawy w obowiązkach określonych przepisami prawa. Można zatem uznać, że objęcie inspektorów biura GIODO prawnokarną ochroną powinno przyczynić się do poprawy skuteczności ich działań, poddając jednocześnie te działania (zwłaszcza żądania skierowane do administratorów danych) dodatkowej kontroli sądu w przypadkach spornych).”, P. Fajgielski, *Nowelizacja ustawy o ochronie danych osobowych – zakładane cele i przewidywane skutki*, dodatek do Monitora Prawniczego, nr 3/2001, s. 1004.

podżegacza i pomocnika (art. 18 § 3 k.k.). Występki z u.o.d.o. można również popełnić w formie usiłowania (art. 13 k.k.).

Wszystkie występki określone w ustawie o ochronie danych osobowych są ścigane z urzędu, z oskarżenia publicznego, a ich karalność ustaje po upływie 5 lat liczonych od daty ich popełnienia (art. 101 k.k.).

Podkreślić należy, że – zgodnie z ogólnymi regułami prawa karnego materialnego i procesowego – odpowiedzialność karną na podstawie przepisów Rozdziału 8 ustawy ponosić będą wyłącznie osoby fizyczne. W przypadku popełnienia przestępstwa z u.o.d.o. przez osobę fizyczną powiązaną z tzw. podmiotem zbiorowym w rozumieniu art. 2 ustawy z dnia 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary[10], podmiot ten nie poniesie odpowiedzialności na zasadach określonych w ustawie, gdyż przepisy karne ustawy o ochronie danych osobowych nie zostały wymienione w katalogu czynów, do których zastosowanie ma rzeczona ustawa (art. 16 ustawy o odpowiedzialności podmiotów zbiorowych).

1.2. Art. 49 – przetwarzanie danych przez nieuprawnionego

Art. 49 ust. 1 u.o.d.o. przewiduje sankcję karną dla osoby, która przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniona.

Art. 49 ust. 2 u.o.d.o. przewiduje postać kwalifikowaną tego typu przestępstwa w sytuacji, gdy niedopuszczalne przetwarzanie albo przetwarzanie bez uprawnienia dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym pokrzywdzonego.

Przestępstwo z art. 49 ust. 1 u.o.d.o. może zostać popełnione w dwóch odmianach, gdy:

1) przetwarzanie danych jest niedopuszczalne,

[10] T.j. Dz.U. z 2014 r., poz. 1417 ze zm.

2) przetwarzanie jest dopuszczalne, ale dokonuje tego osoba nieuprawniona.

Między zakresami tych dwóch odmian zachodzić będzie stosunek krzyżowania[11].

Sprawca przestępstwa z art. 49 u.o.d.o. realizować będzie znamiona tego czynu, jeżeli jego zachowanie naruszy treść art. 23 u.o.d.o. – w przypadku przetwarzania danych zwykłych lub art. 27 u.o.d.o. – w odniesieniu do danych wrażliwych.

Zgodnie z treścią art. 23 ust. 1. u.o.d.o. przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:

1) osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych;

2) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa;

3) jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą;

4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego;

5) jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Zgodnie z treścią art. 27 ust. 1 u.o.d.o. zabrania się przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów

[11] Zob. J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Wyd. 3, Kraków 2004, s. 733.

karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym. Wyjątki od tej reguły określa ust. 2 tego artykułu[12].

Odpowiedzialność karną poniesie zatem tylko taki sprawca, który nie będzie mógł powołać się choćby na jedną z przesłanek legalizujących przetwarzanie danych osobowych[13].

Jak zauważają P. Barta i P. Litwiński „przestępstwo [to] stanowi zabronione przez komentowany przepis przetwarzanie danych osobowych w sytuacji wniesienia przez osobę, której dane dotyczą, sprzeciwu wobec przetwarzania jej danych osobowych, na zasadzie art. 32 ust. 1 pkt 8 u.o.d.o. Nie stanowi natomiast przestępstwa przetwarzanie danych osobowych po wniesieniu przez osobę, której dane dotyczą, pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych na zasadzie art. 32 ust. 1 pkt 7 u.o.d.o., w sytuacji gdy administrator danych nie podziela stanowiska osoby, której dane dotyczą, i nie zaprzestaje przetwarzania

[12] Art. 27 ust 2 u.o.d.o. stanowi, iż przetwarzanie danych, o których mowa w ust. 1, jest jednak dopuszczalne, jeżeli:
1) osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, chyba że chodzi o usunięcie dotyczących jej danych;
2) przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony;
3) przetwarzanie takich danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora;
4) jest to niezbędne do wykonania statutowych zadań kościołów i innych związków wyznaniowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, pod warunkiem, że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych;
5) przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem;
6) przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie;
7) przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych;
8) przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą;
9) jest to niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego; publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone;
10) przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

[13] Tak: P. Barta, P. Litwiński, *op. cit.*, s. 518.

jej danych, przekazując jednocześnie sprawę Generalnemu Inspektorowi, na zasadzie art. 32 ust. 2 u.o.d.o."[14]

Znamię czynnościowe „przetwarzania danych" E. Hryniewicz proponuje rozumieć jako „jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych (art. 7 pkt 2 u.o.d.o.). Zbiór danych osobowych może przyjąć formę kartotek, skorowidzów, ksiąg, wykazów i innych zbiorów ewidencyjnych, a także zbioru sporządzonego doraźnie (art. 2 ust. 2 i 3 u.o.d.o.)."[15]

Przetwarzanie danych poza zbiorem ewidencyjnym (danych) nie będzie przestępstwem na podstawie art. 49 u.o.d.o. Nie realizuje jego znamion również przetwarzanie danych osobowych wyłącznie w celach osobistych[16].

Nie popełnia przestępstwa z art. 49 u.o.d.o. administrator danych, który dopuszcza osobę nieuprawnioną do przetwarzania danych osobowych[17].

Występek z art. 49 u.o.d.o. jest przestępstwem powszechnym i może być popełniony przez każdą osobę, która faktycznie podjęła decyzję o przetwarzaniu danych osobowych z naruszeniem jego znamion. Ponadto jest to przestępstwo formalne. Może być popełnione wyłącznie z winy umyślnej.

Wobec sprawcy typu podstawowego z ust. 1 tego artykułu może zostać orzeczona kara grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2, natomiast w stosunku do sprawcy typu kwalifikowanego z ust. 2 – kara grzywny, ograniczenia wolności albo pozbawienia wolności do lat 3.

1.3. Art. 51 – Udostępnianie danych osobom nieuprawnionym

[14] Idem

[15] E. Hryniewicz, [w:] *Prawo karne gospodarcze. Tom 10*, R. Zawłocki (red.), Warszawa 2012, s. 333

[16] Tak: A. Drozd, Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy. Wyd. 3, Warszawa 2007, s. 321.

[17] Zob. P. Barta, P. Litwiński, *op. cit.*, s. 519.

Przedmiotem ochrony przepisu art. 51 u.o.d.o. jest poufność danych osobowych w granicach wyznaczonych przez zasadę celowości i zasadę bezpieczeństwa danych[18].

Popełnić je może osoba administrująca zbiorem danych lub obowiązana do ochrony danych osobowych, która udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym (przestępstwo indywidualne).

Pojęcie „osoby administrującej zbiorem danych" nie jest tożsame z określeniem „administratora danych". Jak stwierdził Sąd Najwyższy w postanowieniu z 11 grudnia 2000 r., II KKN 438/00[19]: „na gruncie ustawy o ochronie danych osobowych administratorem danych osobowych jest jedynie ten podmiot, który decyduje o celach i środkach przetwarzania tych danych (art. 7 pkt 4 ustawy), natomiast administrującym - także taki podmiot, który zarządza, zawiaduje zbiorem danych (art. 50, 51, 54) lub danymi (art. 52) w procesie ich przetwarzania, w tym i powierzonego mu w trybie wskazanym w art. 31 tej ustawy, przy czym odpowiedzialność karna administrującego nie będącego administratorem danych wchodzi w rachubę wówczas, gdy jego zachowanie - uznane za karalne przez ustawę - wynika z powierzonych mu czynności przetwarzania danych."

Przyjąć zatem należy, że podmiotem przestępstwa z art. 51 u.o.d.o. może być administrator danych osobowych, jak również inna osoba, która zarządza, zawiaduje zbiorem danych lub danymi w procesie ich przetwarzania – zobowiązana do ochrony danych osobowych[20]. Osobami obowiązanymi mogą być w tym przypadku osoby fizyczne przetwarzające dane osobowe na podstawie upoważnienia nadanego przez administratora danych osobowych (art. 37 u.o.d.o.) albo na zlecenie – na podstawie umowy (art. 31 u.o.d.o.). Obowiązek ochrony danych osobowych przez wskazane wyżej osoby wynika wprost z przepisów prawa. W przypadku, gdy umowa przewiduje szerszy zakres odpowiedzialności osób obowiązanych, niż to zostało określone

[18] J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, s. 737

[19] OSNKW 2001, nr 3-4, poz. 33, s. 101. Odmienne stanowisko wyraził A. Adamski, który uznaje za osobę administrującą zbiorem danych tylko tego, kto decyduje o celach i środkach przetwarzania danych osobowych, nie zaś tego, kto usługowo zajmuje się przetwarzaniem danych na podstawie umowy z administratorem, A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 161.

[20] Zob. P. Barta, P. Litwiński, *op. cit.*, s. 522.

w ustawie, naruszenie tych obowiązków rodzić będzie po ich stronie wyłącznie odpowiedzialność cywilnoprawną[21].

W literaturze wyrażany jest pogląd, że po nowelizacji ustawy o ochronie danych osobowych z 2015 r.[22] do odpowiedzialności za niedopełnienie obowiązku ochrony danych osobowych mogą zostać pociągnięci również administratorzy bezpieczeństwa informacji (ABI)[23].

Przepis art. 51 u.o.d.o. przewiduje dwie formy czynności wykonawczej:

- udostępnienie danych osobowych, przez które należy rozumieć formę przetwarzania danych określoną w art. 7 ust. 2 u.o.d.o.; w literaturze za udostępnienie danych uważa się wyłącznie sytuację, w której odbiorcą danych jest inny administrator danych. Udostępnienie danych nastąpi wówczas, gdy administrator danych osobowych w sposób faktyczny przekaże bądź inaczej umożliwi zapoznanie się z danymi innej osobie lub podmiotowi, który to podmiot pełnić będzie w stosunku do tych danych osobowych funkcję administratora danych; nie będzie natomiast udostępnieniem danych osobowych przekazanie danych w ramach struktury organizacyjnej tego samego administratora[24];

- umożliwienie dostępu do danych osobowych, przez które można rozumieć nie tylko dopuszczenie osoby nieupoważnionej do danych osobowych (działanie), ale także pozostawienie ich bez zabezpieczenia (zaniechanie)[25].

Osobami nieupoważnionymi do dostępu do danych osobowych będą zarówno osoby nie mające upoważnienia do przetwarzania danych osobowych, jak również osoby

[21] *Idem*, s. 523.

[22] Na podstawie art. 9 ustawy z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej (Dz.U. z 2014 r., poz. 1662).

[23] Tak: B. Konieczna-Drzewiecka, A. Zubrzycka, *Tajemnica upoważnionego do przetwarzania danych osobowych*, Monitor prawniczy, 2015, Nr 21, s. 1174.

[24] P. Barta, P. Litwiński, *op. cit.*, s. 524.

[25] Zob. B. Kurzępa, *Przestępstwa z ustawy o ochronie danych osobowych*, Prokuratura i Prawo, 1999, nr 6, s. 44; B. Konieczna-Drzewiecka, A. Zubrzycka, *op. cit.*, s. 1174; A. Drozd, *op. cit.*, s. 323. Odmiennie: A. Adamski, *Prawo karne…*, s. 164, który opowiada się wyłącznie za formą zaniechania.

mające co prawda upoważnienie do przetwarzania danych, ale nie tych, które zostały im udostępnione lub z którymi mogły się zapoznać[26].

Nie wyczerpuje znamion występku z art. 51 u.o.d.o. udostępnienie danych lub umożliwienie do nich dostępu jednej osobie[27].

Przestępstwo ma charakter formalny, bowiem dla jego popełnienia nie jest konieczne zapoznanie się z danymi przez ich odbiorcę, a ponadto do znamion tego występku nie należy wystąpienie jakiejkolwiek szkody po stronie osoby, której dane dotyczą.

Przestępstwo z art. 51 u.o.d.o. może być popełnione zarówno umyślnie, jak i nieumyślnie.

Przestępstwo udostępnienia danych osobom nieuprawnionym zagrożone jest karą grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2 (ust. 1), a w przypadku postaci nieumyślnej (ust. 2) – grzywny, ograniczenia wolności albo pozbawienia wolności do roku.

Istnieje możliwość kumulatywnego zbiegu przestępstwa z art. 51 ust. 1 u.o.d.o. z art. 266 § 1 i 2 k.k., który penalizuje ujawnianie lub wykorzystywanie informacji powziętych w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną lub naukową, a w przypadku, gdy sprawca działa nieumyślnie – przestępstwem z art. 231 § 3 k.k., tj. przekroczenia uprawnień lub niedopełnienia obowiązków przez funkcjonariusza publicznego.

1.4. Art. 52 – Naruszenie obowiązku zabezpieczenia danych

Przepis art. 52 u.o.d.o. przewiduje penalizację zachowania polegającego na naruszeniu przez osobę administrującą danymi, chociażby nieumyślnie, obowiązku zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem.

[26] A. Drozd, *op. cit.*, s. 323.

[27] Postanowienie SN z dnia 21 listopada 2007 r., IV KK 376/07, Krakowskie Zeszyty Sądowe, 2008, Nr 11, poz. 47

Indywidualnym przedmiotem ochrony tego przepisu są dane osobowe, a ochrona skierowana jest na niezakłócone ich przechowywanie[28]. Obowiązek zabezpieczenia danych ciąży na osobie administrującej danymi.

Zgodnie z treścią art. 36 ust. 1 u.o.d.o. administrator *danych* jest obowiązany zastosować środki techniczne i organizacyjne zapewniające *ochronę* przetwarzanych *danych osobowych* odpowiednią do zagrożeń oraz kategorii *danych* objętych *ochroną*, a w szczególności powinien zabezpieczyć *dane* przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Do obowiązków administratora należy prowadzenie dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ich ochronę (art. 36 ust. 2 u.o.d.o.).

Ochronę danych osobowych administrator danych może powierzyć innemu podmiotowi, w drodze umowy o przetwarzanie danych, zawartej na piśmie. Podmiot taki może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie. Przed rozpoczęciem przetwarzania danych jest on obowiązany podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36 - 39 ustawy, oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a. W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych (art. 31 ust. 1 – 3 u.o.d.o).

Przestępstwo to może popełnić każda osoba, na której ciąży obowiązek zabezpieczenia danych osobowych przed ich zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem w procesie ich przetwarzania. W szczególności takimi osobami są administrator danych lub podmiot przetwarzający dane osobowe na zlecenie albo osoby działające w imieniu administratora danych lub podmiotu przetwarzającego dane osobowe na zlecenie.[29].

[28] Zob. J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, s. 743.

[29] Tak: P. Barta, P. Litwiński, Ustawa o ochronie danych osobowych. Komentarz. Wyd. 3, Warszawa 2015, s. 527; A. Drozd, op. cit., s. 324. Odmienne stanowisko prezentują J. Barta, P. Fajgielski, R. Markiewicz, którzy wskazują na indywidualny charakter tego występku, który może zostać popełniony wyłącznie przez administrującego danymi osobowymi, op. cit., s. 743. Stanowisko to jednak wydaje się być nieprawidłowe, gdyż znamię podmiotowe tego przepisu odwołuje się do pewnego stanu faktycznego, jakim jest administrowanie danymi, a nie do cechy indywidualizującej podmiot przestępstwa, tj. administratora danych.

Zachowanie sprawcy przestępstwa z art. 52 u.o.d.o. polega na naruszeniu obowiązku zabezpieczenia danych osobowych przed ich zabraniem, uszkodzeniem lub zniszczeniem, bez względu na to, czy do realizacji znamienia czasownikowego doszło, czy też nie. Do przyjęcia, że zostały zrealizowane znamiona tego przestępstwa, nie jest wymagane nastąpienie skutku naruszenia obowiązku zabezpieczenia danych (przestępstwo formalne).

Przedmiotem przestępstwa mogą tu być dane osobowe przetwarzane w zbiorze danych, jak również takie, które są przetwarzane poza zbiorami. Do tej grupy zaliczyć również należy dane w zbiorze ewidencyjnym.

Przestępstwo to może być popełnione zarówno umyślnie, jak i nieumyślnie. Zagrożone jest grzywną, karą ograniczenia wolności albo karą pozbawienia wolności do roku.

1.5. Art. 53 – Niezgłoszenie danych do rejestru

Występek stypizowany w art. 53 u.o.d.o. polega na niezgłoszeniu do rejestracji zbioru danych przez osobę obowiązaną do jego zgłoszenia.

Przestępstwo to, którego przedmiotem ochrony jest umożliwienie ewidencjonowania i kontrolowania przetwarzania danych osobowych [30], popełnić może wyłącznie podmiot obowiązany do zgłoszenia zbioru danych osobowych do rejestracji (przestępstwo indywidualne; odmiennie: A. Drozd[31]), tj. administrator danych – jeżeli jest osobą fizyczną albo osoba działająca w imieniu administratora danych – jeżeli jest on osobą prawną. Obowiązek zgłoszenia danych do rejestru wynikać musi z obowiązku ustawowego, a nie z innej podstawy prawnej, np. umowy (odmiennie: A. Drozd[32]).

Obowiązek zgłoszenia Generalnemu Inspektorowi każdego zbioru danych osobowych do rejestracji ciąży na administratorze danych osobowych, chyba

[30] Zob. J. Barta, P. Fajgielski, R. Markiewicz, *op. cit*., s. 744.

[31] Zob. A. Drozd, *op. cit*., s. 324.

[32] Idem

że zbiór taki został z tego obowiązku zwolniony na podstawie art. 43 ust. 1 u.o.d.o.[33] (art. 40 u.o.d.o.). Obowiązkowi zgłoszenia nie podlegają ponadto zbiory sporządzone doraźnie i na zasadzie art. 2 ust. 3 u.o.d.o., tj. wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką w szkołach wyższych, a po ich wykorzystaniu niezwłocznie usuwanych albo poddanych anonimizacji.

Przestępstwo z art. 53 u.o.d.o. może zostać popełnione wyłącznie umyślnie przez zaniechanie. Nie popełnia występku określonego w tym przepisie osoba, która podaje w zgłoszeniu rejestracyjnym nieprawdziwe informacje lub zataja informacje, jak również taka, która nie wykonuje obowiązku aktualizacji dokonanego zgłoszenia rejestracyjnego, na zasadzie art. 41 ust. 2 u.o.d.o.[34] W takim przypadku można by ewentualnie rozważać odpowiedzialność sprawcy na podstawie art. 271 k.k. (poświadczenie nieprawdy)[35].

Przestępstwo to nie wymaga nastąpienia skutku w postaci powstania szkody wynikającej z niezgłoszenia do rejestracji zbioru danych osobowych, a zatem ma charakter formalny.

---

[33] Na podstawie art. 43 ust. 1 u.o.d.o. z obowiązku rejestracji zbioru danych zwolnieni są administratorzy danych: 1) zawierających informacje niejawne; 1a) które zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych przez funkcjonariuszy organów uprawnionych do tych czynności; 2) przetwarzanych przez właściwe organy dla potrzeb postępowania sądowego oraz na podstawie przepisów o Krajowym Rejestrze Karnym; 2a) przetwarzanych przez Generalnego Inspektora Informacji Finansowej; 2b) przetwarzanych przez właściwe organy na potrzeby udziału Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym; 2c) przetwarzanych przez właściwie organy na podstawie przepisów o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej; 3) dotyczących osób należących do kościoła lub innego związku wyznaniowego, o uregulowanej sytuacji prawnej, przetwarzanych na potrzeby tego kościoła lub związku wyznaniowego; 4) przetwarzanych w związku z zatrudnieniem u nich, świadczeniem im usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się; 5) dotyczących osób korzystających z ich usług medycznych, obsługi notarialnej, adwokackiej, radcy prawnego, rzecznika patentowego, doradcy podatkowego lub biegłego rewidenta; 6) tworzonych na podstawie przepisów dotyczących wyborów do Sejmu, Senatu, Parlamentu Europejskiego, rad gmin, rad powiatów i sejmików województw, wyborów na urząd Prezydenta Rzeczypospolitej Polskiej, na wójta, burmistrza, prezydenta miasta oraz dotyczących referendum ogólnokrajowego i referendum lokalnego; 7) dotyczących osób pozbawionych wolności na podstawie ustawy, w zakresie niezbędnym do wykonania tymczasowego aresztowania lub kary pozbawienia wolności; 8) przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej; 9) powszechnie dostępnych; 10) przetwarzanych w celu przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego; 11) przetwarzanych w zakresie drobnych bieżących spraw życia codziennego; 12) przetwarzanych w zbiorach, które nie są prowadzone z wykorzystaniem systemów informatycznych, z wyjątkiem zbiorów zawierających dane, o których mowa w art. 27 ust. 1.

[34] Zob. P. Barta, P. Litwiński, *op. cit.*, s. 528.

[35] Zob. A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 173.

Niezgłoszenie danych do rejestru podlega karze grzywny, ograniczenia wolności albo pozbawienia wolności do roku.

1.6. Art. 54 – Niedopełnienie obowiązku poinformowania

Ustawa o ochronie danych osobowych nakłada na administratora danych osobowych szereg obowiązków informacyjnych związanych z procesem zbierania danych osobowych (art. 24 i 25 u.o.d.o.), jak i dalszego ich przetwarzania (art. 32 i 33 u.o.d.o.).

Przestępstwo z art. 54 ustawy popełnić może osoba, która administrując zbiorem danych nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w ustawie o ochronie danych osobowych. Przestępstwo to jest przestępstwem indywidualnym, które faktycznie może zostać popełnione wyłącznie przez administratora danych osobowych, co wynika z faktu nienałożenia przez ustawę jakichkolwiek obowiązków informacyjnych na inne osoby administrujące zbiorem danych osobowych[36].

W przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o:

1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku;

2) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych;

3) prawie dostępu do treści swoich danych oraz ich poprawiania;

4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej (art. 24 ust. 1 u.o.d.o.).

[36] Tak m.in. P. Barta, P. Litwiński, *op. cit.*, s. 530.

Natomiast każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych (a zatem niebezpośrednio od tej osoby), a zwłaszcza prawo do:

1) uzyskania wyczerpującej informacji, czy taki zbiór istnieje, oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy, a w przypadku gdy administratorem danych jest osoba fizyczna - jej miejsca zamieszkania oraz imienia i nazwiska;

2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze;

3) uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące, oraz podania w powszechnie zrozumiałej formie treści tych danych;

4) uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące, chyba że administrator danych jest zobowiązany do zachowania w tym zakresie w tajemnicy informacji niejawnych lub zachowania tajemnicy zawodowej;

5) uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane;

5a) uzyskania informacji o przesłankach podjęcia rozstrzygnięcia, o którym mowa w art. 26a ust. 2;

6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane;

7) wniesienia, w przypadkach wymienionych w art. 23 ust. 1 pkt 4 i 5, pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację;

8) wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, wymienionych w art. 23 ust. 1 pkt 4 i 5, gdy administrator danych zamierza

je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych;

9) wniesienia do administratora danych żądania ponownego, indywidualnego rozpatrzenia sprawy rozstrzygniętej z naruszeniem art. 26a ust. 1 (art. 32 ust. 1 u.o.d.o.).

Przestępstwo z art. 54 popełnione jest wówczas, gdy upłynął termin realizacji opisanego w nim obowiązku. W przypadku zbierania danych od osoby, której dane dotyczą (art. 24), najpóźniejszym terminem dla realizacji obowiązku jest okres poprzedzający przekazanie danych przez zainteresowanego. W przypadku zbierania danych nie od osoby, której one dotyczą (art. 25), udzielenie stosownej informacji powinno nastąpić bezpośrednio po utrwaleniu zebranych danych. Obowiązek informacyjny wynikający z art. 32 w zw. z art. 33 ustawy administrator musi wykonać w terminie 30 dni od dnia złożenia wniosku[37].

Nie popełnia przestępstwa z art. 54 u.o.d.o., kto nie podaje osobie, której dane dotyczą, informacji o celu zbierania danych, o odbiorcach danych oraz o dobrowolności albo obowiązku podania danych[38].

Przestępstwo z art. 54 u.o.d.o. może zostać popełnione wyłącznie przez zaniechanie i wyłącznie umyślnie.

Wobec sprawcy może zostać orzeczona kara grzywny, kara ograniczenia wolności albo pozbawienia wolności do roku.

1.7. Art. 54a – Udaremnienie wykonania czynności kontrolnej

Przestępstwo udaremnienia wykonania czynności kontrolnej zostało wprowadzone do ustawy o ochronie danych osobowych w wyniku nowelizacji z 2010 r.[39]

Przedmiotem ochrony tego przepisu jest „prawidłowość wykonywania czynności składających się na kontrolę, która zależy od możliwości wypełnienia przez

[37] Tak: J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, s. 747; A. Drozd, *op. cit.*, s. 325.

[38] P. Barta, P. Litwiński, *op. cit.*, s. 530.

[39] Ustawa z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych oraz niektórych innych ustaw (Dz.U. Nr 229, poz. 1497).

inspektora ochrony danych osobowych w sposób nieskrępowany jego obowiązków."[40] Pośrednim przedmiotem ochrony jest prawo do ochrony danych osobowych.

Przestępstwo określone w art. 54a u.o.d.o. ma charakter powszechny. Osobami, na których ciążą obowiązki związane z przeprowadzaną przez inspektora danych osobowych kontrolą – zgodnie z art. 15 ust. 1 u.o.d.o. – są: kierownik kontrolowanej jednostki organizacyjnej oraz kontrolowana osoba fizyczna będąca administratorem danych osobowych. Jednak krąg podmiotu nie jest ograniczony wyłącznie do tych osób i może objąć każdą inną osobę, której zachowanie stanowi udaremnienie lub utrudnienie czynności kontrolnych.

Strona przedmiotowa przestępstwa z art. 54a u.o.d.o. polega na udaremnianiu lub utrudnianiu czynności kontrolnej. Udaremnienie wykonania czynności kontrolnych polega na całkowitym uniemożliwieniu jej wykonania, utrudnianie zaś to zachowanie, które wpływa na przebieg czynności kontrolnej i prowadzi do jej zakłócenia[41].

Zakres czynności kontrolnych podejmowanych w ramach ustawy przez inspektorów określa art. 14 u.o.d.o. Zgodnie z tym przepisem, w celu wykonania zadań, o których mowa w art. 12 pkt 1 i 2 ustawy, Generalny Inspektor, zastępca Generalnego Inspektora lub upoważnieni przez niego pracownicy Biura, zwani dalej "inspektorami", mają prawo:

1) wstępu, w godzinach od 6^{00} do 22^{00}, za okazaniem imiennego upoważnienia i legitymacji służbowej, do pomieszczenia, w którym zlokalizowany jest zbiór danych, oraz pomieszczenia, w którym przetwarzane są dane poza zbiorem danych, i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą;

2) żądania złożenia pisemnych lub ustnych wyjaśnień oraz wzywania i przesłuchiwania osoby w zakresie niezbędnym do ustalenia stanu faktycznego;

[40] A. Błachnio-Parzych, Prawonokarna ochrona inspektora ochrony danych osobowych – przestępstwo udaremnienia lub utrudnienia kontroli przestrzegania przepisów o ochronie danych osobowych, dodatek do Monitora Prawniczego, 2011, nr 3, s. 1036.

[41] P. Barta, P. Litwiński, *op. cit.*, s. 532.

3) wglądu do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z przedmiotem kontroli oraz sporządzania ich kopii;

4) przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych;

5) zlecania sporządzania ekspertyz i opinii.

Należy podkreślić jednak, że katalog uprawnień inspektora określony w art. 14 u.o.d.o. nie wprowadza ograniczeń w zakresie zachowań stanowiących udaremnienie lub utrudnienie kontroli[42].

Przestępstwo to ma charakter formalny i do jego popełnienia wystarczy samo podjęcie czynności udaremniających lub utrudniających wykonanie czynności kontrolnej.

Przestępstwo udaremnienia lub zakłócenia wykonania czynności kontrolnej jest przestępstwem umyślnym, które może zostać popełnione zarówno w zamiarze bezpośrednim, jak i ewentualnym[43].

Przestępstwo to zagrożone jest karą grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2.

Na tle konkretnych stanów faktycznych może ono podlegać zbiegowi z art. 222 § 1 k.k. oraz z art. 270 § 1 k.k. Możliwa jest także kwalifikacja kumulatywna art. 54a u.o.d.o. z art. 288 § 1 k.k. polegającym na niszczeniu cudzej rzeczy[44].

[42] Tak: A. Błachnio-Parzych, *op. cit.*, s. 1038.

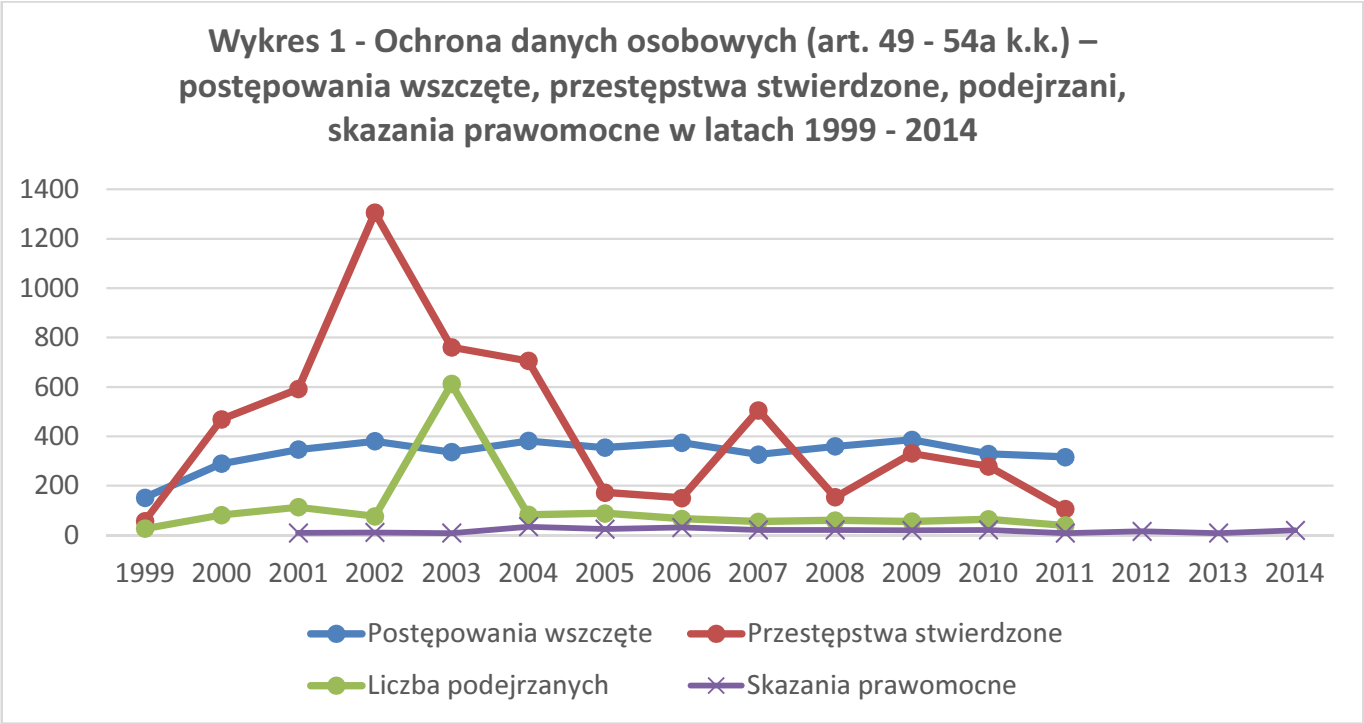
[43] *Ibidem*, s. 1039.

[44] *Idem*, s. 1040.

2. Przestępstwa z ustawy o ochronie danych osobowych w ujęciu statystycznym

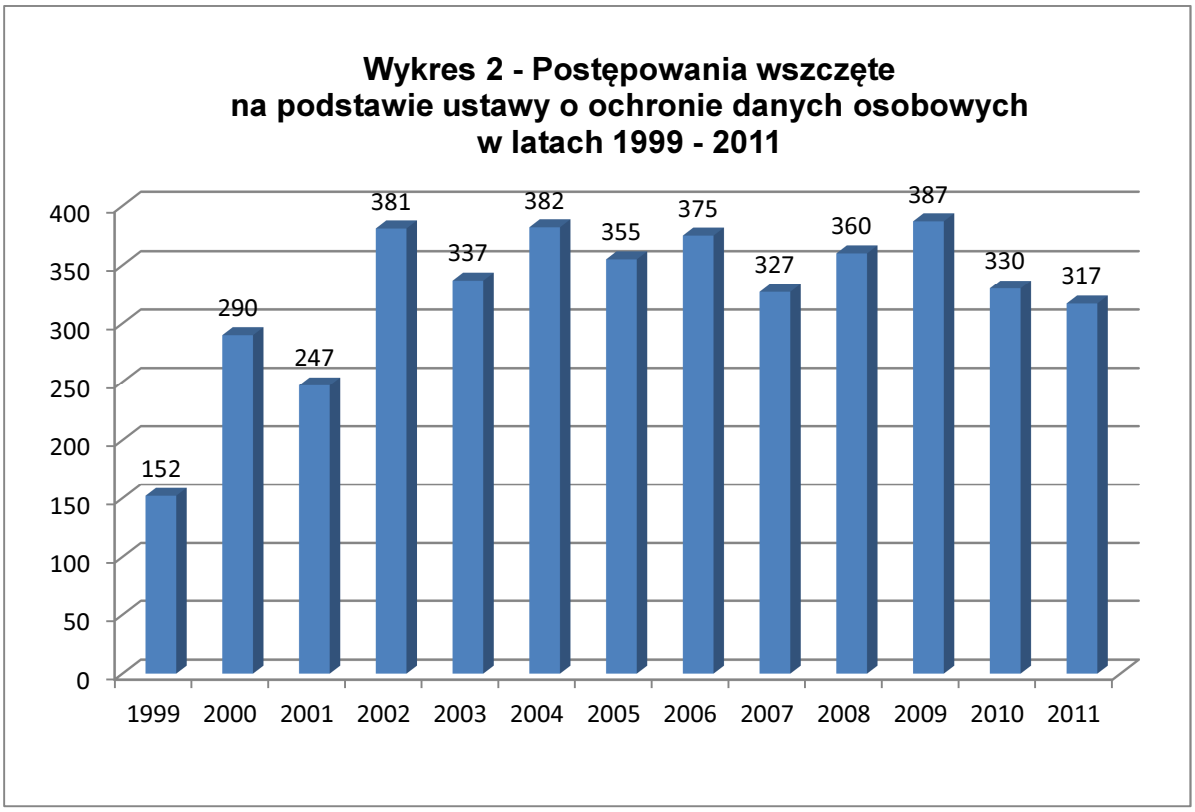
Dane statystyczne publikowane przez policję obejmują okres lat 1999 - 2012 i w odniesieniu do przestępstw z art. 49 – 54a ustawy o ochronie danych osobowych mają charakter zbiorczy.

Wykres 1 prezentuje dane dotyczące postępowań wszczętych, przestępstw stwierdzonych oraz liczby podejrzanych za okres 1999 - 2012 oraz skazań prawomocnych w latach 2001 – 2014.



Powyższy wykres prezentuje utrzymującą się w całym analizowanym okresie, na podobnym poziomie, liczbę postępowań wszczętych, przy bardzo zmiennej liczbie przestępstw stwierdzonych. Liczba osób podejrzanych, poza rokiem 2003, gdy gwałtownie wzrosła do 613, utrzymuje się na względnie podobnym poziome – kilkudziesięciu rocznie. Na tym tle liczba osób skazanych w oparciu o przepisy ustawy o ochronie danych osobowych jest niezwykle niska.

Dane szczegółowe dotyczące postępowań wszczętych w oparciu o art. 49 – 54a u.o.d.o. (w liczbach bezwzględnych) z podziałem na poszczególne lata prezentuje wykres 2.



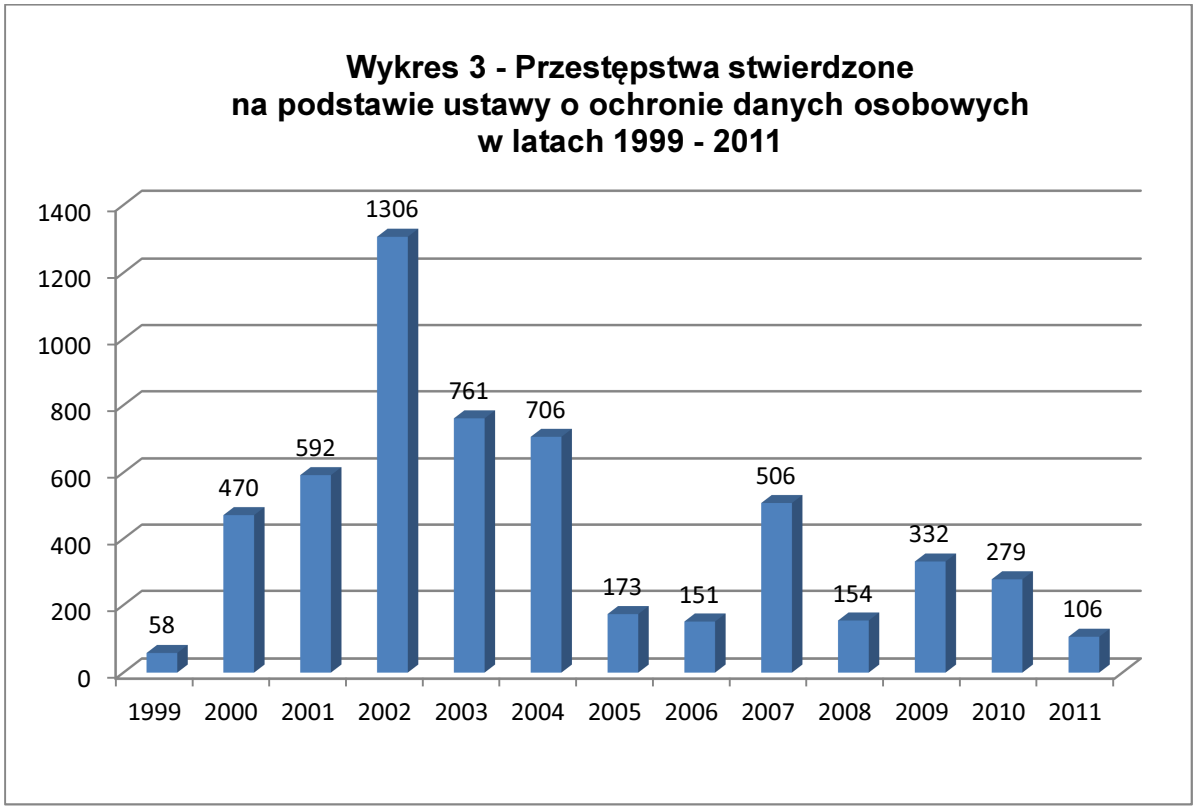
Dane te pokazują, że przez okres pierwszej dekady XXI w. policja wszczynała rocznie przeciętnie ponad 300 postępowań karnych na podstawie przepisów ustawy. W porównaniu rok do roku widzimy niewielkie wahnięcia, jednak nie zmieniające ogólnego trendu.

Analiza danych za lata 1999 – 2011 dotycząca przestępstw stwierdzonych[45] z art. 49 – 54a u.o.d.o. (wykres 3) wskazuje na znaczną zmienność w liczbie przestępstw „rok do roku", które znalazły potwierdzenie w toku postępowania przygotowawczego.

W danych tych daje się zauważyć okres znacznego wzrostu liczby przestępstw stwierdzanych obejmujący lata 2000 – 2004. Warto szczególnie zwrócić uwagę na rok 2002, w którym policja – przy 381 wszczętych postępowaniach – stwierdziła aż 1306 przestępstw, podając jednocześnie, iż w tym roku wskaźnik wykrywalności

[45] Za: http://statystyka.policja.pl/st/wybrane-statystyki/ochrona-danych-osobowy/63855,Ochrona-danych-osobowych.html

przestępstw z u.o.d.o. wyniósł 95,8% (!) i był najwyższy w analizowanym okresie (w pozostałych latach wzrostu kształtował się na poziomie 91,1 – 94,1%).



Trudno jest wskazać przyczyny tak wysokiej liczby przestępstw stwierdzonych w roku 2002, gdyż nie wystąpiły w tym lub poprzedzających latach żadne szczególne czynniki, które by go uzasadniały.

Inaczej może mieć się ze znaczącym spadkiem liczby przestępstw stwierdzanych w latach 2005 i 2006, co może być wynikiem nowelizacji ustawy o ochronie danych osobowych przeprowadzonej w roku 2004 i wprowadzającej szereg istotnych zmian w brzmieniu jej przepisów.

Po tym okresie widzimy znowu wzrost liczby przestępstw stwierdzanych w roku 2007 – do 506, po którym nastąpiły lata wykazujące się dużą zmiennością pod względem liczby potwierdzonych występków z ustawy o ochronie danych osobowych.

Powyższe dane skonfrontować można ze statystyką sądową skazań prawomocnych w oparciu o art. 49 – 54a u.o.d.o.[46] Dane obejmują lata 2001 - 2014 r. (wykres 4).

[46] Źródło: http://isws.ms.gov.pl/pl/baza-statystyczna/opracowania-wieloletnie/download,2853,43.html

Wykres ten pokazuje, jak niewielkie jest realne znaczenie występków określonych w ustawie o ochronie danych osobowych i jak niewielka jest liczba skazań w oparciu o przepisy karne ustawy. Najmniej osób – 9 – skazano w latach 2003, 2011 i 2013. Niewiele więcej w latach 2001 -2002 Z kolei najwięcej w roku 2004 – 35 i 2006 – 32. W pozostałych latach liczba skazanych oscylowała wokół 20 osób rocznie.

Jeszcze gorzej dane te prezentują się, gdy rozdzielimy powyższe dane zbiorcze na poszczególne typy występków określonych przepisami ustawy.

W takim przypadku zauważymy, że większość skazań nastąpiła na podstawie art. 49 u.o.d.o., art. 51 i art. 52 ustawy.

TABELA. SKAZANIA PREWOMOCNE ZA WYSTĘPKI Z USTAWY O OCHRONIE DANYCH OSOBOWYCH W OKRSIE 2001 – 2014 (Z PODZIAŁEM NA ARTYKUŁY)

	LATA													
	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014
	w liczbach bezwzględnych													
Art.49 ust.1		3	1	8	1	7	2	2	5	7	2	3	1	
Art.49 ust.2	1			1	1	1			1	1				1
Art.50	1					1								1
Art.51									1					
Art.51 ust.1	6	2	5	13	10	16	11	10	7	8	4	7	2	6
Art.51 ust.2	1	1	2	4	1	3	2	3	1	2	2	3	1	1
Art.52	1	5	1	7	10	4	7	7	3	1	1	3	5	11
Art.53				1	1				2	3				
Art.54		1		1	1									
	10	**12**	**9**	**35**	**25**	**32**	**22**	**22**	**20**	**22**	**9**	**16**	**9**	**20**

Źródło: Statystyka skazań prawomocnych Ministerstwa Sprawiedliwości

Pozostałe występki stały się podstawą skazania jedynie w kilku przypadkach przez okres 14 lat objętych prezentowanymi danymi, w tym art. 54 oraz uchylony art. 50 – każdy jedynie w trzech.

Warto dodać, że w latach 2011 – 2014 wykonanie wszystkich orzeczonych prawomocnie kar pozbawienia wolności zostało warunkowo zawieszone na okres próby. Orzekano ponadto kary ograniczenia wolności oraz grzywny – w wymiarze nie przekraczającym 5 000 zł.

3. Wyniki badań aktowych

3.1. Założenia badania

Badania przeprowadzono w oparciu akta spraw z art. 49 – 54 ustawy o ochronie danych osobowych zakończonych w roku 2014 odmową lub umorzeniem postępowania oraz postępowań, w których w tym samym roku zapadło prawomocne orzeczenie sądowe[47].

Zapytanie o dane dotyczące liczby postępowań zakończonych na etapie postępowania przygotowawczego, przesłane zostało do wszystkich jednostek prokuratury, za pośrednictwem prokuratur okręgowych.

W odpowiedzi z 280 prokuratur rejonowych uzyskano informację o 1010 postępowaniach, w których wydano postanowienie o odmowie lub umorzeniu postępowania na podstawie analizowanych przepisów ustawy. Szczegółowy podział spraw – z rozbiciem na poszczególne artykuły ustawy - przedstawia się następująco:

Artykuł ustawy	**Liczba postępowań umorzonych / odmów postępowania**
Art. 49	347
Art. 51	585
Art. 52	66
Art. 53	3
Art. 54	9

Na zapytanie o dane dotyczące liczby spraw, w których w roku 2014 zapadło orzeczenie prawomocne wydane w oparciu o przepisy karne ustawy o ochronie danych osobowych w odpowiedzi uzyskano informację o 45 takich sprawach rozpoznanych w 34 sądach rejonowych i jednym sądzie okręgowym. Szczegółowy podział spraw – z rozbiciem na poszczególne artykuły ustawy - przedstawia się następująco:

[47] W żadnej ze spraw nie wystąpiła kwalifikacja z art. 54a u.o.d.o.

Artykuł ustawy	Liczba postępowań zakończonych prawomocnym orzeczeniem sądowym
Art. 49	8
Art. 51	20
Art. 52	17

Do analizy została wylosowana 10% reprezentatywna próba losowa akt postępowań zakończonych na etapie postępowania sprawdzającego lub przygotowawczego w roku 2014 (101 spraw z 21 prokuratur), w tym: z art. 49 u.o.d.o. – 38 spraw, z art. 51 u.o.d.o. – 51 spraw, art. 52 u.o.d.o. – 1 sprawa, art. 53 u.o.d.o. – 3 sprawy, art. 54 u.o.d.o. – 8 spraw. Wśród wylosowanych spraw 36 zostało umorzonych na etapie postępowania przygotowawczego, a w pozostałych 65 wydano decyzję o odmowie wszczęcia postępowania.
W odniesieniu do akt spraw ukończonych prawomocnym orzeczeniem sądowym w badanym okresie (45 spraw) podjęto decyzję o analizie wszystkich postępowań.

Do badania nadesłano 91 postępowań przygotowawczych/akt postępowań sprawdzających i 38 spraw sądowych.

Artykuł ustawy	Liczba nadesłanych postępowań umorzonych/odmów postępowania	Liczba nadesłanych postępowań zakończonych prawomocnym orzeczeniem sądowym
Art. 49	38 (w tym 1 – z art. 49 ust. 2)	6 (w tym 1 – z art. 49 ust. 2)
Art. 51	43	18 (w tym 4 – z art. 51 ust. 2)
Art. 52	1	14
Art. 53	1	0
Art. 54	8	0

W przypadkach, w których nie nadesłano wylosowanych spraw, uzyskano informację o podjęciu na nowo tych postępowań, błędnej kwalifikacji podanej w przesłanej wcześniej informacji (sprawa nie dotyczyła ustawy o ochronie danych osobowych), połączeniu sprawy z innym postępowaniem – wskazanym w zestawieniu albo dołączeniu akt sprawy jako akt związkowych do innego toczącego się przed sądem postępowania.

3.2. Sprawy zakończone na etapie postępowania przygotowawczego

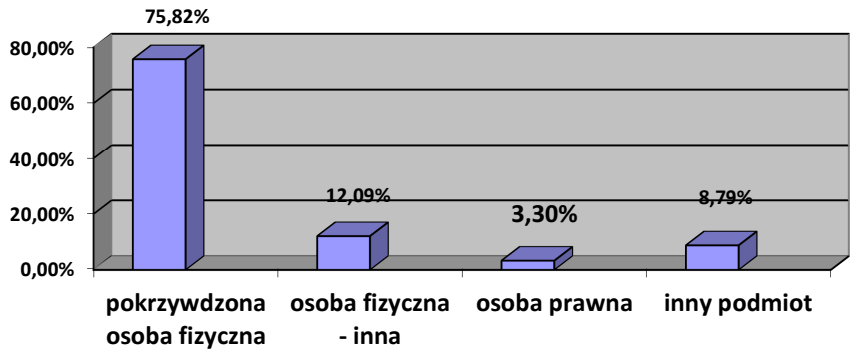
3.2.1. Zawiadomienie o przestępstwie

Ustawa o ochronie danych osobowych określa zasady postępowania przy przetwarzaniu ***danych osobowych*** oraz prawa osób fizycznych, których ***dane osobowe*** są lub mogą być przetwarzane w zbiorach ***danych (art. 2 ust. 1 u.o.d.o***.).

Już sam cel ustawy – opisany w art. 2 ust. 1 – określa, jakie podmioty będą głównymi poszkodowanymi w związku z naruszeniem jej przepisów. Korespondujący z zakresem przedmiotowym ustawy charakter występków stypizowanych w przepisach karnych ustawy o ochronie danych osobowych powoduje, że działania lub zaniechania sprawców skierowane będą przeciwko danym osób fizycznych.

Nie dziwi zatem, że w ponad 75% przypadków zawiadomienia o możliwości popełnienia przestępstwa określonego w ustawie złożone zostało przez osoby fizyczne, w których ocenie zostały naruszone ich dobra osobiste w postaci przetwarzania danych osobowych bez ich zgody, przetwarzania danych wbrew zakazowi ustawowemu, udostępnienia dostępu do danych osobom nieupoważnionym albo nie dopełnienia obowiązku informacyjnego w stosunku do osoby fizycznej.

Wykres 5 - Podmiot zawiadamiający o przestępstwie (w procentach)



W niewiele ponad 12% przypadków zawiadomienia złożone przez osoby fizycznie nie dotyczyły naruszenia bezpośrednio ich dóbr osobistych, ale dóbr osobistych osób im bliskich (rodzic, małżonek) albo zawiadamiający był znalazcą dokumentów zawierających dane osobowe innych osób fizycznych (np. wyrzuconych na śmietnik, bez ich uprzedniego zniszczenia).

Pozostałe ponad 12% zawiadomień złożone zostało przez organy osób prawnych lub inne podmioty (prezes spółdzielni mieszkaniowej, mieszkańcy budynku, prezydent miasta, osoba fizyczna prowadząca działalność gospodarczą) i odnosiły się do naruszeń danych osobowych innych osób. Przykładowo należy wymienić podejrzenie naruszenia danych osobowych wielu osób przez udostępnienie ich danych osobom nieuprawnionym w trakcie zebrania wspólnoty mieszkaniowej.

3.2.2. Charakter czynu przestępnego

Analiza postępowań karnych w sprawach o występki z ustawy o ochronie danych osobowych pozwoliła na wyodrębnienie szeregu mechanizmów przestępczego działania opisywanych przez zawiadamiających o popełnieniu przestępstwa.

Scharakteryzować je można w następujący sposób:

1) pozyskanie danych osobowych przez przedstawiciela firmy/firmę w trakcie rozmowy telefonicznej albo za pośrednictwem portalu internetowego.

Modus operandi w tego rodzaju sprawach polegał na przeprowadzeniu rozmowy przez przedstawiciela firmy w związku z zamiarem przedstawienia oferty świadczenia usług. Osoba fizyczna dobrowolnie podawała swoje dane, które następnie wykorzystywane były przez kolejnych przedstawicieli firmy w celu skontaktowania się z taką osobą. Były to najczęściej występujące rodzaje zawiadomień.

2) przetwarzanie przez administratora portalu internetowego lub serwisu społecznościowego, dostawcy poczty elektronicznej, danych osobowych wbrew przepisom ustawy lub nie będąc do tego uprawnionym.

W takich przypadkach osoby – w ich ocenie – pokrzywdzone przestępstwem zawiadamiały, iż otrzymują informacje mailowe z portali, serwisów lub poczty

elektronicznej, pomimo, iż nie wyrażały zgody na przetwarzanie danych osobowych przez te podmioty.

3) nieuprawnione przetwarzane danych osobowych poprzez przesłanie niezamówionej informacji na adres e-mail.

W przypadku tego zawiadomienia sprawa miała charakter związany z rozsyłaniem w sposób automatyczny informacji handlowej do szerokiego grona odbiorców przez nieustalonego sprawcę (*spamming*). Ze względu na masowy charakter tego czynu ustalenie sprawcy nie było możliwe.

4) wprowadzenie w błąd pokrzywdzonego w trakcie zakładania konta w serwisie obsługującym płatności internetowe w celu pozyskania jego danych osobowych, a następnie wykorzystanie ich przy zakładaniu internetowego rachunku bankowego.

Ten stan faktyczny powiązany był z próbą oszustwa (art. 286 § 1 k.k.). Jego sprawca, nie będąc upoważnionym do przetwarzania danych osobowych, wykorzystał je w celu realizacji znamion innego przestępstwa.

5) udostępnienie danych osobowych osoby fizycznej bez jej zgody osobom nieuprawnionym przez osobę administrującą danymi.

To najczęściej występująca grupa zawiadomień na podstawie art. 51 u.o.d.o. Zawiadomienia w tego rodzaju przypadkach dotyczyły: nieuprawnionego ujawnienia danych osobowych na stronie internetowej, w prasie i telewizji; błędnie wysłanych faktur VAT, udostępnienia danych przez towarzystwo ubezpieczeniowe podmiotowi trzeciemu, umożliwienia dostępu do danych osobowych mieszkańców spółdzielni podmiotom trzecim, przesłania przez bank korespondencji przeznaczonej dla innej osoby, udostępnienia przez administratora dostępu do skrzynki e-mailowej, przesłania przez komornika danych dłużnika podmiotowi nieupoważnionemu.

Wystąpiła również forma nieumyślna takiego udostępnienia w postaci zagubienia przesyłki listowej przez doręczyciela.

6) bezprawnego wykonania kopii danych osobowych z bazy firmowej.

To potencjalnie częste zjawisko, choć w ramach analizowanych postępowań, wystąpiło w niewielu przypadkach. *Modus operandi* sprowadzał się do nieuprawnionego dostępu do danych firmowych przez byłego pracownika firmy, który po skopiowaniu ich, wykorzystał je w kontaktach w ramach nowego zatrudnienia.

7) niedopełnienie obowiązku informacyjnego.

Prawidłowe przetwarzanie danych osobowym wiąże się z szeregiem obowiązków informacyjnych, nałożonych przez ustawę na administratora danych (art. 24 i 25 u.o.d.o.). Brak ich realizacji skutkować może odpowiedzialnością takiego administratora na podstawie art. 54 u.o.d.o. Zawiadomienia w analizowanych sprawach dotyczyły naruszenia tych obowiązków w szeregu różnych sytuacjach, np. przez osobę odpowiedzialną za przechowywanie akt osobowych pracowników, czy administratora strony internetowej.

3.2.3. Uwagi szczegółowe

Rozpatrując naruszenia ustawy o ochronie danych osobowych od strony dolegliwości takich czynów dla osób nimi poszkodowanymi stwierdzić należy, że potencjalnie największe możliwości niezgodnego z prawem przetwarzania danych osobowych mogą mieć miejsce w sieci Internet.

Dla realizacji szeregu usług, klienci zobowiązani są do podawania nie tylko ich imienia i nazwiska czy adresu e-mail, ale takich danych jak numer karty kredytowej czy numer identyfikacyjny (PESEL). Dane te, nieprawidłowo przechowywane, mogą dostać się w posiadanie osób nieuprawnionych i zostać wykorzystane w celach, które mogą wyrządzić szkodę ich posiadaczowi. W takich przypadkach zachowania przestępcze sprawców zostaną zakwalifikowane bądź jako odrębne typy przestępstw, albo w ramach kwalifikacji kumulatywnej z występkami określonymi w ustawie.

Na gruncie ustawy o ochronie danych osobowych nieuprawnione wykorzystanie danych osobowych może przybrać m.in. postać przetwarzania adresu poczty e-mail osoby pokrzywdzonej w celu przesyłania niezamówionej informacji handlowej. O ile informacja taka zawiera dane identyfikujące administratora, zgłoszenie naruszenia

przepisów ustawy będzie stosunkowo proste. Jeżeli zaś ma charakter wysyłki masowej, bez takich danych ustalenie sprawcy czynu może być bardzo trudne lub niemożliwe. Szczególnie jeżeli posłużenie się adresem pocztowym pokrzywdzonego realizowane jest w ramach serwerów pocztowych wykorzystywanych do rozsyłania tzw. spamu.

Przykład: „*Dokonane ustalenia w sprawie odnoszące się do adresów poczty elektronicznej, z których kierowano wiadomości do pokrzywdzonego oraz informacje uzyskana od dostawcy usług internetowych wskazują nie tylko na to, że faktyczne ustalenie sprawców czynu z art. 49 ust. 1 u.o.d.o. jest niemożliwe, ale również na niecelowość ewentualnych dalszych czynności dowodowych w sprawie. Jak wynika z materiałów postępowania wiadomości były kierowane do pokrzywdzonego przez kilkadziesiąt osób, których adresy wskazują na siedziby czy też miejsca zamieszkania w kilkunastu krajach świata takich jak: Wielka Brytania, Niemcy, Włochy, Dania, Finlandia, USA, ale również: Indie, Nowa Zelandia, Kolumbia, Kanada czy Ukraina. Natomiast wiadomości kierowane do pokrzywdzonego z adresów poczty elektronicznej umieszczonych na terenie kraju, już w przypadku sprawdzenia pierwszego z tych adresów doprowadziły do ustalenia, że adres taki nie istnieje.*

W niniejszej sprawie nie sposób nie zauważyć, że wiadomości kierowane na adresy poczty elektronicznej pokrzywdzonego stanowią typowy objaw zjawiska zwanego spammingiem, które jest efektem szerokiego dostępu do Internetu w dzisiejszym społeczeństwie. O okolicznościach takich świadczą już same wydruki kierowanych do pokrzywdzonego wiadomości, gdyż w wielu z nich można zauważyć wpis „spam deteced" już w samym temacie wiadomości. Twierdzenia, iż osoby które albo przesyłają albo koordynują przesyłanie spamu na adresy poczty elektronicznej innych osób, w większości uzyskane przez nieuwagę samych użytkowników sieci Internet w każdym przypadku dopuszczają się przestępstwa z art. 49 ust. 1 u.o.d.o. w żadnym razie nie przystają do rzeczywistości wirtualnej, a nie też do możliwości wykrywczych, którymi dysponują organy ścigania. Zauważyć należy, że uzyskanie adresu poczty elektronicznej przez spamerów jest często niezależne od samego użytkownika takiej poczty, gdyż odpowiednie programy przeszukują niejednokrotnie nie tylko skrzynki adresowe tych użytkowników, których adresy uzyskano, ale również skrzynki adresowe innych osób, z którymi dana osoba korespondowała. Utrzymanie poufności swojego adresu poczty elektronicznej w tych warunkach jest praktycznie niemożliwe, w związku z czym otrzymywanie spamu stało się codziennością każdej niemal osoby posiadającej pocztę elektroniczną i to bez względu na stopień zabezpieczenia czy filtry funkcjonujące na serwerach dostawcy usługi internetowej. Mimo to, profilaktyka postępowania w takich przypadkach pozwala na łatwe i skuteczne usuwanie zagrożenia przez natychmiastowe kasowanie wiadomości – spamu bez

otwierania jakichkolwiek załączonych plików czy linków. Takie postępowanie stanowi dziś o minimalnej świadomości właściwego zachowania się w ramach użytkowania Internetu.

Odnosząc się do realiów przedmiotowej sprawy zaznaczyć należy, że powszechność zjawiska pojawiania się spamu i treść art. 49 ust. 1 u.o.d.o. prowadzi do trudnych do zaakceptowania wniosków, iż czysty formalizm postępowania karnego i obowiązująca w nim zasada legalizmu zmuszałyby organy ściągania w Polsce do prowadzenia setek postępowań o ogólnoświatowym zasięgu w celu wykrycia osób, które przetwarzały prawdopodobnie dane setek osób i to najczęściej bez aktywnego swojego udziału, a jedynie z wykorzystaniem zautomatyzowanych procesów informatycznych. W tych okolicznościach zasadne jest powołane się na zasady ekonomiki postępowania i oportunizmu przez stwierdzenie, że podjęcie jakichkolwiek dalszych czynności w niniejszej sprawie jest całkowicie niecelowe, a dokonane czynności wskazują na niemożność wykrycia ewentualnych sprawców. Wypada także zauważyć, że jakiekolwiek próby kierowania ewentualnych sprawców są z góry skazane na niepowodzenie z uwagi na ograniczenia wynikające z niewykonywania pomocy międzynarodowej de minimis (w sprawach błahych). Okoliczności powyższe powinny być w każdym przypadku uwzględniane w przypadku kierowania do dalszego prowadzenia przez prokuraturę spraw, których przeprowadzenie pod względem dowodowym jest w praktyce niewykonalne." (1 Ds. 1596/14).

W kilkunastu analizowanych przypadkach zawiadomienie o naruszeniu przepisów ustawy o ochronie danych osobowych skutkujących odpowiedzialnością karną sprawcy dotyczyło sytuacji, w której osoby pokrzywdzone odpowiadały na zamieszczone na stronach internetowych ogłoszenia o pracy, podając wymagane w ogłoszeniu dane osobowe. Brak odpowiedzi na przesłane ogłoszenie powodował u nich poczucie, iż ich dane zostały w sposób nieuprawniony wykorzystane. Stąd wnosiły zawiadomienie o popełnieniu przestępstwa.

Zauważyć jednak należy, że w tych przypadkach nie dochodziło do nieuprawnionego przetwarzania danych osobowych przez ich administratora, bowiem dane te były przez ich dysponentów dobrowolnie przekazywane w celach związanych z aplikowaniem o pracę. Z tego też powodu odmowy wszczęcia postępowania czy umorzenia postępowania były jak najbardziej zasadne.

Uwaga powyższa odnosi się również do wszelkiego rodzaju innych przypadków, w których doszło do dobrowolnego podania danych osobowych przez ich

dysponentów (np. konkursy telefoniczne), niezależnie od środka komunikacji, za pośrednictwem którego dane takie zostały przekazane (Internet, telefon).

> **Przykład:** *„Analizując zebrany w sprawie materiał zauważyć należy, iż zawiadamiający odpowiadając na przedmiotowe ogłoszenie w portalu internetowym oraz przesyłając swoje dane działa na własną odpowiedzialność i ryzyko, a więc wbrew ocenie pokrzywdzonego, brak jest cech przestępstwa stypizowanego w art. 49 ustawy o ochrony danych osobowych z dnia 29.08.1997 r. Z treści zawiadomienia nie wynika, aby doszło do popełnienia przestępstwa zawartego w wyżej wymienionej ustawie lub innych ustawach szczególnych. Wobec czego w przedmiotowej sprawie należy odmówić wszczęcia dochodzenia na zasadzie art. 17 § 1 pkt 2 wobec braku znamion czynu zabronionego." (1 Ds. 1139/14).*

> **Przykład:** *„Analiza zgromadzonego w niniejszej sprawie materiału dowodowego prowadzi do wniosku, iż czyn opisywany przez [zawiadamiającą] nie wyczerpuje ustawowych znamion przestępstwa, zwłaszcza przestępstwa wskazanego w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Ustawa nie typizuje przestępstwa posłużenia się cudzymi danymi osobowymi, penalizuje natomiast takie zachowania jak nieuprawnione przetwarzanie ich w zbiorze czy udostępnianie ich przez administratora. Przetwarzanie i wykorzystanie danych dobrowolnie przekazanych przez [zawiadamiającą], w celu podpisania z nią umowy zlecenie, również nie może być rozpatrywane w kategoriach występku stypizowanego w ustawie o ochronie danych osobowych. Jej dane zostały bowiem udostępnione przez nią samą osobie podającej się za prowadzącego działalność gospodarczą, a nie znalazły się z kolei w zbiorze danych ani też nie posłużyła się nimi osoba upoważniona do administrowania danymi osobowymi. Samo podpisanie umowy nie stanowi przestępstwa, a zawiadamiająca może dochodzić swoich roszczeń z niewywiązania się przez drugą stronę tej umowy z jej warunków, na drodze cywilnej. Zauważyć bowiem należy, że zgodnie z art. 22 § 1 kodeksu pracy, pracodawca ma prawo żądać od osoby ubiegającej się o zatrudnienie podania danych osobowych." (2 Ds. 672/14).*

Dla powstania odpowiedzialności sprawcy z tytułu niedopuszczalnego przetwarzania danych osobowych lub nieuprawnionego przetwarzania takich danych niezbędne jest ustalenie, iż przetwarzanie takie miało miejsce w zbiorze danych.

Ustawa w art. 7 pkt 1 definiuje, co należy rozumieć przez zbiór danych. Zgodnie z tą definicją jest to każdy posiadający strukturę zestaw *danych* o charakterze *osobowym*, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie. Przetwarzanie danych poza

zbiorem nie będzie zatem wyczerpywać znamion przestępstwa z art. 49 u.o.d.o. W szczególności dotyczyć to będzie przypadków, w których do przekazania danych osobowych dochodzi wyłącznie na potrzeby realizacji jednorazowej czynności prawnej, np. wynikającej z umowy sprzedaży rzeczy pomiędzy osobami fizycznymi, i poza tym dane nie będą w inny sposób wykorzystywane, a samo zawiadomienie wynika z problemów powstałych na tle realizacji umowy.

Na marginesie warto dodać, że ustawa o ochronie danych osobowych, o czym będzie mowa w dalszej części opracowania, zezwala na przetwarzanie danych bez odrębnej zgody osoby uprawnionej.

> **Przykład:** *„Analizując w tym zakresie zgromadzony w sprawie materiał dowodowy stwierdzić należy, iż czyn opisany przez [zawiadamiającego] nie zawiera znamion czynu zabronionego z art. 49 ust. 1 ustawy o ochronie danych osobowych. Do wyczerpania znamion czynu zabronionego z art. 49 ust. 1 ustawy o ochronie danych osobowych należy działanie sprawcy na zbiorze danych osobowych. Natomiast, aby działanie sprawcy mogło być uznane za wyczerpujące znamiona przestępstwa stypizowanego w komentowanym przepisie, dane osobowe muszą stać się elementem zbioru danych osobowych w rozumieniu art. 7 pkt 1 przywołanej ustawy i w tym właśnie zbiorze musi dochodzić do ich przetwarzania wbrew przepisom ustawy o ochronie danych osobowych. Przetwarzanie danych osobowych w sytuacji, gdy takie przetwarzanie nie jest dopuszczalne albo poprzez przetwarzanie danych przez osobę nieuprawnioną do takiego przetwarzania nie stanowi przestępstwa, jeżeli dane osobowe nie są przetwarzane w zbiorze danych.*
>
> *Za zbiór danych uważa się natomiast każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie. Bezspornym jest zatem, iż dane osobowe dotyczące zawiadamiającego, które zostały uzyskane prywatnie (…) nie stanowią zbioru danych w rozumieniu ustawy o ochronie danych osobowych. Ich przetwarzanie nie wypełniło zatem znamion czynu zabronionego z art. 49 ust. 1 ustawy.*
>
> *Celem ustawodawcy regulującego kwestie karne dotyczące ochrony danych osobowych była bowiem penalizacja czynów popełnionych przez podmioty związane z administrowaniem danych osobowych właśnie na zbiorach danych. W pozostałym zakresie ustawodawca nie przewidział karnoprawnej ochrony przetwarzania danych osobowych, pozostawiając pokrzywdzonym możliwość dochodzenia swoich praw na drodze powództwa cywilnego o ochronę dóbr osobistych.” (5 Ds. 2108/13).*

Przestępstwo z art. 51 ustawy może zostać popełnione wyłącznie przez osobę administrującą danymi lub obowiązaną do ochrony danych osobowych. Z tego też powodu skierowanie zawiadomienia przeciwko osobie, na której nie ciążą takie obowiązki, skutkować musi odmową wszczęcia lub umorzeniem postępowania.

> **Przykład:** *„Analizując zebrany w sprawie materiał zauważyć należy, iż wskazana osoba nie jest administratorem danych w rozumieniu ustawy, czyli osobą fizyczną, która ze względu na zajmowane stanowisko lub powierzone jej obowiązki jest upoważniona do decydowania o celach i środkach przetwarzania baz danych. Reasumując, aby doszło do przestępstwa stypizowanego w dyspozycji art. 51 ustawy o ochronie danych osobowych osobą naruszającą wyżej wymieniony artykuł musi być osoba administrująca zbiorem danych osobowych oraz osoba obowiązana do ochrony danych osobowych. W tym przypadku wskazany nie jest osobą odpowiadającą z powyższego artykułu. Wobec czego w przedmiotowej sprawie należy odmówić wszczęcia dochodzenia na zasadzie art. 17 § 1 pkt 2 wobec braku znamion czynu zabronionego.” (1 Ds. 1138/14).*

Odrębna grupa zawiadomień o popełnieniu przestępstwa dotyczyła przypadków reklamowania produktów przez firmy, z którymi osoba fizyczna miała podpisane umowy na świadczenie jej usług.

Zawierając umowę z dostawcą usług, osoba fizyczna poinformowana powinna zostać m.in. o dobrowolności albo obowiązku podania jej danych, przy czym w sytuacji istnienia obowiązku prawnego, o jego podstawie prawnej (art. 24 ust. 1 pkt 4 u.o.d.o.), które to dane będą następnie przetwarzane przez dostawcę – administrującego tymi danymi.

W powszechnej świadomości pojawiło się w związku z tym przekonanie, że każde przetwarzanie danych osobowych w celach marketingowych wymaga uzyskania dobrowolnej zgody uprawnionego na ich wykorzystywanie w związku z rozsyłaniem informacji handlowej.

Z tego też powodu w części zawiadomień pojawiły się informacje o naruszeniu obowiązku uzyskania takiej zgody przez podmiot je przetwarzający. Tymczasem, w wyniku przeprowadzonego postępowania, okazywało się, że przedmiotowe zawiadomienia wynikały z nieznajomości prawa przez osoby je składające.

Zgodzić się należy, że zgoda na wykorzystanie danych osobowych dla celów marketingowych jest wymagana, gdyż możliwość ich wykorzystania w takim celu nie wynika z podstaw przetwarzania danych określonych w art. 23 ust. 1 u.o.d.o. W szczególności przesłanie informacji marketingowej nie jest niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa, jak również nie jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą, czy też nie jest ono niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego.

Jednakże ustawa sama wskazuje, iż jednym z prawnie usprawiedliwionych celów przetwarzania danych osobowych jest marketing bezpośredni własnych produktów lub usług administratora danych. Oznacza to, że w tych przypadkach podmiot przetwarzający dane, posiadający zawartą umowę z klientem, nie jest obowiązany do uzyskania odrębnej zgody uprawnionego na przetwarzanie jego danych osobowych w związku z marketingiem usług własnych. Zgoda taka byłaby jednak potrzebna, gdyby marketing dotyczył usług podmiotu trzeciego.

> **Przykład:** „*Odnośnie zastrzeżeń zgłoszonych przez [zawiadamiającego], który wyraził sprzeciw co do przetwarzania jego danych osobowych w celach marketingowych, to [zawiadamiający] nie wyraził zgody na przetwarzanie jego danych osobowych przez [spółkę X] w celach marketingu podmiotów trzecich. Nie jest to tożsame z niemożliwością przetwarzania danych osobowych w celach marketingowych przez [spółkę X] w ogóle, bowiem zgodnie z ustawą o ochronie danych osobowych prowadzenie marketingu własnych produktów, a takim jest program lojalnościowy współorganizowany przez [spółkę X] dla klientów [spółki X]; nie wymaga zgody osoby, której dane dotyczą, jest to bowiem wykorzystanie danych przez administratora danych, w usprawiedliwionym celu. W powyższym przypadku [spółka X] nie udostępniła danych osobowych innemu podmiotowi, wykorzystała je jedynie w ramach własnego programu lojalnościowego. (…) Mając powyższe na uwadze, działając na zasadzie art. 17 § 1 pkt 2 k.p.k. wobec braku znamion czynu zabronionego postanowiono jak na wstępie.” (1 Ds. 1568/14).*

Nie może być mowy o naruszeniu przepisów ustawy o ochronie danych osobowych w tych przypadkach, gdy posłużenie się nimi przez określone podmioty wynika z przepisów prawa. Z taką sytuacją będziemy mieli do czynienia np. w razie

dochodzenia przez wierzyciela jego praw w związku z zaległościami w płatnościach przez dłużnika, czy też w związku z działaniami podejmowanymi przez komornika w postępowaniu egzekucyjnym na podstawie przepisów kodeksu postępowania cywilnego.

Należy zauważyć też, że szczególnej ochronie przepisów ustawy o ochronie danych osobowych nie podlegają dane osobowe osób fizycznych prowadzących działalność gospodarczą w zakresie ujawnionym w Centralnej Ewidencji Działalności Gospodarczej.

> **Przykład:** *„Nie ulega wątpliwości, że zarówno numer PESEL jak i NIP, a także imię i nazwisko [zawiadamiającego] podane w zawiadomieniu, zgodnie z art. 6 u.o.d.o. stanowią jego dane osobowe, chronione przepisami ustawy. Niewątpliwym jest również fakt, iż komornik jako administrator danych osobowych w rozumieniu u.o.d.o., zgodnie z jej art. 36 ust .1, obowiązany jest zastosować środki techniczne i organizacyjne zapewniającego ochronę danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Jeżeli chodzi zaś o umieszczenie danych osobowych dłużnika w zawiadomieniu o zajęciu wierzytelności z rachunku bankowego, to w istocie, zgodnie z art. 7 ust. 2 u.o.d.o., czynność taka stanowiła formę przetwarzania danych osobowych.*
>
> *Umieszczenie numeru PESEL oraz NIP dłużnika w kierowanym do banku zawiadomieniu o zajęciu wierzytelności z rachunku bankowego nie mogło jednak realizować znamion przestępstwa z art. 51 ust. 1 u.o.d.o., dla których realizacji wymagane jest udostępnienie chronionych danych osobom nieupoważnionym.*
>
> *Osobą nieupoważnioną w rozumieniu art. 51 ust. 1 u.o.d.o. jest osoba, która nie należy do kategorii podmiotów uprawnionych do otrzymania danych na podstawie przepisów prawa, a więc która otrzymała dostęp do danych osobowych z pogwałceniem przepisów art. 23 lub 27 u.o.d.o.*
>
> *Jako że w przypadku numeru PESEL oraz NIP nie mamy do czynienia z danymi szczególnie wrażliwymi, zdefiniowanymi w art. 27 u.o.d.o., przywołać należy podstawy zgodnego z prawem przetwarzania danych osobowych, wymienione w art. 23 u.o.d.o. Jedną z takich podstaw, jest wymieniona w art. 23 ust. 2 u.o.d.o. konieczność przetworzenia danych dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. W opisywanym przypadku obowiązkiem takim jest egzekwowanie przez komornika świadczeń*

stwierdzonych tytułem wykonawczym. Podstawą przetwarzania danych osobowych w toku postępowania egzekucyjnego jest również wykonywanie prawem określonych zadań realizowanych dla dobra publicznego, jakim jest właśnie postępowanie egzekucyjne. Wszystkie wymagane podstawy prawne przetwarzania danych osobowych przez komornika znajdziemy w przepisach ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego, ustawy z dnia 29 sierpnia 1997 r. o komornikach sądowych i egzekucji oraz rozporządzenia Ministra Sprawiedliwości z dnia 9 marca 1968 r. w sprawie czynności komorników.

Czyn komornika (…), polegający na umieszczeniu w zawiadomieniu numeru PESEL oraz NIP [zawiadamiającego] stanowił niezbędny element realizacji celów postępowania egzekucyjnego, w postaci indywidualizacji osoby dłużnika i umożliwienia zajęcia jego wierzytelności z rachunku bankowego, a więc wypełnienia przez niego obowiązku egzekwowania świadczenia stwierdzonego tytułem wykonawczym. W przypadku braku numeru rachunku dłużnika, nie podanie w zawiadomieniu jego numeru PESEL i NIP prowadziłoby do niemożności zidentyfikowania rachunku bankowego, a w rezultacie braku skuteczności zawiadomienia i udaremnienia egzekucji.

Zgodnie z art. 889 § 2 k.p.c. odpis zawiadomienia o zajęciu wierzytelności z rachunku bankowego otrzymał również wierzyciel. W toku czynności nie udostępniono danych osobowych [zawiadamiającego] żadnym innym osobom.

W związku z faktem, iż zarówno bank, jak i wierzyciel w zaistniałych okolicznościach stanowiły podmioty uprawnione do otrzymania od komornika danych osobowych dłużnika, zgodnie z przytoczonymi powyżej przepisami, czyn [komornika] nie realizował znamion przestępstwa z art. 51 ust. 1 u.o.d.o., gdyż nie ujawniono danych osobowych [zawiadamiającego] żadnymi innym osobom." (3 Ds. 165/14).

W części zawiadomień odnotowano nieznajomość przepisów ustawy o ochronie danych osobowych przez osoby zgłaszające. W szczególności dotyczy to przypadków naruszenia realizacji obowiązków informacyjnych przez administrującego danymi.

Jak to już wskazano powyżej, administrator danych obowiązany jest wobec osoby, której dane będzie przetwarzał, do poinformowania jej o:

1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku;

2) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych;

3) prawie dostępu do treści swoich danych oraz ich poprawiania;

4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej (art. 24 ust. 1 u.o.d.o.).

Natomiast w przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o:

1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku;

2) celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych;

3) źródle danych;

4) prawie dostępu do treści swoich danych oraz ich poprawiania;

5) uprawnieniach wynikających z art. 32 ust. 1 pkt 7 i 8 (art. 25 ust. 1 u.o.d.o.).

Z kolei art. 33 ust. 1 u.o.d.o. wskazuje, iż administrator danych, na wniosek osoby, której dane dotyczą, jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić, odnośnie do jej danych osobowych, informacji, o których mowa w art. 32 ust. 1 pkt 1-5a[48].

[48] Art. 32 ust 1 pkt 1 – 5a stanowi, iż „każdej osobie przysługuje prawo do kontroli przetwarzania *danych*, które jej dotyczą, zawartych w zbiorach *danych*, a zwłaszcza prawo do:
1) uzyskania wyczerpującej informacji, czy taki zbiór istnieje, oraz do ustalenia administratora *danych*, adresu jego siedziby i pełnej nazwy, a w przypadku gdy administratorem *danych* jest osoba fizyczna - jej miejsca zamieszkania oraz imienia i nazwiska;
2) uzyskania informacji o celu, zakresie i sposobie przetwarzania *danych* zawartych w takim zbiorze;
3) uzyskania informacji, od kiedy przetwarza się w zbiorze *dane* jej dotyczące, oraz podania w powszechnie zrozumiałej formie treści tych *danych*;
4) uzyskania informacji o źródle, z którego pochodzą *dane* jej dotyczące, chyba że administrator *danych* jest zobowiązany do zachowania w tym zakresie w tajemnicy informacji niejawnych lub zachowania tajemnicy zawodowej;
5) uzyskania informacji o sposobie udostępniania *danych*, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym *dane* te są udostępniane;

Dlatego też zawiadomienia, w których nie wskazywano na naruszenie tego terminu w związku ze złożeniem takiego wniosku, nie mogły zostać rozpoznane w inny sposób, niż umarzający wszczęte postępowanie w sprawie o czyn z art. 54 u.o.d.o.

> **<u>Przykład:</u>** *„Zgodnie z art. 33 ust. 1 ustawy o ochronie obrony danych osobowych na wniosek osoby, której dane dotyczą, administrator danych jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić, odnośnie do jej danych osobowych, informacji, o których mowa w art. 32 ust. 1 pkt 1 - 5a. Odpowiedzialność z art. 54 ustawy o ochronie danych osobowych ponosi ten, kto administrując zbiorem danych nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystania z praw przyznanych jej w tej ustawie.*
>
> *W piśmie z dnia (…) skarżący nie zwracał się o poinformowanie go o jego prawach, stąd zaniechania w tym zakresie i w tym czasie nie sposób uznać za bezprawne. Skarżący nadto nie żądał też udzielenia informacji na piśmie, a tylko w takiej sytuacji informacja ta jest udzielana na piśmie (art. 33 ust. 2). Zaniechanie więc w tej sytuacji udzielenia pisemnej odpowiedzi również nie może być potraktowane jako bezprawne, a tym bardziej umyślne. Dalej zauważyć należy, iż art. 54 ustawy o ochronie danych osobowych nie penalizuje każdej sytuacji nieudzielenia informacji a tylko sytuację dotyczącą nieudzielania informacji uniemożliwiającej wykonywania praw z ustawy. Skarżący zważywszy, że był zatrudniony w spółce dysponował wiedzą, co do tego kto jest administratorem jego danych osobowych, w jakim zakresie i celu były pozyskane, od kiedy zostały pozyskane (data zatrudnienia), a więc mógł w tym zakresie wykonywać swoje prawa z ustawy. Pomijając kwestię znamion czynu zabronionego, nie sposób tu zatem mówić o społecznej szkodliwości wyższej niż znikoma.” (III Kp 695/14).*

Podsumowując należy stwierdzić, że analiza wnoszonych zawiadomień o popełnieniu przestępstw określonych w ustawie o ochronie danych osobowych sygnalizuje pozytywne zjawisko polegające na tym, że coraz więcej osób jest wyczulonych na naruszenia i bezprawne próby wykorzystywania ich danych, choćby w wyniku przeprowadzonego postępowania okazywało się, że działania lub zaniechania podmiotów wskazywanych jako sprawcy naruszeń nie stanowiły czynu zabronionego. W tym miejscu warto jednak wskazać na potrzebę prowadzenia szeroko zakrojonej akcji informacyjnej na temat przepisów ustawy o ochronie danych osobowych, która wyjaśniałaby, w jakich przypadkach ujawnienie takich danych jest

---

5a) uzyskania informacji o przesłankach podjęcia rozstrzygnięcia, o którym mowa w art. 26a ust. 2.

prawnie dopuszczalne. Przyczynić to by się mogło do wyeliminowania, co najmniej części nieuzasadnionych zawiadomień o przestępstwie, a tym samym oszczędziłoby niepotrzebnej pracy organom ścigania.

3.2.4. Kwalifikacja prawna czynu

W znacznej większości analizowanych przypadków spraw o występki z ustawy o ochronie danych osobowych kwalifikacja prawna czynu dotyczyła wyłącznie typu przestępstwa, do którego odnosiło się zawiadomienie, tj. poszczególnych występków określonych w ustawie.

Przypadki, w których dochodziło do zbiegu lub kwalifikacji kumulatywnej z innymi przepisami wystąpiły w zaledwie kilkunastu przypadkach. Przy czym, przede wszystkim, były to kwalifikacje z innymi występkami z ustawy o ochronie danych osobowych (art. 49 ust. 1 w zb. z art. 51 ust. 1 ustawy w zw. z art. 11 § 2 k.k., czy art. 51 ust. 2 w zb. z art. 52 u.o.d.o.).

Jedynie w 7 przypadkach, za podstawę przyjęto kwalifikację z przestępstwami stypizowanymi w kodeksie karnym. Były to:

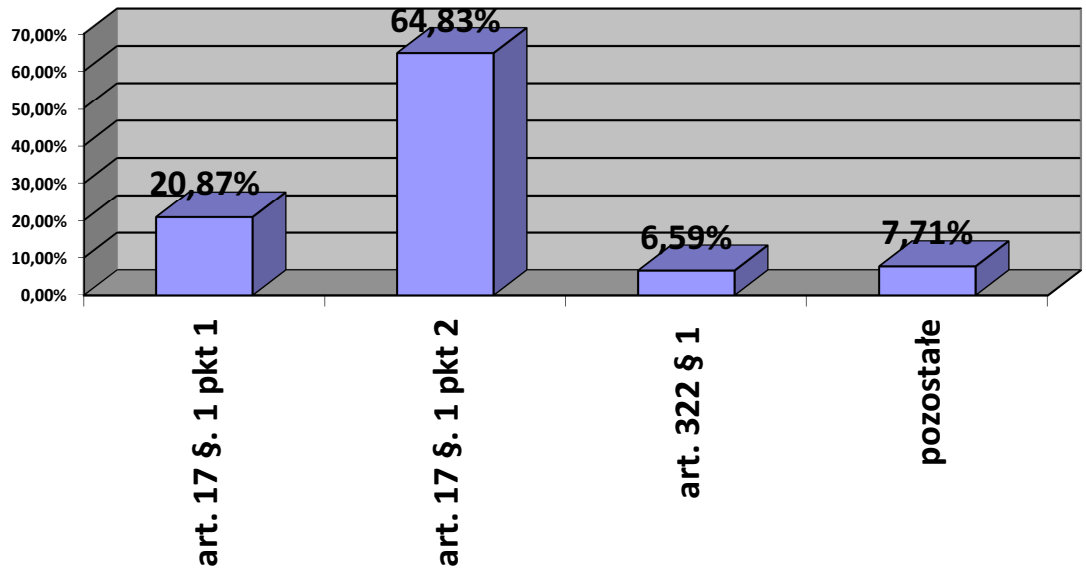
- art. 13 § 1 k.k. w zw. z art. 49 ust. 1 u.o.d.o. w zb. z art. 286 § 1 k.k. w zw. Z art. 11 § 2 k.k. (2 przypadki),
- art. 49 ust. 1 u.o.d.o. i art. 190a § 1 k.k.,
- art. 231 § 1 i art. 51 § 1 u.o.d.o. w zw. z art. 11 § 2 k.k. (3 przypadki),
- art. 231 § 1 k.k., art. 266 § 1 k.k. i art. 51 u.o.d.o. w zw. z art. 11 § 2 k.k.

3.2.5. Podstawy odmów/ umorzeń postępowania

Jak wynika z wykresu nr 6 przeważająca większość postępowań została umorzona na podstawie art. 17 § 1 pkt 2 k.p.k., czyli w oparciu o stwierdzenie, iż czyn nie zawiera znamion czynu zabronionego (prawie 65% badanych spraw).

W kolejnych niemal 21% przypadków podstawę odmowy lub umorzenia postępowania stanowiła przesłanka z art. 17 § 1 pkt 1 k.p.k., tj. w następstwie stwierdzenia, iż czynu nie popełniono.

Wykres 6 - Podstawy prawne zakończenia postępowań (w procentach)



Pozostałe 14% obejmowało takie przesłanki zakończenia postępowania jak: art. 305 § 1 k.p.k., art. 322 § 1 k.p.k., art. 17 § 1 pkt 6 k.p.k., art. 17 § 1 pkt 1 i 2 k.p.k. oraz art. 305 § 1 w zw. z art. 325a § 2 k.p.k.

W niewiele ponad 24% przypadków decyzja o odmowie wszczęcia postępowania lub o jego umorzeniu została zaskarżona, w tym w ponad 81% przez zawiadamiającego o popełnieniu przestępstwa. W 54% przypadków zażalenie to nie zostało uwzględnione.

3.2.6. Czas trwania postępowania

Stwierdzić należy, że analizowane postępowania w większości przypadków prowadzone były sprawnie i szybko.

W grupie postępowań zakończonych odmową wszczęcia postępowania – okres czasu pomiędzy wpłynięciem zawiadomienia, a wydaniem postanowienia o odmowie w niemal 65% przypadków nie przekraczał 1 miesiąca. W kolejnych ponad 24% wynosił od 1 do 2 miesięcy. W pozostałych 11% wynosił ponad 2 miesiące (max. 6 miesięcy).

W grupie postępowań zakończonych umorzeniem postępowania pomiędzy wszczęciem a wydaniem postanowienia o umorzeniu - w przypadku ponad 21% spraw nie upłynął nawet jeden miesiąc. W ponad 32% przypadków postępowanie toczyło się powyżej 1 miesiąca do 2 miesięcy, w kolejnych 27% spraw – od 2 do 5 miesięcy. Pozostałe niemal 19% przypadków obejmuje postępowania toczone przez okres powyżej 5 miesięcy. W skrajnym przypadku było to 5 lat, co skutkowało decyzją o zakończeniu jego prowadzenia ze względu na przedawnienie karalności czynu nim objętego.

3.3. Sprawy zakończone prawomocnym orzeczeniem sądowym

3.3.1. Analiza postępowań sądowych

Stany faktyczne spraw zakończonych prawomocnym orzeczeniem sądowym nie różniły się istotnie od stanów faktycznych analizowanych w ramach postępowań przygotowawczych.

Zachowania przestępcze wyczerpywały znamiona tylko trzech typów przestępstw określonych w ustawie o ochronie danych osobowych: art. 49, art. 51 i art. 54.

W przypadku postępowań zakończonych na etapie postępowania sądowego zwraca jednak uwagę większa liczba spraw, w których oskarżonymi były osoby administrujące zbiorem danych lub będąc obowiązanymi do ochrony danych osobowych umożliwiły dostęp do nich osobom nieupoważnionym poprzez

wyrzucenie dokumentów zawierających dane osobowe (dokumentacji finansowo – księgowej, kopii umów pożyczek, umów z operatorem telekomunikacyjnym, akta osobowych pracowników) na śmietnik czy porzucenie ich w innymi miejscu (przesyłki pocztowe) albo pozostawienie ich w miejscu nieprawidłowo zabezpieczonym lub powierzenie dokumentacji w celu zabezpieczenia osobie nie powołanej do takiej ochrony. Osobom takim stawiano zarzut albo z art. 51 ust. 1 u.o.d.o. (udostępnienie danych albo umożliwienie dostępu do nich), albo z art. 52 u.o.d.o., tj. naruszenie obowiązku zabezpieczenia danych przed ich zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem.

Niewielką grupę spraw stanowiły przypadki udostępnienia danych osobowych pojedynczych osób fizycznych w Internecie lub na łamach gazet. Były to działania o charakterze nieumyślnym (np. przytoczenie w informacji prasowej nazwiska pokrzywdzonego) lub takie, w których celem sprawcy było przymuszenie osoby, której dane zostały ujawnione, do odpowiedniego zachowania się (zwrotu długu).

W dwóch przypadkach oskarżonymi byli funkcjonariusze państwowi, którzy przekraczając zakres swoich obowiązków, w sposób nieuprawniony otrzymali dostęp do baz danych zawierających dane osobowe obywateli albo udostępnili dane osobowe świadka do wiadomości publicznej, czym narazili dobro prowadzonego postępowania.

Z analizy stanów faktycznych spraw zakończonych na etapie postępowania sądowego wynika, że w większości przypadków naruszenie przez sprawców przepisów ustawy o ochronie danych osobowych, co skutkowało postawieniem im zrzutu popełnienia przestępstwa z art. 49 – 52 u.o.d.o., wynikała z nieznajomości przepisów lub nieświadomości sprawców co do ciążących na nich obowiązkach prawidłowego zabezpieczenia zbiorów danych przed ich ujawnieniem albo dostępem do nich przez osoby nieuprawnione. Świadczyć o tym może znaczna liczba uniewinnień czy umorzeń albo warunkowych umorzeń postępowania. Również w tych przypadkach, w których dochodziło do skazania sprawców, sąd wymierzał im – niewielkie – kary grzywny (samoistnej), uznając iż jest to wystarczająca kara za naruszenie przepisów ustawy.

Zawiadomienia o popełnieniu przestępstwa z ustawy o ochronie danych osobowych składane były przede wszystkim przez dwie grupy osób: pokrzywdzonych przestępstwem, których dane osobowe w sposób nieuprawniony zostały przetworzone lub udostępnione (niemal 29% zawiadomień) oraz osoby, które znalazły wyrzucone dokumenty zawierające dane osobowe innych osób i zawiadomiły o tym fakcie policję lub straż miejską (prawie 37% przypadków). W ponad 26% przypadków odnalezienie dokumentów zawierających dane osobowe, które zostały wyrzucone lub które były w sposób nienależny przechowywane nastąpiło na drodze czynności podejmowanych przez policję lub straż miejską. Pozostałe zawiadomienia złożone zostały w imieniu pokrzywdzonej osoby prawnej, przez prezesa spółdzielni mieszkaniowej oraz w ramach czynności podejmowanych przez Straż Graniczną.

Odnosząc się do kwalifikacji prawnej czynów sprawców przestępstw z ustawy o ochronie danych osobowych stwierdzić należy, że przede wszystkim występowały kwalifikacje samodzielne z poszczególnych artykułów ustawy: art. 49 ust. 1, art. 49 ust. 2, art. 51 ust. 1, art. 51 ust. 2 oraz art. 52. Stanowiły one ponad 76% wszystkich analizowanych przypadków. Ponadto występowały zbiegi pomiędzy poszczególnymi typami przestępstw z ustawy: art. 51 ust. 2 w zb. z art. 52, czy też art. 51 ust.1 w zb. z art. 51 ust. 2 ustawy.

Jedynie w 4 przypadkach (ponad 10%) doszło do wystąpienia kwalifikacji kumulatywnej z przepisami kodeksu karnego. Były to:

- art. 297 § 1 k.k. w zb. z art. 270 § 1 k.k. w zb. z art. 49 ust. 1 u.o.d.o. w zw. z art. 11 § 2 k.k.[49];
- art. 231 § 1 k.k i art. 49 § 1 u.o.d.o. w zw. z art. 11 § 2 k.k. w zw. z art. 91 § 1 k.k.;[50]

[49] W sprawie tej oskarżono pracownicę jednej ze Spółdzielczych Kas Oszczędnościowo Kredytowej (SKOK) zatrudnioną na stanowisku referenta, iż w celu uzyskania dla siebie pożyczek z tej kasy sporządziła szereg umów pożyczek na nazwiska osób fizycznych i podrobiła ich podpisy. Oskarżona została skazana na karę roku i 10 miesięcy pozbawienia wolności z warunkowym zawieszeniem jej wykonania na okres 5 lat oraz na karę grzywny w wysokości 2000 zł (po przeliczeniu ze stawek dziennych).

[50] Stan faktyczny polegał na przekroczeniu uprawnień przez funkcjonariusza publicznego w zakresie niezbędnym do wykonywania zadań – dostępu do bazy danych Centralnej Ewidencji Wydanych

- art. 18 § 2 k.k. w zw. z art. 266 § 1 k.k. w zw. z art. 51 ust. 1 u.o.d.o.[51];
- art. 231 § 1 k.k. i art. 51 ust. 1 u.o.d.o.[52]

Analizując czas trwania postępowań sądowych zauważyć należy, że nie należały one do takich, które były toczone przez długi okres czasu. Niemal 79% wszystkich postępowań zakończonych zostało wydaniem prawomocnego orzeczenia w okresie do 8 miesięcy od daty wniesienia aktu oskarżenia. Dłuższy czas trwania związany był z wniesieniem apelacji od wyroku.

Apelacje wniesiono w 21% spraw, z czego w ponad 62% była to apelacja prokuratora, w pozostałych – skazanego. W 50% przypadków zostały one uwzględnione, a sprawa przekazana do ponownego rozpoznania.

Warto odnotować, że w dwóch sprawach wniesiony został przez pokrzywdzonego subsydiarny akt oskarżenia. Jednak w obu z nich został następnie cofnięty, co skutkowało umorzeniem postępowania.

3.3.2. Rodzaje orzeczeń

W badanych postępowaniach zarzut popełnienia przestępstw z ustawy o ochronie danych osobowych postawiono 49 osobom. Szczegółowa charakterystyka sprawców została przedstawiona w dalszej części opracowania.

---

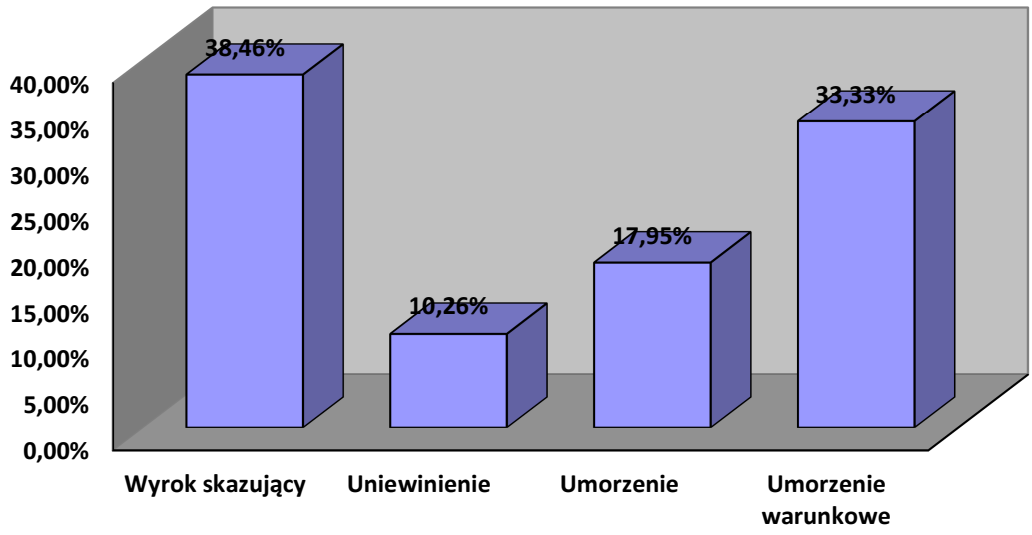
i Utraconych Paszportów w ten sposób, że bez uzasadnionej czynnościami zawodowymi przyczyny wprowadzał do tej bazy zapytania na podstawie imion i nazwisk oraz nr PESEL oraz innych danych osobowych, a następnie się z nimi zapoznawał, czym działał na szkodę interesu prywatnego tych osób. Postępowanie karne w stosunku do oskarżonego zostało warunkowo umorzone na okres 2 lat oraz orzeczono w stosunku do niego środek karny w postaci świadczenia pieniężnego w wysokości 3000 zł.

[51] W tej sprawie syn, powołując się na rzekome ustne pełnomocnictwo przekazane mu przez ojca, przekonał administratora danych osobowych w gabinecie stomatologicznym i wszedł, w sposób nieuprawniony, w posiadanie dokumentacji medycznej ojca, co stanowiło dodatkowo naruszenie tajemnicy lekarskiej. Postępowanie w stosunku do sprawcy zostało umorzone na podstawie art. 17 § 1 pkt 9 k.p.k.

[52] W przypadku tego postępowania funkcjonariusz publiczny nieumyślnie przekroczył swoje uprawnienia i nie dopełnił swoich obowiązków służbowych w ten sposób, że będąc zobowiązanym do ochrony danych osobowych świadków oraz do zachowania tajemnicy śledztwa, nie zachowując należytej ostrożności przesłał na szereg skrzynek e-mail portret pamięciowy sprawcy zabójstwa zawierający dane osobowe świadka, w oparciu o zeznania którego ten portret został opracowany, udostępniając tym samym te dane osobom nieupoważnionym. Postępowanie w stosunku do tego funkcjonariusza zakończyło się warunkowym umorzeniem na okres jednego roku.

W stosunku do 38,46% oskarżonych wydano wyrok skazujący (15 osób), wobec 17,95% - postępowanie zostało umorzone (7 osób) lub umorzone warunkowo na okres roku lub 2 lat (13 osób – 33,33%). W pozostałych 4 przypadkach wydano wyrok uniewinniający (10,26% oskarżonych).

Wykres 7 - Sposób zakończenia postępowania sądowego



Przestępstwa z ustawy o ochronie danych osobowych nie są zagrożone wysokimi sankcjami, bo maksymalnie do 3 lat pozbawienia wolności w przypadku typu kwalifikowanego występku z art. 49 ust. 1 u.o.d.o. Badanie pokazuje, że w grupie osób skazanych, karę pozbawienia wolności orzeczono tylko w stosunku do 20% z nich i wynosiła ona od 3 do 22 miesięcy. We wszystkich przypadkach jej wykonanie zawieszono na okres próby w wymiarze od 2 do 5 lat.

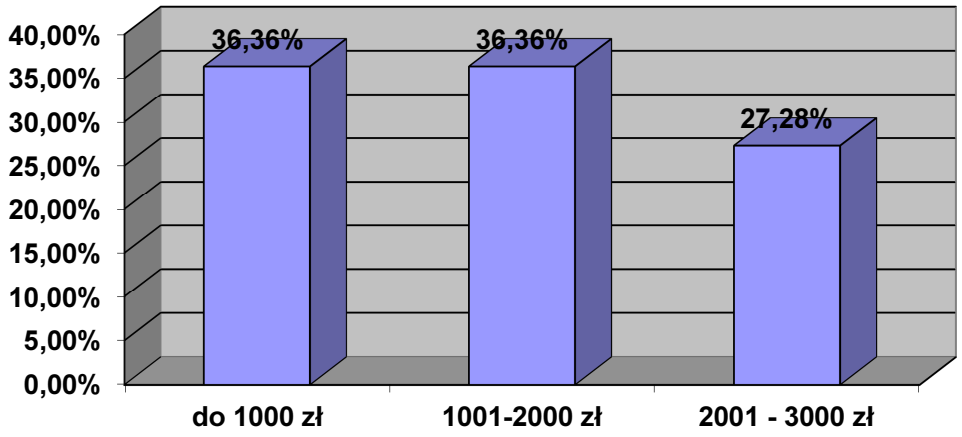
Wobec kolejnych 20% sprawców orzeczono – na podstawie art. 11 § 3 k.k. w zw. z art. 34 k.k. w zw. z art. 35 § 1 k.k. – karę ograniczenia wolności w wymiarze od 8 do 10 miesięcy w postaci nieodpłatnej, kontrolowanej pracy na cele społeczne w wymiarze od 20 do 36 godzin miesięcznie.

W stosunku do 9 skazanych (60%) orzeczono karę grzywny samoistnej, a wobec kolejnych 13% (2 osoby) - orzeczono grzywnę obok kary pozbawienia wolności.

W obu rodzajach orzeczone grzywny nie przekroczyły kwoty 3000 zł (po przeliczeniu ze stawki dziennej). Wskazać jednak należy, że ich wysokość była współmierna do społecznej szkodliwości czynu.

W jednym przypadku wykonanie kary grzywny zostało zawieszone na okres 2 lat – na podstawie art. 69 § 1 k.k. i art. 70 § 1 pkt 2 k.k.

Wykres 8 – Wysokość orzeczonej kary grzywny



W stosunku do 9 sprawców, wobec których zastosowano warunkowe umorzenie postępowania, orzekano dodatkowo świadczenie pieniężne w kwocie od 200 do 3000 zł., przy czym większość nie przekroczyła kwoty 800 zł.

Wobec 7 osób postępowanie karne zostało umorzone na podstawie art. 17 § 1 pkt 3 k.p.k. (społeczna szkodliwość czynu jest znikoma) albo w oparciu o art. 17 § 1 pkt 9 k.p.k. (brak skargi uprawnionego oskarżyciela).

3.3.3. Sprawcy przestępstw z ustawy o ochronie danych osobowych

W objętych badaniem postępowaniach zakończonych wydaniem prawomocnego wyroku skazującego w roku 2014 akt oskarżenia o popełnienie przestępstwa z art. 49 – 52 ustawy o ochronie danych osobowych skierowano przeciwko 39 osobom, w tym: w stosunku do 6 z art. 49 u.o.d.o., wobec 18 z art. 51 u.o.d.o. oraz 15 z art. 52 u.o.d.o.

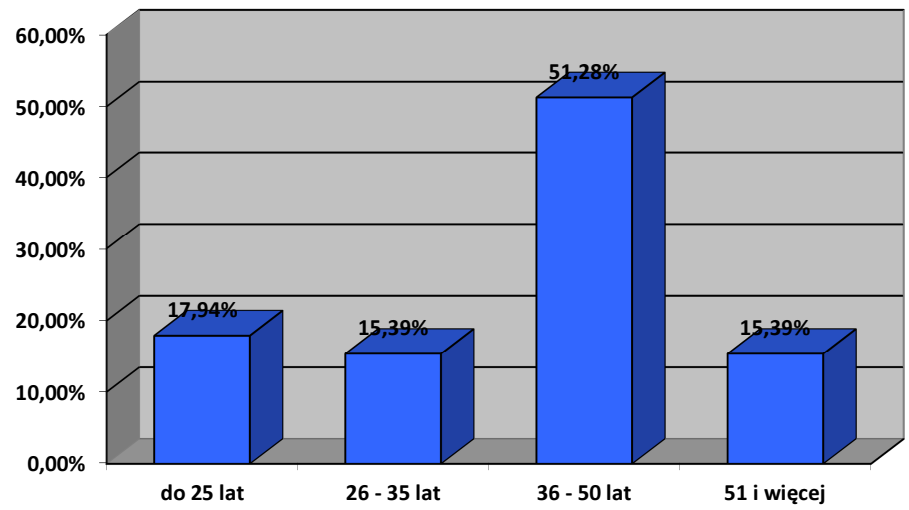
Badanie pokazało, że sprawcami przestępstw z ustawy o ochronie danych osobowych są w większości mężczyźni, którzy stanowią 61,5% ogółu sprawców, kobiety zaś pozostałe 38,5%. Dosyć wysoki udział kobiet jako oskarżonych o czyny naruszające przepisy ustawy może wynikać z charakteru występków w niej stypizowanych. Administrowanie danymi osobowymi lub dostęp do nich w równym stopniu mogą mieć mężczyźni, jak i kobiety. Do naruszenia przepisów ustawy nie są wymagane jakieś szczególne, dodatkowe, cechy po stronie sprawcy, które wskazywałyby na większą możliwość popełnienia tych przestępstw przez mężczyzn.

Rozpatrując osobę sprawcy oszustwa komputerowego pod kątem wieku stwierdzić należy, że najliczniejszą grupę oskarżonych o naruszenie przepisów ustawy stanowiły osoby w przedziale wiekowym 36 – 50 lat (ponad 51% wszystkich).

Równie dużą grupę stanowili sprawcy w wieku 26 – 35 lat oraz powyżej 51 lat (każda z tych kategorii po ponad 15%).

Osoby młode – do 25 roku życia – zostały oskarżone w niemal 18% spraw.

Wykres 9 - Wiek sprawców

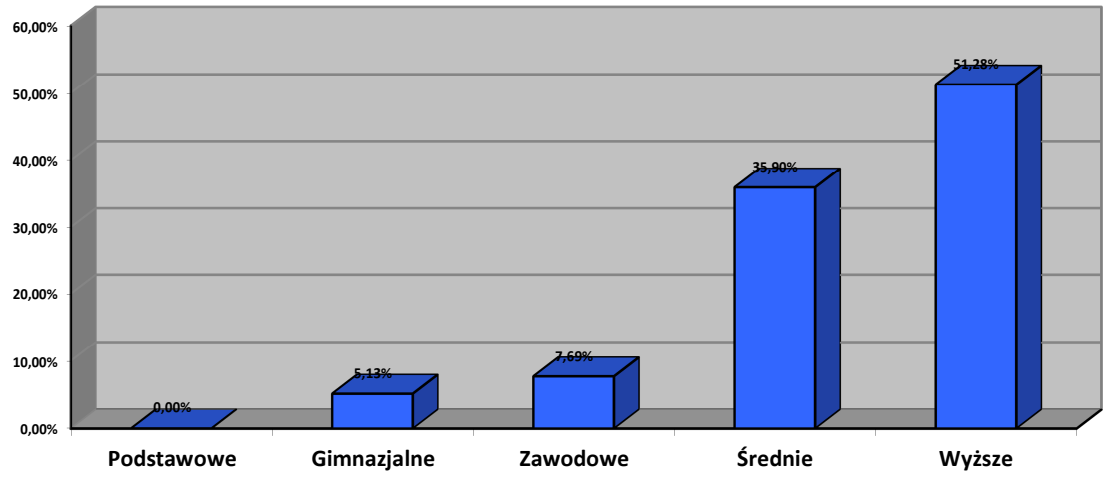


Sprawca występku z ustawy o ochronie danych osobowych jest raczej dobrze wykształcony. W ponad 51% posiada on wykształcenie wyższe, a w kolejnych niemal

36% średnie (co stanowi łącznie ponad 87% wszystkich sprawców). Wykształcenie zawodowe ma poniżej 8% ogółu sprawców, a gimnazjalne – niewiele ponad 5%.

Przyczyn, które powodują, iż sprawcami naruszeń przepisów w zakresie ochrony danych osobowych są głównie osoby z wyższym lub średnim wykształceniem można szukać również w charakterze czynów, jakie dokonują. Muszą to być bowiem osoby mające dostęp do zbiorów danych osobowych lub je nadzorujące. A zatem zajmować muszą one określony rodzaj stanowiska (np. prezes spółki będący z mocy ustawy administratorem danych) lub wykonywać pracę, przy której wymagane jest posiadanie określonego wykształcenia (pracownik instytucji finansowej odpowiedzialny za zawieranie umów z klientami).

Wykres 10 - Wykształcenie sprawców



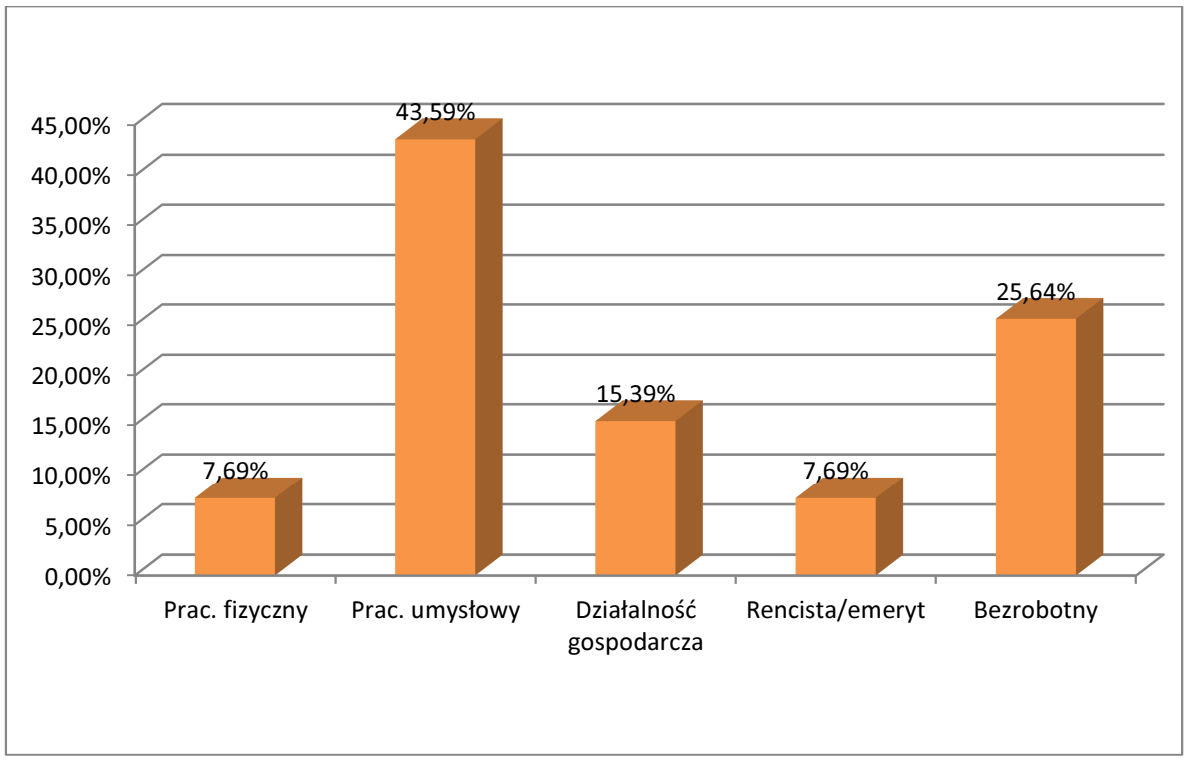
Powyższe tezy potwierdzają dane dotyczące rodzajów zatrudnienia osób podejrzanych o popełnienie przestępstw z ustawy o ochronie danych osobowych.

W ponad 43% przypadków wykonywali oni pracę o charakterze umysłowym, a w kolejnych ponad 15% prowadzili własną działalność gospodarczą.

Pracownicy fizyczni i osoby na emeryturze czy rencie stanowiły po ponad 7% sprawców.

Sprawcy bezrobotni w chwili postawienia im zarzutu popełnienia przestępstwa to grupa ponad 25%.

Wykres 11 – Sytuacja zawodowa sprawców



Jedynie sześciu oskarżonych (ponad 15%) było wcześniej karanych za przestępstwa określone w kodeksie karnym.

Wobec żadnego z oskarżonych nie zastosowano środka zabezpieczającego ani zapobiegawczego.

4. Podsumowanie

Ochrona danych osobowych, w szczególności danych osób fizycznych, jest zagadnieniem podejmowanym przez większość państw na całym świecie. Powstają w tym celu krajowe lub ponadnarodowe instytucje, których zadaniem jest nadzorowanie prawidłowego stosowania przepisów dotyczących przetwarzania danych tego typu. W zależności od przyjętego modelu, rozwiązania takie są bardziej lub mniej skuteczne.

Stosowany w Polsce model karnoprawnej ochrony danych osobowych, na podstawie przeprowadzonych badań, uznać należy za mało skuteczny. Podstawowym argumentem jest tutaj niewielka liczba spraw kierowanych do sądów z aktami oskarżenia – od kilku do niewiele ponad 20 rocznie – co przy skali potencjalnych naruszeń danych osobowych, nie można uznać za liczbę wystarczającą.

Sama struktura kar orzekanych w zaledwie kilkunastu przypadkach rocznie (głównie niskie grzywny) pokazuje, że przepisy karne nie są wystarczające dla zapewnienia właściwej ochrony danych osobowych.

Ponadto, kształt normatywny występków z art. 49 – 54a u.o.d.o. powoduje, że dla ustalenia odpowiedzialności sprawcy niezbędne jest wykazanie naruszenia innych przepisów ustawy (w szczególności dotyczących zakresu dozwolonego przetwarzania danych czy obowiązków informacyjnych) lub ustalenie roli osoby w związku z przetwarzaniem danych, tj. stwierdzenia czy była ona administrującym danymi czy też nie. W razie braku ustalenia takich przesłanek – niezbędne jest umorzenie prowadzonego postępowania lub wręcz odmowa jego wszczęcia.

Funkcjonująca w społeczeństwie świadomość ochrony danych osobowych, przy jednoczesnej nieznajomości, przyznać trzeba – skomplikowanych – przepisów ustawy powoduje, że w znacznej liczbie przypadków zawiadomienia o możliwości naruszenia danych osobowych są niezasadne, gdyż osoba zawiadamiająca dobrowolnie wyraziła zgodę na ich przetwarzanie. Między innymi również stąd wynikać może tak duża liczba umorzeń postępowań lub odmów ich wszczęcia.

Znacznie bardziej skutecznym dla ochrony danych osobowych byłby system oparty wyłącznie na prawie administracyjnym i organie wyspecjalizowanym w postaci Generalnego Inspektora Ochrony Danych Osobowych, który zostałby wyposażony w możliwość szerokiego nakładania kar w trybie administracyjnym, lub przynajmniej system mieszany, w którym GIODO mógłby, niezależnie od uprawnień w ramach prawa administracyjnego, w sprawach, w których uzna to za uzasadnione, kierować do prokuratury wnioski o ściganie.[53] Wydaje się, że ten drugi system w ramach polskiego systemu prawnego byłby łatwiejszy do wprowadzenia, gdyż – w przypadku, w którym to GIODO wyposażony został w możliwość represji w postaci nakładania kar – należałoby zagwarantować osobie „podejrzewanej" o naruszenie ustawy analogiczne uprawnienia i gwarancje, jakie przysługują oskarżonemu w postępowaniu karnym oraz zadbać o możliwość zaskarżania tych decyzji do sądu. Wówczas być może uniknęlibyśmy sytuacji, w której organa ścigania muszą prowadzić co najmniej postępowania sprawdzające w znacznej (kilkaset rocznie) liczbie przypadków, w tym w większości takich, w których do popełnienia czynu określonego w przepisach karnych ustawy nie doszło.

Ochrona danych osobowych w obecnych czasach jest koniecznością, dlatego istotne jest, by nie była ona iluzoryczna, lecz skuteczna, a sprawcy naruszeń szybko karani, i to niezależnie od tego, czy stanie się to na drodze administracyjnej, czy prawnokarnej.

[53] Pewne wzorce w budowaniu tego rodzaju rozwiązania już mamy odnośnie do prania pieniędzy, gdzie Generalny Inspektor Informacji Finansowej, posiada stosowne uprawnienia w celu przeciwdziałania tego typu zjawiskom.