Przegląd Prawno-Ekonomiczny

REVIEW OF LAW, BUSINESS & ECONOMICS

styczeń–luty–marzec

Nr 42
(1/2018)

WYDAWCA

Katolicki Uniwersytet Lubelski Jana Pawła II | Wydział Zamiejscowy Prawa i Nauk o Społeczeństwie w Stalowej Woli

ADRES REDAKCJI

Redakcja „Przeglądu Prawno-Ekonomicznego" | 37-450 Stalowa Wola, ul. Ofiar Katynia 6a | e-mail: ppe@kul.pl

DRUK I OPRAWA

VOLUMINA.PL DANIEL KRZANOWSKI | ul. Ks. Witolda 7-9, 71-063 Szczecin | tel. 91 812 09 08 | e-mail: druk@volumina.pl

ISSN 1898-2166 | Nakład 300 egz.

Spis treści

Artykuły

Glosa

Contents

Articles

Gloss

Adrian Romkowski

Przepisy karne ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. w kontekście standardów ochrony danych osobowych w rozporządzeniu GDPR (RODO) z dnia 27 kwietnia 2016 r.

Criminal infringements of the ustawa o ochronie danych osobowych 1997 in the perspective of personal data protection standards of the General Data Protection Regulation 2016

Wprowadzenie

Problematyka ochrony danych osobowych w demokratycznym państwie prawnym, jakim, zgodnie art. 2 Konstytucji z 1997 r.[1], jest Rzeczpospolita Polska, znalazła swe odzwierciedlenie zarówno w samej ustawie zasadniczej (art. 47 i art. 51), jak i w wielu aktach prawnych niższej rangi, z których zdecydowanie najistotniejszym jest ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[2]. Regulacje te, wraz z międzynarodowymi standardami w zakresie ochrony i rozporządzania danymi osobowymi, zdefiniowanymi m.in. w systemach prawnych Rady Europy (tj. w rezolucji nr 22 z 1973 r. o zasadach ochrony danych w sektorze prywatnym oraz rezolucji nr 29 z 1974 r. o zasadach ochrony danych w sektorze publicznym[3], Konwencji nr 108 o ochronie osób w związku

[1] Dz.U. z 1997, Nr 78 poz. 483, ze zm.

[2] Dz.U. z 1997, Nr 133 poz. 883, ze zm., cyt. dalej jako uodo.

[3] Szerzej o niniejszych rezolucjach i ich założeniach: M. Jagielski, *Prawo do ochrony danych osobowych. Standardy europejskie*, Warszawa 2010, s. 10-11.

z automatycznym przetwarzaniem danych osobowych z 1981 r.[4] i przede wszystkim w art. 8 Europejskiej Konwencji Praw Człowieka z 1950 r.), Unii Europejskiej (w szczególności w dyrektywie Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, a od 25 maja 2018 r. w mającym fundamentalne znaczenie rozporządzeniu Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE[5] (dalej: GDPR[6]), a także w Karcie Praw Podstawowych UE[7]), jak również ONZ (Rezolucja 45/95 Zgromadzenia Ogólnego ONZ z 1985 r.[8]) składają się na spójną, aczkolwiek nie w każdym aspekcie kompleksową[9], strukturę regulacji dotyczących ochrony danych osobowych w prawie polskim.

System ochrony danych osobowych, także w obszarze prawnokarnym, ulegnie jednak rozległej transformacji wraz z chwilą, od której zastosowanie mieć będzie wspomniane już rozporządzenie GDPR, co nastąpi 25 maja 2018 r. (zgodnie z art. 99 ust. 2 GDPR). Rozporządzenie to sprawi, iż ustawodawca stanie przed koniecznością uchwalenia całkowicie nowej ustawy o ochronie danych osobowych. Regulacja ta wprowadzi bowiem szereg nieznanych obecnie polskiemu porządkowi prawnemu instytucji, takich jak np. instytucję inspektora ochrony danych (art. 37 i n. GDPR), prawo do bycia „zapomnianym" (prawo do usunięcia danych - art. 17 GDPR) czy prawo do ochrony danych osobowych już w fazie

---

[4] Dz.U. z 2003, Nr 3, poz. 25.

[5] Dz.Urz. UE L 119 z 2016 r. Warto nadmienić, iż rozporządzenie to uchylało wymienioną w jego tytule dyrektywę (95/46/WE), której celem było przystosowanie aspektów ochrony danych osobowych do standardów „utworzenia i funkcjonowania rynku wewnętrznego" w związku z wprowadzaniem „wspólnego rynku" na mocy Traktatu z Maastricht z 1992 r. (tzw. „pierwszy filar" – Wspólnota Europejska). Egzemplifikacją konieczności wprowadzenia ponadnarodowych uregulowań w zakresie ochrony danych osobowych, zapewniających prawidłowe funkcjonowanie rynku wewnętrznego, była sytuacja, w której francuski inspektor danych osobowych, ze względu na brak uregulowań dot. danych osobowych we Włoszech, uniemożliwił przekazanie tychże danych z francuskiej do włoskiej filii Fiata, wymagając od oddziału włoskiego zawarcia z oddziałem francuskim umowy zobowiązującej do przestrzegania regulacji francuskich. Por. C. Kuner, *European data privacy law and online business*, Oksford-Nowy Jork 2003, s. 78-79.

[6] „GDPR" jest skrótem od angielskiej nazwy rozporządzenia - General Data Protection Regulation.

[7] Dz.Urz.UE C 202 z 2016 r. Mowa tu zwłaszcza o art. 7 i 8 Karty.

[8] Ogłoszona w dniu 14 grudnia 1990 r. Rezolucja ta zawierała jedynie niewiążące wytyczne dotyczące warunków koniecznych, jakie w ustawie powinno określić dane państwo w zakresie komputerowego (informatycznego, cyfrowego) przetwarzania danych osobowych.

[9] Teza ta, w zakresie płaszczyzny prawnokarnej ochrony danych osobowych, będzie przedmiotem dalszych rozważań.

projektowania rozwiązań związanych z ich przetwarzaniem (art. 25 GDPR), co w sposób fundamentalny wpłynie na obszar ochrony danych osobowych. Jakkolwiek jednak GDPR stosowane będzie bezpośrednio, nie zajmuje się ono problematyką regulacji karnych dotyczących ochrony danych osobowych, co ustawodawcy polskiemu da sporą dozę elastyczności w kształtowaniu odpowiedzialności w tym zakresie.

Abstrahując od przyjętych przez projektodawcę nowej uodo koncepcji, przedmiotem rozważań w niniejszym opracowaniu będzie analiza przepisów karnych (Rozdziału 8) aktualnie obowiązującej uodo, z uwzględnieniem rodzajów chronionych przez poszczególne typy czynów zabronionych dóbr prawnych, konstrukcji znamion typów, ich roli w kształtowaniu zupełności systemu ochrony danych osobowych (w postaci środków ochrony subsydiarnej) zarówno w perspektywie obecnie obowiązującej ustawy, jak i mającego znajdować zastosowanie od maja 2018 rozporządzenia GDPR, w celu udzielenia odpowiedzi na pytanie, czy wskutek powstałej (w wyniku wejścia rozporządzenia w życie) konieczności dostosowania regulacji polskich do prawa unijnego ustawodawca, w zakresie ochrony prawnokarnej, powinien decydować się na jakiekolwiek zmiany, a jeśli tak, to jaką zmiany te miałyby mieć postać, mając na uwadze zarówno perspektywę ewentualnego zawężania/rozszerzania tej sfery poprzez eliminację/dodawanie typów czynów zabronionych chroniących dane osobowe, jak również same zmiany wewnątrz istniejących typów, w szczególności w zakresie ewentualnej konieczności przeformułowania ich znamion.

Geneza prawnokarnej ochrony danych osobowych

Poprzedzając szczegółową analizę dotyczącą obowiązujących obecnie w prawie polskim regulacji penalnych w zakresie ochrony danych osobowych, należy pokrótce przedstawić proces wyodrębniania i kształtowania koncepcji prawnokarnej ochrony tychże danych.

Sama koncepcja ochrony danych osobowych jako takich, postrzegana przez pryzmat prymarnego dla jednostki prawa do prywatności, zrodziła się pod koniec lat pięćdziesiątych XX wieku w Stanach Zjednoczonych. Dyskusję dotyczącą prawa do prywatności jednostki w kontekście gromadzonych przez podmioty trzecie (zarówno publiczne, jak i prywatne) informacji na jej temat rozpoczął proces informatyzacji przechowywania i przetwarzania tych danych, co skutkowało koniecznością zapewnienia jednostce odpowiednich mechanizmów

ochrony przed płynącymi stąd zagrożeniami[10]. Liczne nadużycia, jakie miały miejsce w tamtym okresie, a w szczególności łatwość udostępniania przez organy państwowe zgromadzonych o obywatelach danych, skutkowały silną krytyką przedstawicieli doktryny dotyczącą braku odpowiednich mechanizmów ochronnych[11]. Odpowiedzią (choć trzeba zauważyć, że nieco spóźnioną) prawodawcy na te tendencje był uchwalony w 1974 r. przez Kongres Act of Privacy[12]. Ustawa ta wprowadzała mechanizmy ochrony przed naruszaniem ochrony danych osobowych na różnych płaszczyznach, w tym także i na płaszczyźnie prawnokarnej[13].

Na gruncie europejskim, aktem prawnym, który miał kapitalne znaczenie w rozwoju regulacji dotyczących ochrony danych osobowych była wspomniana już Europejska Konwencja Praw Człowieka z 1950 r., a szczególnie jej art. 8, definiujący prawo do prywatności. W ust. 2 wspomnianego artykułu, określającym granice ingerencji władzy publicznej w prywatność człowieka poprzez ustanowienie ściśle określonych przesłanek tej ingerencji (podstawa ustawowa, konieczność ingerencji z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne, dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności osób), w sposób bezpośredni zakreślono także spektrum przysługujących jednostce

---

[10] W sposób szczególnie wyraźny konieczność wprowadzenia regulacji chroniących dane osobowe, a także metodę ich uzyskiwania, ujawniła się w wyniku działań instytucji kredytujących i banków w Stanach Zjednoczonych w latach pięćdziesiątych i sześćdziesiątych. Instytucje te stosowały niejednokrotnie niemal „szpiegowskie" praktyki w celu samodzielnego gromadzenia informacji o klientach, uzyskując często informacje pochodzące z poufnych źródeł. Osoba, której te informacje dotyczyły, nie miała możliwości ani zapoznania się z ich treścią, ani dochodzenia zasadności ich gromadzenia, ani wreszcie kontroli właściwego i bezpiecznego przechowywania tych informacji – zob. A. Sakowicz, *Prawnokarne gwarancje prywatności*, Kraków 2006, s. 359.

[11] A. Westin, *Privacy and freedom*, Nowy York 1967, s. 125-128.

[12] Ułomność tej regulacji polegała jednak na tym, że jakkolwiek normowała ona gromadzenie, wykorzystywanie i ujawnianie wszystkich typów informacji osobistych, to czyniła to jedynie w odniesieniu do organów państwowych (w tym i organów ścigania), co tworzyło jednak swoistą lukę w zakresie instytucji prywatnych. Szerzej na temat założeń ustawy: F. Bignami, *The US legal system on data protectionin the field of law enforcement. Safeguards, rights and remedies for EU citizens*, Bruksela 2015, s. 5 i n.

[13] Ten akt prawny czynił to jednak w sposób niezwykle skąpy, gdyż wprowadzono zaledwie 3 typy czynów zabronionych w zakresie ochrony danych osobowych: 5 U.S.C. § 552a(i)(1) - (3), dotyczące kolejno: (1) posiadania lub uzyskiwania dostępu do dokumentów organów federalnych zawierających indywidualnie możliwe do zidentyfikowania informacje, których ujawnienie jest zabronione, (2) utrzymywania (administrowania) systemu ewidencji bez spełnienia wymagań dotyczących powiadomienia osoby, której dotyczą zbierane dane i (3) żądania lub uzyskiwania dokumentacji dotyczącej jednostki od organu federalnego pod fałszywym pozorem. Dwa pierwsze typy czynów zabronionych są typami indywidualnymi („*Any officer Or employee of anyagency*"), zaś jedynie trzeci typem powszechnym („*any person*"), co zakreśla stosunkowo wąskie spektrum kryminalizacji.

praw do ochrony dotyczących jej danych gromadzonych przez władze publiczne. W stosunku do podmiotów innych niż publiczne, uprawnienie jednostki do ochrony zgromadzonych przez te podmioty danych wywieść można z łącznej interpretacji art. 8 ust. 1 i 2 Konwencji, co, choć ogólnie, aczkolwiek szeroko, pozwala zakreślić ramy ochrony danych osobowych.

EKPCz, wraz z orzecznictwem Europejskiego Trybunału Praw Człowieka, a także przytaczanymi wyżej systemami prawnymi Unii Europejskiej oraz ONZ, stworzyły podwaliny pod regulacje i konstytucyjne, i ustawowe w bardzo wielu państwach europejskich.

Po transformacji ustrojowej z 1989 r., prawodawca polski stanął przed koniecznością dostosowania i pogodzenia ze sobą wolnorynkowych warunków obrotu gospodarczego oraz funkcjonowania organów administracji publicznej w demokratycznym państwie prawnym z prawem do prywatności jednostki, także w zakresie ochrony dotyczących jej, a zgromadzonych przez podmioty trzecie, informacji. Dając wyraz powadze i wysokiej randze zagadnieniu ochrony danych osobowych, problematykę ochrony tychże danych umieszczono we wspomnianych już art. 47 (*implicite*) i 51 (*explicite*) Konstytucji, a także w będącej realizacją upoważnienia z art. 51 ust. 5 Konstytucji uodo.

Ustawodawca, bazując na doświadczeniach państw-członków Rady Europy i Unii Europejskiej[14], uchwalając w 1997 r. uodo, zdecydował się na przyjęcie dwutorowej koncepcji ochrony danych osobowych: ochrony na płaszczyźnie administracyjnoprawnej i, jako *ultima ratio*, na płaszczyźnie prawnokarnej. Ochrona cywilnoprawna „przydzielona" została jednostce jedynie w formie klasycznej ochrony dób osobistych (art. 23 i 24 k.c.) oraz, w przypadku wystąpienia szkody majątkowej wynikającej z naruszenia danych osobowych, w postaci odpowiedzialności deliktowej (art. 415 i n. k.c.), bądź, w pewnych przypadkach, także odpowiedzialności kontraktowej (art. 471 i n. k.c.).

Typy czynów zabronionych z uodo

Przechodząc do właściwej części rozważań, analizie poddać należy przepisy art. 49 (bezprawne przetwarzanie danych osobowych), art. 51 (udostępnianie lub umożliwianie dostępu do danych osobowych osobom nieuprawnionym), art. 52 (naruszenie obowiązku zabezpieczenia danych), art. 53 (niezgłoszenie,

[14] J. Borecka, *Geneza prawnej ochrony danych osobowych i pojęcie danych osobowych*, Zeszyty Naukowe Instytutu Administracji Akademii im. Jana Długosza w Częstochowie, IV/2006, s. 9.

wbrew obowiązkowi, zbioru danych do rejestracji), art. 54 (niepoinformowanie, wbrew obowiązkowi, osoby, której dotyczą dane, o jej prawach) oraz art. 54a (utrudnianie lub udaremnianie inspektorowi wykonania czynności kontrolnej) uodo. Uwagą dotyczącą wszystkich typów przestępstw jest fakt, iż zgodnie z art. 116 k.k. stosuje się do nich przepisy części ogólnej tego kodeksu, bowiem uodo nie wyłącza wyraźnie ich zastosowania.

Typ czynu zabronionego z art. 49 ust. 1, czyli przestępstwo przetwarzania w zbiorze danych osobowych, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania podmiot sprawczy nie jest uprawniony, jest typem powszechnym z działania, o umyślnej stronie podmiotowej. Dobrem prawnym chronionym na gruncie tego przepisu jest prywatność jednostki, a także związana z nią poufność informacji jej dotyczących. Przestępstwo to jest typem formalnym (bezskutkowym).

Art. 49, zarówno w ust. 1, jak i ust. 2, jest klasycznym przepisem odsyłającym, co oznacza, że do rekonstrukcji znamion typów konieczne jest odwołanie się do innych przepisów ustawy[15]. Kolejno, przy wykładni normy z przepisu art. 49 ust. 1 uodo, konieczne będzie odtworzenie znaczenia znamion: „danych osobowych", „przetwarzania", „zbioru danych", „dopuszczalności" przetwarzania danych oraz „uprawnienia" do ich przetwarzania.

Ustawa definiuje pojęcie „danych osobowych" w art. 6 ust. 1 jako „wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej". Osobą fizyczną „możliwą do zidentyfikowania" jest, zgodnie z ust. 2 cytowanego artykułu, „osoba, której tożsamość można określić bezpośrednio lub pośrednio(…)". Pośrednim zidentyfikowaniem osoby może być przykładowo określenie jej specyficznych cech, zachowania czy innych informacji, jeżeli pozwalają one na zindywidualizowanie osoby (np. szczupła rudowłosa kobieta w zielonej sukience, która była wczoraj w sklepie w godzinach wieczornych). Szerokie ujęcie „danych osobowych" jako „informacji" dotyczących określonej osoby powoduje kolejną niejasność w określeniu znamienia typu, korygowaną jednak przez aprobowaną w doktrynie wykładnię pojęcia „informacji" jako „przenoszalnego dobra niematerialnego zmniejszającego niepewność"[16].

Definicja legalna znamienia czynności wykonawczej, „przetwarzania" danych, zawarta została w art. 7 pkt 2 uodo. „Przetwarzaniem" są „jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie,

[15] Zob. A. Drozd, *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy*, Warszawa 2004, s. 298.

[16] G. Szpor, Pojęcie *informacji a zakres danych osobowych*, (w:) P. Fajgielski (red.), Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia, Lublin 2008, s. 8.

przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych". Ustawodawca bardzo szeroko określił więc spektrum kryminalizacji, znamieniem czynności wykonawczej obejmując sytuacje związane zarówno z gromadzeniem, jak i wykorzystywaniem danych. Wyliczenie to jest wyliczeniem jedynie przykładowym, nieenumeratywnym, co oznacza, iż jakiekolwiek inne „przetwarzanie", niebędące żadną z czynności opisanych w art. 7 pkt. 2, będzie realizowało przesłankę znamienia czynnościowego z art. 49 ust. 1. „Przetwarzanie" odbywać się może zarówno w systemach informatycznych, jak i bez ich udziału, tak w sposób zautomatyzowany, jak i niezautomatyzowany[17]. „Systemem informatycznym" jest natomiast „zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych", jak stanowi art. 7 pkt 2a uodo.

Przedmiotem czynności wykonawczej typu z art. 49 ust. 1 jest „zbiór danych osobowych". I to pojęcie posiada swoją definicję legalną, bowiem zgodnie z art. 7 pkt 1 ustawy jest to „każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie"[18].

Znamię „niedopuszczalności" przetwarzania danych również jest znamieniem odsyłającym, tym razem do art. 23 ust. 1, w którym ustawodawca wyczerpująco wyliczył przesłanki dopuszczalności przetwarzania danych (osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych; jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa; 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; jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego; jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych,

[17] J. Barta, P. Fajgielski, R. Markiewicz, *Komentarz do art. 7* - teza 16, (w:) Ochrona danych osobowych. Komentarz, Warszawa 2015.

[18] Art. 4 pkt 2 rozporządzenia GDPR stanowi o „scentralizowaniu, zdecentralizowaniu czy rozproszeniu funkcjonalnym lub geograficznym" zbioru danych, co pomaga w wykładni pojęć „rozproszenia" i „podziału funkcjonalnego" zbioru danych z uodo. W związku z tym, „rozproszeniem" jest taka partycja zbioru danych, która polega na jego decentralizacji i/lub dekoncentracji geograficznej. „Podziałem funkcjonalnym" jest natomiast taki podział zbioru danych, który nie polegając na jego decentralizacji czy rozproszeniu geograficznym, ma na celu zwiększenie efektywności wykorzystywania danych zbioru (np. rozdzielenie zbioru danych na komórki organizacyjne w przedsiębiorstwie).

a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą), a także do art. 27 ust. 2 w zw. z ust. 1 uodo (przesłanki dopuszczalności przetwarzania tzw. danych sensytywnych (wrażliwych)[19], m.in. osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, chyba że chodzi o usunięcie dotyczących jej danych; dopuszczalność przetwarzania takich danych bez zgody osoby, której dane dotyczą, przewiduje przepis szczególny, który stwarza pełne gwarancje ochrony tychże danych; przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem; przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą; przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym, etc.). Jakkolwiek wyliczenie to jest wyliczeniem enumeratywnym, każda z tych przesłanek ma charakter samoistny i wystarczy spełnienie choćby jednej, by przetwarzanie danych było dopuszczalne[20].

Znamię „uprawnienia", a ściślej: niebycia uprawnionym do przetwarzania danych, wykładać należy zarówno jako brak stosownego uprawnienia, jak i działanie wbrew warunkom uprawnienia przysługującego sprawcy. Z „brakiem uprawnienia" będziemy mieć do czynienia w sytuacji nieposiadania przez sprawcę żadnego tytułu prawnego do przetwarzania (uprawnienia z umowy, ustawy, decyzji właściwego organu), natomiast z działaniem „wbrew warunkom uprawnienia" (z przekroczeniem przyznanych sprawcy kompetencji), do czynienia mieć będziemy w sytuacji, gdy sprawca, pomimo tego, że jest uprawniony do przetwarzania danych, czyni to niezgodnie z warunkami tego uprawnienia, przekraczając przyznane mu kompetencje[21].

Typ z art. 49 ust. 1 jest występkiem, zagrożonym karą grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2, ściganym z oskarżenia publicznego.

Art. 49 ust. 2 uodo jest typem kwalifikowanym w stosunku do ust. 1 przez znamię statyczne dotyczące przedmiotu czynu zabronionego. Okolicznością

---

[19] Tzw. danymi wrażliwymi są, stosownie do art. 27 ust. 1 uodo, dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

[20] J. Barta, P. Fajgielski, R. Markiewicz, *Komentarz do art. 23* - teza 1.

[21] Wydaje się, że znamię „niebycia uprawnionym" z art. 49 ust. 1 uodo zawiera w sobie przypadki „braku uprawnienia" i „działania wbrew warunkom uprawnienia", a znamiona takie zawarte zostały w art. 116 ustawy prawo autorskie i prawa pokrewne, zatem znamię to należałoby wykładać *per analogiam* do znamion ze wspomnianej ustawy. Por. J. Raglewski, *Komentarz do art. 116* – teza 8 i 9, (w:) D. Flisak (red.), Prawo autorskie i prawa pokrewne. Komentarz, Warszawa 2015.

modalną wpływającą na wyższą karalność jest rodzaj danych, których dotyczyłoby bezprawne przetwarzanie. Jeśli byłyby to dane ujawniające 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, karalność zaostrzona zostałaby do górnej granicy 3 lat pozbawienia wolności (zagrożenie karą grzywny i ograniczenia wolności pozostałoby takie, jak w ust. 1, zgodnie z art. 37a k.k. w zw. z art. 33 § 1 i art. 34 § 1 k.k.). Warto także zauważyć, iż te kategorie danych ustawodawca traktuje wyjątkowo, wprowadzając w art. 27 ust. 2 *lex specialis* w stosunku do dopuszczalności przetwarzania danych w art. 23 ust. 1. Kryteria te są bardziej restrykcyjne niż w art. 23 ust. 1 i opierają się głównie na zawężeniu i dookreśleniu przesłanek wymienionych w tym przepisie. Wyliczenie z art. 27 ust. 2 jest wyliczeniem enumeratywnym.

Kolejny z typów czynów zabronionych z uodo, określony w art. 51 ust. 1, dotyczy udostępniania lub umożliwiania dostępu osobom nieuprawnionym do zbioru danych przez administratora lub osobę obowiązaną do ochrony danych osobowych. Przestępstwo to jest typem indywidualnym właściwym (*delictum proprium*), bowiem ustawodawca zawęził krąg podmiotów sprawczych do osób administrujących zbiorem danych oraz do osób obowiązanych do ochrony danych osobowych. Przestępstwo to popełnić można tak z działania, jak i z zaniechania[22]. Typ ten jest typem o umyślnej stronie podmiotowej. Dobrem prawnym chronionym na gruncie tego przepisu jest, podobnie jak na gruncie art. 49, prywatność jednostki i poufność dotyczących jej informacji. Przestępstwo to jest przestępstwem formalnym, bowiem w wyniku „udostępnienia" lub „umożliwienia dostępu" nie musi dojść do zapoznania się z danymi przez osobę nieuprawnioną[23].

[22] Inaczej na ten temat wypowiedział się Sąd Najwyższy w postanowieniu z dnia 11 grudnia 2000 r., II KKN 438/00, uznając, iż tylko „umożliwianie dostępu" może mieć postać tak działania, jak i zaniechania, samo zaś „udostępnianie" uznając „z założenia za działanie sprawcy". Jest to pogląd oczywiście nietrafny, bowiem sama już wykładnia językowa pojęcia „udostępniania" (będzie o niej mowa podczas analizy tego znamienia w dalszej części opracowania), wraz z wykładnią funkcjonalną, jednoznacznie wskazują, iż udostępniać można także przez zaniechanie (przykład: dane osobowe ze zbioru X udostępniane są automatycznie określonym osobom. Administrujący zbiorem dostaje polecenie wprowadzenia zmian do listy osób, którym dane te są udostępniane, jednakże obowiązek ten zaniedbuje).

[23] Tak trafnie m.in. A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 166 oraz M. Organiściak, R. Zakrzewski, *Ochrona danych osobowych – przepisy karne*, Przegląd Ustawodawstwa Gospodarczego 2002, nr 8 s. 17. Na przeciwnym stanowisku stoją J. Barta., P. Fajgielski, R. Markiewicz, *Komentarz do art. 51* – teza 3, argumentując, iż „niezbędne jest (…) zapoznanie się z danymi osobowymi przez co najmniej jednego „nieupoważnionego odbiorcę". Abstrahując od rozważań na temat liczby odbiorców, pogląd ten należy uznać za całkowicie nietrafny,

Sprawcą czynu może być, jak wspomniano wyżej, jedynie osoba „administrująca zbiorem danych" lub „osoba obowiązana do ochrony danych osobowych". Wykładni pierwszego z tych znamion dokonał Sąd Najwyższy w tezie 2 postanowienia z dnia 11 grudnia 2000 r. II KKN 438/00[24], stwierdzając, iż „administrującym zbiorem danych" jest zarówno „administrator danych osobowych", zdefiniowany w art. 7 pkt 4 uodo, jak „także taki podmiot, który zarządza, zawiaduje zbiorem danych (art. 50, 51, 54) lub danymi (art. 52) w procesie ich przetwarzania, w tym i[25] powierzonego mu w trybie wskazanym w art. 31 tej ustawy (powierzenie przez administratora danych, w formie umowy pisemnej, przetwarzania danych innemu podmiotowi – dop. AR)". Odpowiedzialność karna w tym drugim przypadku, zdaniem SN, uzależniona jest od tego, czy bezprawność zachowania sprawcy „wynika z powierzonych mu czynności przetwarzania danych.". Pogląd ten uznać należy za trafny, bowiem bezzasadnym, w kontekście zawężenia kręgu podmiotów sprawczych, byłoby rozszerzanie odpowiedzialności osoby umocowanej do przetwarzania danych na gruncie art. 31 (lub na mocy innego niż umowny stosunku prawnego, np. administracyjnoprawnego) na przypadki, które zakresem tego umocowania objęte nie były.

Odnośnie do znamienia osoby „obowiązanej do ochrony danych osobowych", w literaturze przedstawiono dwa poglądy – węższy oraz szerszy. Wedle pierwszego z nich, desygnatem tego znamienia są „wszystkie osoby fizyczne przetwarzające dane osobowe na podstawie upoważnienia administratora danych osobowych (art. 37 uodo), względnie zawartej z nim umowy (art. 31 uodo), o ile zostały one zobowiązane do ochrony takich danych"[26]. Wedle drugiego, oprócz wskazanych powyżej osób, mogą być to także osoby wprawdzie niemające upoważnienia do przetwarzania danych, ale zobowiązane do ich ochrony na podstawie umowy, np. na podstawie stosunku pracy czy innej umowy cywilnoprawnej[27]. Oba poglądy są niepełne, a przez to nietrafne, jednak pogląd drugi należy uznać za bardziej trafny, wzbogacając go jednak o to, iż obowiązek ochrony danych osobowych w stosunku do osoby niemającej upoważnienia do ich przetwarzania wynikać może nie tylko z umowy (stosunku cywilnoprawnego), ale

w szczególności w kontekście wykładni językowej znamion „udostępniania" i „umożliwiania" dostępu, o czym będzie mowa w dalszej części opracowania.

[24] OSNKW 2001, nr 3-4, poz. 33.

[25] Oprócz podstawy ustawowej i umownej, jak zaznaczył SN, mogą istnieć także i inne podstawy uprawnień „administrującego" (na przykład administracyjnoprawna). Pokrywa się to z definicją „administrującego" rekonstruowaną na podstawie rozporządzenia GDPR, o czym będzie mowa w dalszej części opracowania.

[26] Por. J. Barta, P. Fajgielski, R. Markiewicz, *Komentarz do art. 51* – teza 2.

[27] Por. A. Drozd, *op. cit.*, s. 300.

także (czy może nawet przede wszystkim) ze stosunku administracyjnoprawnego (decyzji właściwego organu w stosunkach zewnętrznych, np. w przypadku outsourcingu zadań w zakresie ochrony danych, czy upoważnienia/polecenia służbowego w stosunkach wewnętrznych). Ponadto, samo już sformułowanie znamienia podmiotowego jako osoby „obowiązanej", a nie „zobowiązanej" do ochrony danych i wykładnia językowa tego znamienia (przymiotnik „obowiązany" wywodzi się etymologicznie od „obowiązku", natomiast „zobowiązany" od „zobowiązania" co miałoby jednoznacznie cywilistyczne konotacje) muszą prowadzić do jednoznacznej konstatacji, iż „obowiązek" może mieć charakter nie tylko cywilnoprawny.

Pierwsze znamię czynności wykonawczej typu dwuodmianowego, jakim jest art. 51 ust. 1, polega na „udostępnianiu" danych/zbioru danych osobom nieupoważnionym. Zgodnie z wykładnią językową, termin „udostępniać" oznacza „ułatwić kontakt z czymś lub umożliwić korzystanie z czegoś"[28]. „Ułatwianiem dostępu", czyli drugim członem alternatywy znamienia czynności wykonawczej, będzie natomiast takie zachowanie, które będzie w sposób znaczący upraszczało osobie nieuprawnionej zapoznanie się z danymi. W tym kontekście jednoznacznie widać, iż typ z art. 51 ust. 1 (a także i ust. 2) jest typem formalnym.

W literaturze wątpliwości wywołuje znamię „osób nieupoważnionych", bowiem sporne jest to, czy na gruncie takiego sformułowania przesłanki udostępnić/ułatwić dostęp do danych wystarczy tylko jednej osobie, czy osoby te muszą być co najmniej dwie. Nietrafnie wypowiedział się na ten temat Sąd Najwyższyw postanowieniu z dnia 21 listopada 2007 r., IV KK 376/07[29], konstatując, iż „Wobec obecnej treści przepisu art. 51 ust. 1 (…) udostępnienie danych lub umożliwienie do nich dostępu jednej osobie nie wyczerpuje znamion omawianego przestępstwa". Takie zawężenie pola kryminalizacji mogłoby prowadzić do nieuzasadnionego ograniczenia prawnokarnej ochrony danych osobowych, i to nawet mając na uwadze relację art. 51 ust. 1 uodo do art. 266 § 1 (względnie § 2 - stosunki zakresowe normowania tych przepisów pozostają w relacji krzyżowania), czyli możliwy kumulatywny zbieg tych przepisów[30]. W sytuacji bowiem, w której nie zachodziłby ten zbieg, a dane udostępniono by/ułatwiono by dostęp do nich tylko jednej osobie, zachowanie takie w ogóle nie byłoby karalne, co przeczyłoby *ratio legis* analizowanego przepisu. Należy więc stanąć

[28] Słownik języka polskiego PWN online: https://sjp.pwn.pl/.

[29] KZS 2008, nr 11, poz. 47, Legalis.

[30] W. Kulesza, *Ochrona danych osobowych a nowa kodyfikacja prawa karnego w Polsce*, (w:) M. Wyrzykowski (red.), Ochrona danych osobowych, Warszawa 1999, s. 89–97.

na stanowisku, iż wbrew wykładni językowej znamię „osób" nieupoważnionych oznacza także jedną osobę[31].

Samo zaś znamię „nieupoważnienia" rozumieć należy w sposób tożsamy ze znamieniem „uprawnienia" (ściślej: „nieuprawnienia") z art. 49 ust. 1[32], tj. zarówno jako brak upoważnienia (uprawnienia), jak i jako przekroczenie jego granic, interpretując je ponadto w świetle art. 23 (przesłanki dopuszczalności przetwarzania i uprawnione do tego podmioty), art. 27 (przesłanki dopuszczalności przetwarzania tzw. „danych wrażliwych") oraz art. 37 uodo (dopuszczenie do przetwarzania osób upoważnionych przez administratora).

Typ z art. 51 ust. 1 jest występkiem, zagrożonym karą grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2, ściganym z oskarżenia publicznego.

W art. 51 ust. 2 ustawodawca wprowadził typ zmodyfikowany uprzywilejowany w stosunku do ust. 1 poprzez znamię statyczne w postaci nieumyślnej strony podmiotowej (tak w postaci świadomej, jak i nieświadomej nieumyślności, zgodnie z art. 9 § 2 k.k.). Jeżeli sprawca działa nieumyślnie, zagrożenie karami zostało złagodzone do kary grzywny, ograniczenia wolności oraz pozbawienia wolności do roku.

Przestępstwo stypizowane w art. 52 uodo, kryminalizuje naruszenie przez administrującego danymi, choćby nieumyślnie, obowiązku zabezpieczenia danych przed ich zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem. Przestępstwo to, podobnie jak w art. 51, jest typem indywidualnym właściwym, gdyż odpowiedzialność karną ponieść może tylko podmiot administrujący danymi[33]. Dobrami prawnymi chronionymi na gruncie tego

---

[31] Tak też A. Herzog, *Glosa do postanowienia SN z dnia 21 listopada 2007 r. IV KK 376/07*, Prokuratura i Prawo 2008, nr 11, s. 165.

[32] Por. uwagi do art. 49 ust. 1. Różnicą pomiędzy „upoważnieniem" a „uprawnieniem" na gruncie uodo jest rodzaj stosunku prawnego umożliwiającego dostęp do danych (ustawa o „upoważnieniu" stanowi np. w kontekście „upoważnienia" pracowników Biura GIODO do różnych czynności – parz art. 14).

[33] Odnośnie osoby „administrującej danymi" por. uwagi do art. 51 ust. 1 i znamienia osoby „administrującej zbiorem danych". Rozróżnienie pomiędzy „danymi" a „zbiorem danych" jest jednak istotne i wprowadzone przez ustawodawcę celowo. Chodzi o rozszerzenie prawnokarnej ochrony, bowiem administrować można także danymi osobowymi (w rozumieniu art. 6 ust. 1) nietworzącymi zbioru danych (w rozumieniu art. 7 pkt 1). Warto się jednak zastanowić, dlaczego w art. 51 ust. 1 ustawodawca posłużył się konstrukcją znamienia podmiotowego jako „administrującego zbiorem danych" oraz osoby „obowiązanej do ochrony danych osobowych", zaś w art. 52 – „administrującego danymi". Rozróżnienie to nie zostało przez ustawodawcę przemyślane, bowiem, jakkolwiek w przypadku art. 51, mówić możemy o właściwie pełnym unormowaniu podmiotowej płaszczyzny kryminalizacji (bo nawet, jeśli ktoś administrowałby jedynie danymi, a nie ich zbiorem, to i tak byłby osobą „obowiązaną do ochrony danych osobowych" – jeśli podstawą byłaby umowa, to *directe* art. 31 ust. 3, jeśli inny stosunek prawny – *per analogiam* art. 31 ust. 3), natomiast ograniczenie w art. 52 kręgu podmiotów sprawczych do „administrujących danymi",

przepisu są, podobnie jak w przypadku art. 49 i 51 uodo, prawo do prywatności i prawo do ochrony danych osobowych. Typ ten jest typem formalnym, wszakże ustawodawca penalizuje jedynie abstrakcyjne narażenie na niebezpieczeństwo dobra w postaci prawa do prywatności i prawa do poufności danych osobowych, zaś do pełnej realizacji znamion nie jest konieczne wystąpienie skutku w postaci zabrania, uszkodzenia czy zniszczenia danych. Realizacja znamion nastąpić może zarówno w wyniku działania, jak i zaniechania sprawcy. Ponadto, typ z art. 52 charakteryzuje się mieszaną, umyślno-nieumyślną stroną podmiotową, bowiem ustawodawca wprowadził klauzulę nieumyślności już w typie zasadniczym.

Czynność sprawcza określona została w tym przepisie jako „naruszenie obowiązku zabezpieczenia (danych) przed (ich) zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem". W tym miejscu ponownie mamy do czynienia z konstrukcją znamion, których zdekodowanie częściowo oparte jest o odesłanie do innego z przepisów ustawy, a konkretniej do art. 36 ust. 1 uodo. Przepis ten statuuje obowiązek administratora danych do stosowania „środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń (kryterium proporcjonalności – dop. AR) oraz kategorii danych objętych ochroną (kryterium celowości – dop. AR), a w szczególności (administrator) powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem"[34]. Obowiązki te, zgodnie z wcześniejszymi ustaleniami w zakresie znamienia „administrującego" danymi/zbiorem danych, dotyczą nie tylko administratora, ale także m.in. osoby, której, zgodnie z art. 31 ust. 1, administrator, w drodze umowy pisemnej, powierzył przetwarzanie danych (art. 31 ust. 3 samoistnie nakłada na taką osobę obowiązek stosowania się do wymagań z art. 36 – 39), a także każdej innej niż wyżej wskazane osoby, której administrowanie powierzone zostało w drodze innej niż umowa (*argumentum per analogiam* z art. 31 ust. 3 uodo).

Art. 52 stanowi o „obowiązku" zabezpieczenia danych przed zabraniem przez osobę nieuprawnioną[35], uszkodzeniem lub zniszczeniem. Obowiązek ten

poza sferą normowania niesłusznie pozostawia istotne, z punktu widzenia *ratio legis* regulacji, podmioty nieadministrujące danymi, ale obowiązane do ich ochrony. Kwantum naganności zachowań tych podmiotów może być bowiem takie samo, jak w przypadku „administrujących danymi". Konstrukcja znamienia podmiotowego w art. 52 powinna być więc tożsama z tą z art. 51 ust. 1 uodo.

[34] W art. 36a – 39 uodo ustawodawca wprowadził techniczne regulacje dotyczące zadań i obowiązków administratora w zakresie ochrony przetwarzanych danych osobowych.

[35] Odnośnie do znamienia „osoby nieuprawnionej" por. uwagi do art. 49 i 51.

będzie miał przede wszystkim charakter ustawowy (wspomniane art. 36 i 31 uodo), może jednak, w stosunku do podmiotów innych niż wymienione w przytoczonych artykułach, mieć podstawę umowną bądź administracyjnoprawną.

Przestępstwo z art. 52 jest występkiem, zagrożonym karą grzywny, karą ograniczenia wolności albo pozbawienia wolności do roku, ściganym z oskarżenia publicznego.

Konsekutywnym typem czynu zabronionego, zdefiniowanym w art. 53 uodo, jest przestępstwo naruszenia obowiązku zgłoszenia do rejestracji zbioru danych. Przestępstwo to, podobnie jak przestępstwa określone w przepisach je poprzedzających (art. 51 i 52) jest typem indywidualnym właściwym (odpowiedzialność ponieść może jedynie podmiot, na którym ciąży obowiązek zgłoszenia zbioru do rejestracji), którego znamiona zrealizowane zostać mogą jedynie przez zaniechanie, o umyślnej stronie podmiotowej. Dobrem prawnym podlegającym ochronie na mocy tego przepisu jest możliwość sprawowania kontroli nad właściwym gromadzeniem, przetwarzaniem i udostępnianiem danych przez organ do tego powołany[36]. Typ ten, podobnie jak jego poprzednicy, jest typem formalnym.

Art. 53, w kontekście znamienia podmiotu sprawczego, stanowi o „obowiązku zgłoszenia do rejestracji zbioru danych". Tak skonstruowane znamię typu ponownie oparte jest o odesłanie do innych przepisów ustawy (art. 40 – 46f), choć warto, w świetle ustaleń w zakresie znamion podmiotowych art. 51-52, zaznaczyć, iż znamię „obowiązku" dotyczyć będzie nie tylko „administratora danych", jak stanowi art. 40, ale także i „administrującego" danymi, jak również podmiotu niebędącego ani administratorem, ani administrującym, który na podstawie stosunku cywilnoprawnego/administracyjnoprawnego również byłby obowiązany do dokonania zgłoszenia[37].

Znamię czasownikowe „niezgłoszenia (zbioru) do rejestracji" powoduje trojaką wątpliwość w zakresie jego prawidłowej rekonstrukcji. Niejasne jest to, czy penalizacji podlegają, po pierwsze, zgłoszenie niepełne (niespełniające wszystkich ustawowych wymogów), po drugie, zawarcie w zgłoszeniu informacji

[36] Zgodnie z art. 8 ust. 1 uodo, obecnie organem tym jest Generalny Inspektor Danych Osobowych. W nowym stanie prawnym, od wejścia w życie projektowanej uodo, instytucja ta zastąpiona zostanie instytucją Prezesa Urzędu Ochrony Danych Osobowych. *Ratio legis* tej zmiany przedstawione zostanie w dalszej części opracowania.

[37] Tak trafnie A. Drozd, *op. cit.*, s. 302. Odmienne stanowisko prezentują w tej kwestii J. Barta., P. Fajgielski, R. Markiewicz, *Komentarz do art. 53* – teza 2, ograniczając krąg podmiotów sprawczych do „administrujących danymi". Autorzy ci argumentują, że ustawodawca nie posłużył się określeniem „administrującego zbiorem danych" analogicznie jak w art. 51 wyłącznie dlatego, by uniknąć nieścisłości, ponieważ do czasu rejestracji zbioru osoba taka nie byłaby jeszcze formalnie „administrującym". Nie uzasadniają jednak tego, dlaczego ograniczają zbiór desygnatów znamienia podmiotowego tylko do wskazanych denotacji.

nieprawdziwych, a po trzecie, niezgłoszenie zmian w zbiorze już istniejącym (obligatoryjne na mocy art. 41 ust. 2 uodo). Na wszystkie te pytania odpowiedzieć trzeba przecząco. Należy jednakże zaznaczyć, iż brak możliwości pociągnięcia do odpowiedzialności karnej na gruncie art. 53 jest możliwy jedynie w przypadku, gdy: w sytuacji nr 1 zgłoszenie niepełne bądź podanie w nim dane fałszywe nie uniemożliwiałyby sprawowania kontroli przez GIODO[38], zaś w sytuacjach 2 i 3 - wtedy, gdy zmiany te miałyby charakter niezasadniczy, niezmieniający charakteru i istoty całego zbioru.

Typ czynu zabronionego z art. 53 uodo jest występkiem, zagrożonym karą grzywny, karą ograniczenia wolności albo pozbawienia wolności do roku, ściganym z oskarżenia publicznego.

W tym miejscu, burząc nieco szyk zaproponowany przez ustawodawcę (w celu logicznej systematyzacji wywodu, bowiem przepisy art. 53 i 54a mają wspólny „rdzeń" w postaci chronionego dobra prawnego, tj. szeroko pojętych uprawnień kontrolnych GIODO), analizie poddane zostanie przestępstwo określone w art. 54a ustawy, tj. udaremnienie lub utrudnienie inspektorowi wykonania czynności kontrolnej. Przestępstwo to jest typem powszechnym, zarówno z działania, jak i z zaniechania, o umyślnej stronie podmiotowej. Dobrem prawnym chronionym przez tenże typ jest prawidłowość przeprowadzania czynności kontrolnych przez GIODO, a pośrednio także zgodność ustaleń kontrolnych ze stanem rzeczywistym. Przestępstwo to ma charakter materialny (skutkowy) – znamieniem skutku jest bowiem wywołanie obiektywnego stanu udaremnienia lub utrudnienia możliwości przeprowadzenia czynności kontrolnych[39].

Czynności wykonawcze znamienne w tym typie to „udaremnienie" i „utrudnienie" wykonania czynności kontrolnej. Zgodnie z przyjętą na gruncie art. 225 § 1 k.k. wykładnią tych znamion, „udaremnieniem" jest stworzenie (lub dopuszczenie do powstania) trudności/przeszkody uniemożliwiającej przeprowadzenie określonej czynności kontrolnej[40]. „Utrudnieniem"[41] jest spowodowana

[38] Tak też J. Barta, P. Fajgielski, R. Markiewicz, *Komentarz do art. 53* – teza 3 oraz M. Bieniak, *Odpowiedzialność karna menedżerów*, Warszawa 2015, s. 291.

[39] Por. J. Giezek, *Komentarz do art. 225* – teza 6, (w:) J. Giezek (red.), *Kodeks karny. Część szczególna. Komentarz*, Warszawa 2014. Na marginesie należy dodać, iż konstrukcja znamion czynności wykonawczych w art. 54a uodo jest tożsama z tą z art. 225 § 1 kk, a mając na uwadze *ratio legis* obu przepisów, również wykładnia tych znamion powinna być jednakowa.

[40] A. Barczak-Oplustil, *Komentarz do art. 225* – teza 9, (w:) A. Zoll (red.), *Kodeks karny. Część szczególna. Tom II. Komentarz do art. 117-277 k.k.*, Warszawa 2013.

[41] Niektórzy autorzy znamię „utrudnia" interpretują dwutorowo: jako „utrudnienie" i „utrudnianie". Podział ten nie wydaje się celowy, bowiem i „utrudnienie", i „utrudnianie" doprowadzić mają do tego samego rezultatu, tj. nieefektywności działań kontrolnych. Rozróżnienie to, oparte na założeniu, iż „utrudnieniem" jest „jakakolwiek forma zakłócenia przebiegu czynności kontrolnej,

działaniem sprawcy (lub będąca wynikiem jego bierności) sytuacja, w której przeprowadzenie kontroli przez inspektora jest znacznie mniej efektywne i wymaga niewspółmiernego do oczekiwanego rezultatu wysiłku[42].

Udaremnienie/utrudnienie dotyczyć musi „czynności kontrolnej". Art. 12 pkt 1 uodo statuuje kompetencję GIODO do „kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych", natomiast art. 14 – uprawnienia kontrolne Generalnego Inspektora, zastępcy Generalnego Inspektora lub upoważnionych przez niego pracowników Biura. Samo zaś pojęcie kontroli wykładać należy tak, jak czyni to nauka prawa administracyjnego, tj. jako „badanie, czy działania podmiotu kontrolowanego są zgodne ze stanem powinnym, wymaganym przez prawo, i formułowanie wniosków w przypadku odstępstw od tego stanu"[43].

Występek z art. 54a uodo jest zagrożony karą grzywny, karą ograniczenia wolności albo pozbawienia wolności do roku, ścigany w trybie publicznoskargowym.

Ostatni z analizowanych typów czynów zabronionych z uodo, art. 54, dotyczy niedopełnienia przez administrującego zbiorem danych obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w uodo. Przestępstwo to jest typem indywidualnym właściwym (odpowiedzialność ponieść może wyłącznie administrujący zbiorem danych[44]), umyślnym, z zaniechania. Dobrem prawnym chronionym przez ten typ jest prawo do kontrolowania przez jednostkę przetwarzania dotyczących jej danych. Przestępstwo to jest typem formalnym.

---

w wyniku której jej cel nie może być osiągnięty", prowadziłoby do utożsamienia znamion „utrudnia" i „udaremnia" w tym zakresie („udaremnianie" oznacza przecież sytuację niemożliwości przeprowadzenia czynności kontrolnej, co rozumieć należy jako niemożność osiągnięcia celu kontroli, a nie jako bezwzględną niemożność podjęcia jakichkolwiek czynności w trakcie kontroli). Por. A. Błachnio-Parzych, Prawnokarna ochrona inspektora ochrony danych osobowych – przestępstwo udaremnienia lub utrudnienia kontroli przestrzegania przepisów o ochronie danych osobowych, Dodatek Specjalny do Monitora Prawniczego 2011, nr 3, s. 37.

[42] A. Barczak-Oplustil, *op. cit.* - teza 8.

[43] T. Woś, *Postępowanie administracyjne*, Warszawa 2015, s. 56.

[44] Odnośnie do znamienia „administrującego zbiorem danych", por. uwagi do art. 51 ust. 1 i 52 uodo. Odmienne stanowisko w kwestii kręgu desygnatów znamienia podmiotowego prezentują B. Kurzępa, *Przestępstwa z ustawy o ochronie danych osobowych*, „Prokuratura i Prawo" 1999, nr 6, s. 53-55 oraz P. Barta, P. Litwiński, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2016, s. 551-552, nietrafnie wskazując, iż pomimo tego, że w art. 54 mowa o „administrującym zbiorem", ustawa obowiązki informacyjne przypisuje jedynie administratorowi, zatem w tym wypadku jako „administrującego" rozumieć należy wyłącznie „administratora". Stanowisko to, zwłaszcza w kontekście poprzedzających typ z art. 54 typów czynów zabronionych, bazuje na wykładni *contra legem*.

Ustawodawca wprowadził definicję legalną pojęcia (znamienia) „obowiązku" informacyjnego. Zakres tego obowiązku zdefiniowany został w art. 24 i 25 ustawy (obowiązek informowania osoby, której dotyczą zbierane dane, o przysługujących jej prawach „z urzędu", zarówno w przypadku, gdy dane te są zbierane od niej – art. 24, jak i w przypadku, gdy dane nie są zbierane od niej – art. 25), a także w art. 32 i 33 (uprawnienie jednostki do kontroli przetwarzania dotyczących jej danych – art. 32, uprawnienie jednostki do złożenia wniosku o poinformowanie o przysługujących jej prawach oraz o otrzymanie informacji, o których mowa w art. 32 ust. 1 pkt 1-5a – art. 33). „Obowiązek" może więc mieć charakter wyłącznie ustawowy[45] – jest tak nawet w przypadku, gdy ciąży on na „administrującym" niebędącym administratorem. W takim wypadku nie wynika to *expressis verbis* z ustawy, lecz można wyinterpretować to *per analogiam* z art. 31 ust. 3 uodo (tj. z ciążących na podmiocie administrującym obowiązków w zakresie zabezpieczania zbioru danych i towarzyszących temu wymogów technicznych). Należy ponadto zgodzić się ze stanowiskiem, że naruszenie „obowiązku" (a przez to realizacja znamion typu) nastąpi także w przypadku udzielenia informacji niekompletnej, jak również w przypadku udzielenia jej po terminie wynikającym z art. 33 ust. 1 ustawy (30 dni od dnia otrzymania wniosku)[46].

Art. 54 wprowadza dla występku określonego w tym przepisie zagrożenie karą grzywny, karą ograniczenia wolności albo pozbawienia wolności do roku. Przestępstwo to ścigane jest z oskarżenia publicznego.

Przepisy karne uodo a rozporządzenie GDPR

Po poddaniu analizie typologiczno-normatywnej przestępstw określonych w rozdziale 8 uodo, należy odnieść te regulacje do standardów wyznaczanych przez kluczowe w tej kwestii rozporządzenie GDPR, badając przepisy karne ustawy przede wszystkim pod kątem ich roli w kształtowaniu zupełności systemu ochrony danych osobowych (tj. tego, czy prawnokarna ochrona danych osobowych, ukonstytuowana przez ustawodawcę w sposób taki, jak ma to miejsce w obecnej uodo, byłaby w świetle rozporządzenia ochroną pełną

[45] Mowa tu oczywiście o prawnokarnie relewantnym „obowiązku", stanowiącym znamię typu czynu zabronionego. Obowiązek informowania może być szerszy i wynikać np. z umowy między klientem powierzającym dane a administratorem zbioru tychże danych, ale w zakresie takim, w jakim przekracza on regulacje ustawowe, nie będzie on należał do zakresu normowania regulacji z art. 54 uodo.

[46] J. Barta, P. Fajgielski, R. Markiewicz, *Komentarz do art. 54* - teza 3.

i wystarczającą). Obszar ten eksplorowany będzie zarówno w pryzmacie samej konstrukcji znamion poszczególnych typów, jak i ewentualnych luk prawnych w sferze przepisów karnych obecnej uodo w świetle tak samego rozporządzenia GDPR, jak i całego systemu ochrony danych osobowych. Analiza ta zostanie oparta o hipotetyczne założenie współobowiązywania przepisów karnych uodo (w formie takiej, w jakiej ma to miejsce obecnie) i rozporządzenia GDPR. Założenie to jest niezbędne do udzielenia odpowiedzi na pytanie, czy przepisy karne uodo w obecnym kształcie mogłyby, od chwili wejścia rozporządzenia w życie, faktycznie współtworzyć system ochrony danych osobowych wraz z GDPR.

Wywód rozpocząć należy od stwierdzenia, iż samo rozporządzenie, w pkt. 149 preambuły, stwarza państwom członkowskim UE możliwość „ustanawiania przepisów przewidujących sankcje karne za naruszenie niniejszego rozporządzenia, w tym za naruszenie krajowych przepisów przyjętych na jego mocy i w jego granicach. Sankcje karne mogą również obejmować pozbawienie zysków wynikających z naruszenia niniejszego rozporządzenia". Oznacza to, że przepisy karne w państwach członkowskich UE mogą, po pierwsze, przewidywać sankcje za naruszenie przepisów samego rozporządzenia, a po drugie, kryminalizować naruszenie danych osobowych nawet w stopniu szerszym, niż ochrona wynikająca z samego GDPR.

Art. 49 uodo (przestępstwo przetwarzania danych, gdy nie jest to dopuszczalne oraz przetwarzania ich przez osobę nieuprawnioną) jako przepis odsyłający przy rekonstrukcji znamion do innych przepisów uodo, odwoływać „mógłby" się przez to także do ich odpowiedników wśród przepisów rozporządzenia – art. 4 pkt 1, 2, 5 (definicje „danych osobowych", „przetwarzania", „zbioru danych"), art. 5 (zasady przetwarzania danych), art. 6 (przesłanki zgodności przetwarzania z prawem), art. 9 ust. 2 i art. 10 (przesłanki dopuszczalności przetwarzania „danych wrażliwych"). Regulacje te są, pomimo pewnych różnic w sformułowaniach i nieco kazuistycznej formy rozporządzenia, niemalże tożsame z unormowaniami ustawowymi. W tej kwestii rozporządzenie GDPR nie zmieniłoby zatem nic – jedynie, ze względu na jego bezpośrednią skuteczność, to do niego sięgać musielibyśmy podczas rekonstrukcji znamion typów.

Istotne znaczenie w kontekście realizacji znamion typów z art. 49 ma jednak art. 6 ust. 4 GDPR, interpretowany w świetle jednej z przesłanek dopuszczalności (legalności) przetwarzania danych, zdefiniowanej w art. 23 ust. 2 uodo (tj. zgody na przetwarzanie danych osobowych w przyszłości, jeśli nie zmieni się cel przetwarzania). Art. 6 ust. 4 GDPR zezwala bowiem, przy spełnieniu ściśle określonych przesłanek, na przetwarzanie danych osobowych w celu innym niż ten, w którym zostały zebrane, bez zgody osoby, której te dane dotyczą,

natomiast art. 23 ust. 2 uodo w przypadku, gdy przetwarzanie danych odbywa się na podstawie zgody osoby, bez uzyskania ponownej zgody na przetwarzanie w przypadku zmiany jego celu, taką możliwość jednoznacznie wyklucza[47]. Regulacje te w tym zakresie pozostają ze sobą w wyraźnej sprzeczności, a *de lege lata* należy skonstatować, iż znacznie pełniejszą i klarowniejszą ochronę prawnokarną w odniesieniu do „bezprawności" przetwarzania daje rekonstrukcja znamion na bazie art. 23 ust. 2 uodo. Niestety, od momentu rozpoczęcia obowiązywania przez GDPR, art. 23 uodo całkowicie straci rację bytu, co więcej – zostanie on także abrogowany z systemu prawa wraz z wejściem w życie nowej uodo. W związku z tym podstawą odesłania przy rekonstrukcji znamion typów z art. 49 będzie jedynie art. 6 ust. 4 GDPR, co istotnie ograniczy zakres prawnokarnej ochrony na gruncie art. 49 uodo.

Warto wspomnieć także o rozbieżności pomiędzy art. 6 ust. 1 lit. c GDPR a art. 23 ust. 1 pkt 2 uodo[48]. Rozporządzenie stanowi o tym, iż przetwarzanie „jest zgodne z prawem (…) gdy jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze", natomiast art. 23 ust 1 pkt 2 uodo – o jego dopuszczalności „tylko wtedy, gdy (…) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa". Podobne wątpliwości pojawiły się już w kontekście art. 7 lit. c dyrektywy 95/46/WE[49],

[47] Na gruncie rozporządzenia sytuacja, w której osoba wyraziła zgodę na przetwarzanie danych w przyszłości, lecz następczo zmienił się cel przetwarzania, byłaby całkowicie legalna, jeżeli spełnione zostałyby przesłanki z art. 6 ust. 4 (uszczegóławiające przesłankę zgodności „innego (nowego – dop. A.R.) celu z celem, w którym dane zostały pierwotnie zebrane"). Zgodnie jednak z art. 23 ust. 2 uodo, sytuacja taka byłaby wykluczona i konieczna byłaby ponowna zgoda na przetwarzanie, bowiem jakakolwiek zmiana celu przetwarzania, bez uzyskania zgody, czyniłaby to przetwarzanie bezprawnym. Ta subtelność ma fundamentalne znaczenie dla określenia podstaw odpowiedzialności, gdyż podmiotem uprawnionym do ustalania, czy cel „nowy" jest zgodny, czy niezgodny z celem pierwotnym, jest, zgodnie z GDPR, administrator danych. Przyjęcie perspektywy z rozporządzenia, a nie z ustawy, może prowadzić do poważnych nadużyć w przetwarzaniu danych, a nadto uniemożliwiać pociągnięcie administratora do odpowiedzialności, wszak niepodobna przypisać odpowiedzialność karną podmiotowi, który działa w majestacie prawa. Sytuacji „nie poprawia" także obowiązek informowania o zmianie celu przetwarzania, określony w art. 13 ust. 3 GDPR, ani możliwość wycofania zgody na przetwarzanie, określona w art. 7 ust. 3. Zgodnie bowiem z art. 61 § 1 k.c., który jednoznacznie wskazuje na tzw. teorię doręczenia jako na moment skutecznego złożenia oświadczenia woli, od momentu poinformowania do momentu dojścia do administrującego oświadczenia woli o wycofaniu zgody (np. w postaci listu) przetwarzanie byłoby w pełni legalne, nawet jeśli odbywałoby się wbrew woli podmiotu, który przecież zgodę wycofał.

[48] Por. G. Sibiga, *Dostosowywanie prawa polskiego do ogólnego rozporządzenia o ochronie danych*, Warszawa 2016, s. 16.

[49] W wyniku zaleceń Komisji Europejskiej, art. 23 ust. 1 pkt 2 uodo został znowelizowany z dniem 22 stycznia 2004 r. i zyskał obowiązujące obecnie brzmienie. Brzmienie to nie urzeczywistniało jednak do końca zaleceń Komisji. Szerzej na ten temat: J. Barta, P. Fajgielski, R. Markiewicz, *Komentarz do art. 23* - teza 14.

jednak wówczas nie miały one aż takiej doniosłości z uwagi na charakter prawny aktu unijnego (dyrektywa wiąże co do celu, rozporządzenie jest bezpośrednio skuteczne – art. 288 TFUE). Obecnie należy uznać, iż rozbieżności wykładnicze pomiędzy rozporządzeniem GDPR a obecnie obowiązującą uodo doprowadziłyby, od momentu rozpoczęcia obowiązywania przez GDPR, do rozszerzenia zakresu kryminalizacji typów z art. 49 uodo, bowiem na gruncie aktu unijnego przesłanka dopuszczalności przetwarzania została określona znacznie węziej, niż ma to miejsce w uodo (dotyczy jedynie obowiązku prawnego, a nie także zrealizowania uprawnienia, a nadto obowiązku ciążącego jedynie na administratorze, a nie na kimkolwiek innym).

W przypadku kolejnych typów czynów zabronionych, zdefiniowanych w art. 51 uodo (udostępnienie lub umożliwienie dostępu do zbioru danych osobom nieupoważnionym), rozporządzenie GDPR nie daje, w przeciwieństwie do sytuacji z art. 49 ustawy, jednoznacznych podstaw mogących wpływać znacząco na różnice interpretacyjne pomiędzy wykładnią typów opartą o inne przepisy ustawy a wykładnią opartą o GDPR. Warte uwagi są naturalnie definicje legalne z rozporządzenia (w szczególności art. 4 pkt 7 i 8, definiujące „administratora" i „podmiot przetwarzający"[50]), a nadto przepisy zakreślające zakres obowiązków administratora polegających na właściwym zabezpieczaniu danych i ich przetwarzania (art. 24, 25, 28, 32). W świetle tych uregulowań norma z art. 51, wykładana w oparciu o inne przepisy uodo, zdaje się nie budzić żadnych wątpliwości, jak też w żadnym zakresie nie stać w opozycji do regulacji z rozporządzenia, tak jak to miało miejsce w przypadku art. 49. W związku z tym, oparcie wykładni typów czynów zabronionych z art. 51 wyłącznie o przepisy rozporządzenia nie powinno, poza sytuacją poniższą, prowadzić do rezultatów znacząco odmiennych od wykładni opartej na przepisach uodo.

De lege lata, należy podkreślić słuszne podejście ustawodawcy polskiego, którego próżno szukać w GDPR, statuujące możliwość pociągnięcia do odpowiedzialności karnej podmiotu wprawdzie nieadministrującego, lecz obowiązanego do ochrony danych osobowych, co zakreśla szersze pole ochrony niż ta, która wynikałaby bezpośrednio z rozporządzenia (w świetle rozdziału IV rozporządzenia, odpowiedzialność za bezpieczeństwo danych ciąży na administratorze

[50] Na gruncie GDPR dużo łatwiej, niż w uodo, jest znaleźć podstawę normatywną znamienia „administrującego" danymi/zbiorem danych. W świetle definicji legalnych z art. 4 pkt 7 i 8, należy uznać, iż „administrującego" rekonstruować należałoby jako „administratora" oraz „podmiot przetwarzający". Należy także zwrócić uwagę na słuszność przytoczonego wcześniej poglądu SN, który, definiując znamię „administrującego", wskazał na różnorakie podstawy prawne uprawnień tegoż podmiotu, co pokrywa się z art. 28 ust. 3 rozporządzenia: „Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego(…)".

i podmiocie przetwarzającym, czyli *de facto* jedynie na „administrującym", posługując się terminologią z ustawy polskiej). W wyniku takiej konstrukcji znamienia podmiotowego w art. 51 uodo, ochrona ta jest pełna w kontekście *ratio legis* przepisu, obejmując wszelkie możliwe do wyobrażenia sytuacje, których społeczna szkodliwość naruszenia obowiązku ochrony danych wymagałaby kryminalizacji.

Należy jednak skonstatować, że konstrukcja znamienia podmiotowego w art. 51 nie byłaby w żadnej mierze sprzeczna z regulacjami rozporządzenia, obejmuje bądź co bądź swym zakresem zarówno odpowiedzialność podmiotów, które w rozporządzeniu *expressis verbis* zostały wskazane jako odpowiedzialne za bezpieczeństwo i prawidłowe przetwarzanie danych, jak i także innych osób obowiązanych do ochrony danych osobowych, co daje jednostce znacznie szerszą i pełniejszą ochronę niż ta wynikająca wprost z GDPR. W związku z tym, taka konstrukcja znamienia (a właściwie „znamion", w kontekście ust. 1 i ust. 2 wspomnianego artykułu) podmiotowego mogłaby, bez konieczności wprowadzania zmian, obowiązywać także na gruncie nowego stanu prawnego, od momentu rozpoczęcia obowiązywania przez GDPR.

Następne z przestępstw z uodo, stypizowane w art. 52, pozostaje w bezpośredniej relacji z art. 24, 25, 28, 32, a pośrednio także z art. 33 i 34 rozporządzenia GDPR. Art. 52 uodo jest przestępstwem częściowo odsyłającym, bowiem przewiduje „obowiązek zabezpieczenia danych", a obowiązki te oraz towarzyszące im warunki określone zostały w art. 36-39 ustawy. Abstrahując od niedostatków w konstrukcji znamienia podmiotowego w tym typie[51], należy łącznie w stosunku zarówno do regulacji z uodo, jak i z GDPR wysnuć wniosek o niewystarczającym określeniu spektrum podmiotów obowiązanych do zabezpieczenia danych (na gruncie art. 52 jest to „administrujący danymi", podobnie jak i na gruncie art. 32 GDPR[52]). O ile w przypadku samego rozporządzenia skutek ów nie będzie prawnokarnie relewantny, o tyle w przypadku samej ustawy ma to, dla odpowiedzialności karnej, kolosalne znaczenie, o czym wspomniano we wcześniejszej części opracowania. Zasadne jest zatem postulowanie wprowadzenia do art. 52 zmiany w zakresie znamienia podmiotowego, polegającej na dodaniu do określenia kręgu podmiotów sprawczych także przesłanki „osoby obowiązanej do

[51] Por. uwagi odnośnie do znamienia „administrującego danymi" w art. 52.

[52] Jakkolwiek rozporządzenie nie posługuje się pojęciem „administrującego" zbiorem danych/danymi, definicja „administratora" i „podmiotu przetwarzającego" z rozporządzenia oraz łączne interpretowanie tych pojęć prowadzą do konkluzji, iż stosunek zakresowy zbioru desygnatów pojęcia „administrujący" z uodo z sumą zbiorów desygnatów pojęć „administrator: i „podmiot przetwarzający" z rozporządzenia będzie stosunkiem zamienności, o czym była mowa wcześniej.

ochrony danych osobowych". Zmiana taka nie stałaby w sprzeczności z unormowaniami GDPR, a dawałaby jednostce znacznie szerszą (a tak naprawdę pełną) ochronę, mając na uwadze *raio legis* przepisu.

W zakresie samych obowiązków zabezpieczania, należy stwierdzić, że art. 36 i n. uodo, które podlegają wykładni podczas rekonstrukcji znamion typu z art. 52, istotnie pokrywają się z unormowaniami art. 32 GDPR. Unormowania z rozporządzenia, jakkolwiek mają zakres szerszy i bardziej precyzyjny niż te z ustawy (dotyczy to np. aspektów związanych z pseudonimizacją i szyfrowaniem danych osobowych, regularnym testowaniem środków technicznych mających zapewniać bezpieczeństwo danych – art. 32 ust. 1 czy kryteriów uwzględniania ochrony danych już w fazie projektowania sposobów przetwarzania – art. 25 ust. 1), w perspektywie *stricte* normatywnej mają charakter uzupełniający i uszczegóławiający przepisy uodo. Oznacza to, że wejście w życie rozporządzenia GDPR nie wpłynie w żaden sposób na samą konstrukcję znamion, stanowić będzie jedynie swoistą modyfikację wykładniczą, rozszerzająca i uszczegóławiającą zakres kryminalizacji (gdyż, jak wspomniano powyżej, obowiązki w zakresie bezpieczeństwa przetwarzania danych są nieco szersze w akcie prawa unijnego niż w uodo).

Najbardziej powściągliwy, jeśli chodzi o budowę, typ czynu zabronionego z art. 53 uodo, odwołujący się w konstrukcji znamion do art. 40 i n. ustawy, koresponduje jednoznacznie z art. 30 GDPR (przepisy ustawy i rozporządzenia statuują obowiązek prowadzenia rejestru danych osobowych). Naczelną sprzecznością pomiędzy regulacją ustawową a wynikającą z rozporządzenia jest fakt, iż, zgodnie z art. 40 ust. 1 uodo administrator (administrujący) ma obowiązek zgłoszenia zbioru danych do rejestracji, sam zaś rejestr zbiorów danych osobowych prowadzony jest przez GIODO (art. 42 ust. 1 uodo). Z kolei, zgodnie z art. 30 rozporządzenia GDPR, rejestr czynności przetwarzania danych osobowych prowadzą „każdy administrator oraz – gdy ma to zastosowanie – przedstawiciel administratora"[53]. Rozbieżność ta ma charakter fundamentalny dla całego art.

[53] Samo określenie podmiotu obowiązanego zarówno na gruncie art. 53 uodo, jak i na gruncie art. 30 GDPR jest zatem tożsame. Bazując na wcześniejszych ustaleniach (por. uwagi do art. 53 i znamienia podmiotu sprawczego), zgodnie z uodo obowiązek rejestracyjny ciąży na „administrującym" i innej osobie obowiązanej do dokonania zgłoszenia (np. na podstawie stosunku cywilnoprawnego czy administracyjnoprawnego), z kolei zgodnie z art. 30 GDPR, ciąży on na „administratorze" i „przedstawicielu administratora". „Przedstawicielem administratora" jest zatem zarówno „podmiot przetwarzający", co wynika *explicite* z art. 4 ust. 8 rozporządzenia, jak i także inne podmioty. W rezultacie należy uznać, iż stosunek zakresowy zbiorów desygnatów tych pojęć w obu regulacjach jest stosunkiem zamienności, potwierdza to zatem słuszność przyjętego przy interpretacji znamienia podmiotowego z art. 53 stanowiska.

53 uodo, bowiem bez przetransformowania znamion typu, stałby się on od momentu wejścia w życie rozporządzenia normą pustą. *De lege ferenda* należy zatem postulować, by ustawodawca, wraz z chwilą wejścia w życie GDPR, następująco skonstruował znamiona tego typu czynu zabronionego z art. 53: „Kto będąc do tego obowiązany nie prowadzi rejestru czynności przetwarzania danych osobowych, za które odpowiada, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku". Tak uformowane znamiona pozwoliłyby urzeczywistnić modyfikację *ratio legis* przepisu, konieczną ze względu na unormowania rozporządzenia, nie powodując jednocześnie żadnych konsekwencji systemowych w obszarze prawnokarnej ochrony danych osobowych.

Zachowując konwencję przyjętą podczas analizy typologicznej przestępstw z uodo, kolejnym poddawanym analizie w świetle GDPR przepisem będzie art. 54a uodo. Norma wynikająca z tej regulacji, mająca za zadanie chronić niezależność GIODO[54] i zapewniać mu swobodę realizacji kompetencji kontrolnych, pozostaje w bezpośrednim związku z art. 51, 52, 55, 56, 57 (zwłaszcza ust. 1 lit a i h) oraz pośrednio z art. 58 rozporządzenia. Przepisy te, statuujące obowiązek państwa członkowskiego zapewnienia funkcjonowania przynajmniej jednego niezależnego organu monitorującego przetwarzanie danych osobowych (art. 51 i 52 GDPR) oraz określające kompetencje tegoż organu (art. 55-57), korespondują klarownie z art. 12 i n. uodo, formułującymi zadania, kompetencje i aspekty organizacyjne działalności GIODO. Ze względu jednak na fakt, iż norma z art. 54a uodo tyczy udaremnienia/utrudnienia jedynie czynności kontrolnej, a nie wszystkich wymienionych w ustawie (rozporządzeniu) czynności dokonywanych przez inspektora, należy uznać, że przepisy rozdziału VI rozporządzenia nie będą w sposób znaczący wpływały na zakres kryminalizacji art. 54a. Jedyną zasadniczą różnicą będzie tutaj fakt, że z momentem wejścia w życie nowej ustawy o ochronie danych osobowych[55], do rekonstrukcji znamion (czyli

[54] W przytaczanym już wcześniej projekcie nowej uodo, instytucja Generalnego Inspektora Ochrony Danych Osobowych zostanie zniesiona, a w jego miejsce powołana zostanie instytucja Prezesa Urzędu Ochrony Danych Osobowych. Zmiana ta jest jednak w dużej mierze zmianą nie organizacyjną, a terminologiczną. Chodzi bowiem o to, że art. 37 GDPR wprowadza instytucję „inspektora ochrony danych" (będzie o tym mowa poniżej), który byłby podmiotem całkowicie odrębnym od „niezależnego organu publicznego", mającego zapewniać przestrzeganie przepisów rozporządzenia (art. 51 GDPR), czyli GIODO. Doszłoby zatem do sytuacji, w której GIODO i podlegli mu inspektorzy byliby odmienną kategorią „inspektorów" od „inspektorów" z art. 37 GDPR. W celu uniknięcia nieścisłości terminologicznych, projektodawcy proponują więc zastąpienie GIODO „Prezesem Urzędu Ochrony Danych Osobowych" (art. 20 i n. projektu nowej uodo).

[55] Oczywiście przy hipotetycznym (i prawdopodobnie kontrfaktycznym, o czym będzie mowa w dalszej części opracowania) założeniu, że w nowej uodo znalazłby się odpowiednik obecnego art. 54a.

do określania uprawnień „kontrolujących" podległych PUODO lub samemu PUODO) konieczne byłoby odwołanie nie do ustawy, jak ma to miejsce obecnie, a do rozporządzenia GDPR. Sam jednak normatywny sens przepisu byłby tożsamy z tym, jaki wynika z obecnego stanu prawnego.

W przypadku ostatniego z badanych przepisów karnych uodo, art. 54, przy rekonstruowaniu znamion typu i dekodowaniu normy odwołać się musimy do bodaj najszerszej spośród wszystkich przepisów karnych ustawy grupy uregulowań z GDPR. Jakkolwiek, o czym była mowa, w obecnym stanie prawnym odczytywanie normy z art. 54 uodo odbywa się jedynie w oparciu o odesłanie do samej ustawy, a ściślej do art. 24, 25, 32 i 33, o tyle z chwilą wejścia rozporządzenia w życie, istotnie rozszerzony zostałby zakres kryminalizacji objęty normą z art. 54, bowiem zarówno uprawnienia informacyjne, jak i kontrolne, na gruncie aktu unijnego są znacząco szersze niż na gruncie samej ustawy.

Mając na uwadze okoliczność, że art. 54, podobnie jak jego poprzednicy, jest przepisem odsyłającym w rekonstrukcji znamion do innych przepisów ustawy, należy zestawić ze sobą odpowiednie unormowania ustawowe i wynikające z rozporządzenia: art. 24 uodo i art. 13 GDPR (obowiązek informacyjny wobec osoby w przypadku, gdy dane osobowe jej dotyczące zbierane są od niej samej), art. 25 uodo i art. 14 GDPR (informowanie osoby w przypadku, gdy dane jej dotyczące zbierane są w sposób inny niż od niej samej), art. 32 ust. 1 uodo i art. 15 ust. 1 GDPR (zakres uprawnień dostępu/kontroli przetwarzania danych), art. 32 ust. 1 pkt 6 uodo i art. 16 i pośrednio 17 GDPR (prawo do żądania korekty: sprostowania, uzupełnienia, usunięcia, etc. danych). Warto także wspomnieć o art. 12 GDPR, konstruującym ogólne warunki informowania o prawach osoby, której dotyczą dane, a także statuującym tryb wykonywania przez tę osobę praw w celu uzyskania od administratora/administrującego, przy zastosowaniu „odpowiednich środków w celu zwięzłej, przejrzystej, zrozumiałej i w łatwo dostępnej formie, jasnym i prostym językiem – w szczególności gdy informacje kierowane są do dziecka" informacji, o których mowa w artykułach następnych rozporządzenia.

Nie wchodząc w szczegółowe analizy, które przekraczałyby zakres niniejszego opracowania, należy skupić się na najistotniejszych odmiennościach pomiędzy poszczególnymi przepisami, wskazując ich wpływ na zakres normowania art. 54 uodo. Dotyczą one szerszego katalogu obowiązków informacyjnych w GDPR niż w uodo, które to różnice dotyczą nieobjętych unormowaniami ustawy art. 13 ust. 1 lit. b, d, f oraz ust. 2 lit. a, c, d, f, oraz ust. 3 rozporządzenia.

Kolejno, wymieniając powinności, które nie zostały zawarte w art. 24 uodo, art. 13 ust. 1 lit. b GDPR wprowadza obowiązek poinformowania podmiotu,

od którego zbierane są dotyczące go dane, o danych kontaktowych inspektora ochrony danych osobowych[56], w sytuacji oczywiście, gdy będzie mieć to zastosowanie (tj. wtedy, gdy istnieć będzie w danej jednostce instytucja inspektora ochrony danych osobowych). Zgodnie natomiast z art. 13 ust 1 lit f, również, gdy będzie miało to zastosowanie, administrujący mieć będzie obowiązek poinformowania o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub, w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi GDPR, uczynienia wzmianki o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych. Wątpliwość może budzić art. 13 ust. 1 lit. d rozporządzenia (obowiązek poinformowania, jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f – o prawnie uzasadnionych interesach realizowanych przez administratora lub przez stronę trzecią). Zważywszy na fakt, iż obowiązek udzielenia takiej informacji nie został uwzględniony w art. 24 ust. 1 uodo, stwierdzić należy, iż w tym zakresie wejście rozporządzenia w życie rozszerzyłoby zakres kryminalizacji normy z art. 54 ustawy.

Dalsze, szersze niż na gruncie uodo obowiązki informacyjne administrującego wprowadzają art. 13 ust. 2 lit a, c, d oraz f, a także ust. 3 GDPR. Konieczne zatem będzie informowanie o, kolejno: okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu; jeżeli przetwarzanie odbywałoby się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) – o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem; o prawie wniesienia skargi do organu nadzorczego (mowa tu o PUODO (obecnie GIODO), a nie o wspomnianym inspektorze danych – dop. A.R.); o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne

[56] Zgodnie z art. 37 i n. GDPR, z chwilą wejścia rozporządzenia w życie, w przypadkach określonych w rozporządzeniu (art. 37 ust. 1 – sytuacje obligatoryjne, ust. 4 – fakultatywne i obligatoryjne), konieczne (lub możliwe) będzie ustanowienie przez podmioty przetwarzające dane tzw. „inspektorów danych osobowych". W najszerszym zakresie obowiązek ustanowienia inspektora dotknie organy i podmioty publiczne (art. 37 ust. 1 pkt a), bowiem będą musiały one ustanowić inspektora zawsze, bez względu na rodzaj i cel przetwarzania danych. Kompetencje i zadania inspektora będą znacznie szersze, niż np. administratora bezpieczeństwa informacji, zdefiniowanego w art. 36a uodo. W zakresie, w którym kompetencje tych organów (nazwanie „organem" administratora bezpieczeństwa informacji jest oczywiście umowne) będą się pokrywały, niewątpliwie rola i kompetencje administratora bezpieczeństwa informacji zostaną ograniczone.

informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą. Ust. 3 nakłada z kolei na administrującego obowiązek poinformowania, w przypadku, gdy planuje on dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed dalszym przetwarzaniem, osoby, której dane dotyczą, o tym innym celu oraz udzielenia jej wszelkich innych stosownych informacji, o których mowa w ust. 2 art. 13 GDPR. Warto także zaznaczyć, że „odpadnie" przesłanka zwalniająca od obowiązku informacyjnego, zawarta w art. 24 ust. 2 pkt 1 uodo, bowiem art. 13 ust. 4 GDPR dopuszcza możliwość wyłączenia obowiązku informacyjnego jedynie w przypadku, gdy osoba, której dane dotyczą, dysponuje już informacjami objętymi zakresem przedmiotowym obowiązku.

Przechodząc do komparycji art. 25 uodo i art. 14 GDPR, należy zwrócić uwagę na to, iż artykuły te są rozszerzone w stosunku do swoich odpowiedników, odpowiednio art. 24 uodo i art. 13 GDPR, powielając jednak w większości unormowania tych przepisów. W związku z tym, przedstawione zostaną te różnice, które nie zostały już omówione powyżej.

Naczelną różnicą pomiędzy uregulowaniami uodo a uregulowaniami GDPR jest termin, w którym wskazane wyżej informacje miałaby zostać przez administrującego udzielone. Zgodnie z art. 25 ust 1 zd. 1 uodo, obowiązek poinformowania powinien być spełniony „bezpośrednio po utrwaleniu zebranych danych", natomiast zgodnie z art. 14 ust. 3 rozporządzenia, termin ten określony został: lit. a – jako rozsądny termin po pozyskaniu danych osobowych, ale najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych; lit. b - jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lit. c - jeżeli (administrujący) planuje ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu. Obecnie zatem termin udzielenia informacji określony jest w uodo nieostro, doktrynalnie twierdzi się, iż „może to być przy okazji pierwszej operacji na danych, w tej jednak sytuacji operacja ta powinna być przeprowadzona w możliwie krótkim odstępie czasu od zgromadzenia danych"[57]. Chodzi zatem o poinformowanie w możliwie jak najkrótszym odstępie czasu od utrwalenia danych. Nieostrość tego sformułowania nastręcza jednak wielu problemów w kontekście zasady *nullum crimen sine lege certa* i może prowadzić do nadużyć, stąd też precyzyjne

[57] D. Wociór, *Ochrona danych osobowych i informacji niejawnych z uwzględnieniem ogólnego rozporządzenia unijnego*, Warszawa 2016, System Informacji Prawnej Legalis.

wskazanie terminów (a ściślej – nieprzekraczalnych ich granic) w GDPR należy odczytywać pozytywnie w kontekście ustawowej określoności znamion typu z art. 54 uodo.

Istotne rozbieżności w kontekście rekonstrukcji znamion typu z art. 54 uodo powodować może także różnica między art. 25 ust. 2 ustawy a art. 14 ust. 5 rozporządzenia, tj. inkongruencja dotycząca wyłączeń obowiązków informacyjnych. Najwięcej trudności interpretacyjnych nastręczają art. 25 ust. 2 pkt 1 i 5 uodo, bowiem regulacje te nie są tożsame z regulacją z art. 14 ust. 5 lit. c GDPR. Wydaje się jednak, iż relacja tych norm do siebie nie jest relacją wykluczania, a krzyżowania, w związku z tym w zakresie, w jakim czy to sytuacja, w której przepis innej ustawy przewidywałby lub dopuszczałby zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą (art. 25 ust. 2 pkt 1 uodo), nie przewidując jednocześnie odpowiednich środków chroniących prawnie uzasadnionych interesów osoby, której dane dotyczą, czy to sytuacja, w której dane przetwarzane byłyby przez administratora (administrującego), o którym mowa w art. 3 ust. 1 i ust. 2 pkt 1 uodo, na podstawie przepisów prawa (art. 25 ust. 2 pkt 5 uodo), byłyby niezgodne z art. 14 ust. 5 lit. c GDPR (tj. wyłączeniem obowiązku informowania w sytuacji, gdy pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator (administrujący), przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą), norma wyinterpretowywana z art. 54 uodo miałaby szerszy (ze względu na węższy, w zakresie wspomnianym powyżej, obszar normowania) zakres kryminalizacji niż ten, który wynika z rekonstrukcji znamion typu w oparciu o art. 25 ust. 2 obecnej uodo.

Rozporządzenie wprowadza także jeszcze jedną przesłankę dopuszczającą nieinformowanie jednostki o przysługujących jej prawach, która obecnej uodo jest nieznana. Mowa tu o art. 14 ust. 5 lit d, który to uchyla obowiązek informacyjny, gdy dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej, przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy. Przesłanka ta, *summa summarum*, również częściowo pokrywa się ze wspominanym powyżej art. 25 ust. 2 pkt 1 uodo, aczkolwiek norma z przepisu ustawowego jest od normy z rozporządzenia niewątpliwie szersza. Powodować to musi dla regulacji ustawowej takie same skutki, jak te wyżej wymienione w kontekście relacji tej normy do normy z art. 14 ust. 5 lit. c GDPR, tj. rozszerzenie spektrum sytuacji, w których konieczne byłoby spełnienie obowiązku informacyjnego, a w efekcie tego także rozszerzenie obszaru kryminalizacji przepisu art. 54 uodo.

Kolejne z przepisów immanentnych w kontekście interpretacji art. 54 uodo, tj. art. 32 ust. 1 ustawy i art. 15 ust. 1 GDPR[58], mają charakter całkowicie niesprzeczny i, w perspektywie *stricte* normatywnej, wzajemnie się dopełniający. Część z poszczególnych unormowań jest swoimi odpowiednikami, różniącymi się jedynie redakcją językową (art. 32 ust. 1 pkt 1 zd. 1 uodo i art. 15 ust. 1 zd. 1 GDPR, art. 32 ust. 1 pkt 2 *in principio* uodo i art. 15 ust. 1 lit. a GDPR, art. 32 ust. 1 pkt 5 uodo i art. 15 ust. 1 lit. c GDPR, art. 32 ust. 1 pkt 6 uodo i art. 15 ust. 1 lit. e GDPR), pozostałe zaś, ze względu na to, iż dotyczą odmiennych kwestii, bez przeszkód mogłyby jednocześnie koegzystować. Nic nie stałoby bowiem na przeszkodzie, by regulacje ustawowe przydawały jednostce dodatkowych uprawnień kontrolnych, których mocą samego rozporządzenia jednostka nie otrzymała. Jednakowoż, wskutek rozszerzenia uprawnień kontrolnych jednostki na mocy GDPR na przypadki nieobjęte regulacją ustawową, a nadto w związku z nieuwzględnieniem w rozporządzeniu niektórych z uprawnień kontrolnych wymienionych w art. 32 ust. 1 uodo, zmieni się charakter obowiązku informacyjnego ciążącego na administrującym, a przez to także i prawnokarnie relewantne okoliczności odpowiedzialności na podstawie art. 54 uodo. Z chwilą wejścia w życie nowej uodo, która w ogóle nie posiada odpowiednika art. 32 obecnej ustawy, obszar kryminalizacji normy z art. 52 ulegnie zatem swoistemu „przesunięciu", bowiem trudno określić go jako „rozszerzenie" lub „zawężenie" w stosunku do obszaru kryminalizacji na gruncie obecnego stanu prawnego.

W tym świetle, należy jednak zwrócić uwagę na doniosłą w kontekście uprawnień kontrolnych jednostki różnicę między art. 32 ust. 1 pkt 6 uodo a art. 16 i 17 GDPR (definiującymi rozporządzeniowy odpowiednik art. 32 ust. 1 pkt 6 uodo, a więc art. 15 ust. 1 lit. e GDPR). Na gruncie ustawy, przesłanki korekty („uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia") określone zostały inaczej (jak się wydaje węziej), niż na gruncie art. 16 i (zwłaszcza) art. 17 GDPR (prawo do usunięcia danych, tzw. „prawo do bycia zapomnianym"). W związku z tym, obowiązek informacyjny, stanowiący jedno ze znamion typu z art. 54 uodo, wraz z momentem wejścia w życie rozporządzenia, wyglądać będzie inaczej niż do tej pory. Administrujący, aby uniknąć realizacji znamion typu z art. 54 uodo,

[58] Wskazanie na niniejsze regulacje jest istotne w kontekście art. 33 uodo, który statuuje obowiązek udzielenia informacji na wniosek osoby, której dotyczą dane. Rozporządzenie GDPR nie zawiera takowej regulacji, istotnie jednak oddziałuje na unormowania ustawowe poprzez redefiniowanie przysługujących jednostce uprawnień, np. w zakresie sprostowania/uzupełnienia/usunięcia danych.

zmuszony będzie do udzielenia znacznie rozleglejszej informacji niż dotychczas, uwzględniającej unormowania art. 16 i 17 GDPR.

W tym miejscu, zważywszy na systemową wagę i doniosłość art. 17 GDPR, należy rozważyć, czy ustawodawca polski nie powinien dostosować systemu prawnokarnej ochrony danych osobowych do tej regulacji, a ściślej, czy w systemie prawnokarnej ochrony danych osobowych, zakładając, iż zachowałby on swój obecny kształt także w „przyszłym" stanie prawnym, nie byłoby luki polegającej na braku odpowiedniego unormowania dotyczącego odpowiedzialności za naruszenie obowiązku usunięcia danych, i to zarówno w sytuacji wniesienia odpowiedniego żądania przez osobę, której te dane dotyczą, jak i w sytuacji, gdy obowiązek usunięcia powstałby „z urzędu". Mając na uwadze powinność dążenia ustawodawcy do systemowej spójności i zupełności prawnokarnej ochrony danych osobowych, należy stanąć na stanowisku, iż wprowadzenie takiej regulacji nie tylko nie zaburzałoby systematyki przepisów karnych uodo, ale wydaje się wręcz niezbędne w kontekście hierarchii chronionych przez te przepisy dóbr. Trudno bowiem zaprzeczyć twierdzeniu, że ustawodawca, wprowadzając np. prawnokarną ochronę czynności kontrolnych GIODO, podjął się ustanowienia ochrony poprzez prawo karne dobra prawnego o znacznie niższej wartości, niż miałoby to miejsce w przypadku ustanowienia typu (typów) chroniących prywatność jednostki i zabezpieczających prawnokarnie jej żądanie do usunięcia bezprawnie przetwarzanych danych[59].

Analogiczne uwagi odnieść należy nie tylko do samego prawa do żądania usunięcia informacji w przypadku zaistnienia określonych w art. 17 GDPR przesłanek, ale także do całej sekcji 3 rozporządzenia, a przede wszystkim do art. 16 (prawo żądania sprostowania danych) i art. 18 (prawo żądania ograniczenia przetwarzania).

Potrzebę wprowadzenia typu czynu zabronionego chroniącego jednostkę w tym zakresie uwypukla także sama Konstytucja RP, bowiem jej art. 51 ust. 2 wprowadza, w stosunku do władz publicznych, zakaz pozyskiwania, gromadzenia i udostępniania informacji o obywatelach innych niż niezbędne w demokratycznym państwie prawnym[60], a nadto w ust. 4 przyznaje każdemu prawo do

[59] Oceny tej nie zmienia fakt, iż w projektowanej uodo ustawodawca zdecydował się na przesunięcie regulacji dotyczącej zakłócania czynności kontrolnych organu kontrolnego ze sfery prawa karnego do sfery prawa wykroczeń. O szczegółach tej zmiany będzie mowa w podsumowaniu opracowania.

[60] Jakkolwiek pojęcie „niezbędności" jest niezwykle nieostre, a w związku z tym może utrudniać ustalenie „zbędności" przetwarzania danych, należy tu przytoczyć rozumienie tego pojęcia, jakie zaproponował Trybunał Konstytucyjny w wyroku z dnia 12 listopada 2002 r., SK 40/01,OTK Seria A 2002 nr 6, poz. 81. Zdaniem TK, „wprawdzie przesłanka „niezbędności" nie

„żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą". Nadanie przez ustrojodawcę tak wysokiej rangi wspomnianym uprawnieniom, a także szerokie ujęcie uprawnień do żądania sprostowania/usunięcia/ograniczenia przetwarzania danych na gruncie GDPR muszą prowadzić do jednoznacznej konkluzji, iż system prawnokarnej ochrony danych osobowych jest niezupełny i niekonsekwentny. Jest tak nawet pomimo tego, że ustawodawca wprowadza prawo jednostki do „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" (art. 32 ust. 1 pkt 6 uodo), a także przydaje jej prawa określone w art. 36 ut. 1 pkt 7 i 8 uodo (prawo żądania zaprzestania przetwarzania danych ze względu na szczególną sytuację jednostki oraz prawo wniesienia sprzeciwu wobec przetwarzania 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 danych osobowych innemu administratorowi danych). W związku z tym, w celu pełniejszego zabezpieczenia uprawnień przyznanych jednostce w GDPR, a także mając na uwadze koherentność prawnokarnej ochrony danych osobowych, należy postulować wprowadzenie subsydiarnej, w stosunku do wynikającej z aktu unijnego, regulacji, zapewniającej ochronę prywatności jednostki w tym zakresie.

Proponując brzmienie owego przepisu, jedna z możliwości językowej redakcji tej jednostki mogłaby, mając na uwadze sekcję 3 GDPR, mieć następującą postać: „Kto będąc do tego obowiązany nie dokonuje sprostowania[61] lub usunięcia danych albo nie ogranicza ich przetwarzania, podlega karze…".

jest w art. 51 ust. 2 Konstytucji samodzielnie definiowana, to nie powinno budzić wątpliwości, że pojęcie to nawiązuje do treści art. 31 ust. 3 (zasada proporcjonalności) – chociaż pełni tu rolę czynnika samoistnie ograniczającego wprost zakres gwarancji konstytucyjnej, podczas gdy zasada proporcjonalności uzasadnia ingerencję w treść samego prawa, niezależnie od jego ujęcia w normie konstytucyjnej". To zatem, czy gromadzenie danych jest „niezbędne", czy też „zbędne", oceniać należy każdorazowo w kontekście zasady proporcjonalności. Por. D. Witczak, *Prawnokarna ochrona danych osobowych zawartych w oświadczeniu majątkowym funkcjonariusza pożarnictwa*, „Zeszyty Naukowe SGSP", nr 58 (tom 1)/2/2016, s. 152.

[61] Art. 32 ust. 1 pkt 6 uodo posługuje się sformułowaniem „uzupełnienia, uaktualnienia, sprostowania danych osobowych". Zgodnie jednak z art. 16 GDPR, a także zgodnie z wykładnią językową i celowościową terminu „sprostowanie" należy uznać, iż termin ten zawiera w sobie i „uzupełnienie", i „uaktualnienie", i także inne przypadki korekty błędności danych.

Podsumowanie

Wraz z momentem wejścia w życie rozporządzenia GDPR, regulacje tego aktu w sposób istotny wpłyną na sferę prawnokarnej ochrony danych osobowych, i to niezależnie od tego, czy do czasu rozpoczęcia obowiązywania przez ów akt wejdzie w życie także nowa ustawa o ochronie danych osobowych (obecnie najnowszym projektem ustawy jest ten z 12.09.2017 r. – numer wykazu: UC101[62]). Analizując przepisy karne obecnej uodo w kontekście GDPR, skonstatować należy, iż rozporządzenie, najczęściej, miałoby wpływ jedynie na aspekt wykładniczy znamion typów (art. 49, 51, 52, 54, 54a), zmieniając co prawda mniej lub bardziej obszar normowania niniejszych przepisów, nie powodując jednak konieczności przeformułowania znamion typów bądź ich eliminacji z porządku prawnego. Inaczej sytuacja mieć się będzie w przypadku art. 53, który to, w wyniku zmian wprowadzonych przez GDPR, stałby się normą pustą. Jednakże, do zachowania kryminalnopolitycznego *ratio legis* przepisu i dostosowania go do wymogów określonych w art. 30 GDPR wystarczyłaby jedynie operacja przeformułowania znamion typu, której przykład został w niniejszym artykule zaproponowany.

Stanowczo nie należy zgodzić się z zaproponowaną w uzasadnieniu wspomnianego wyżej projektu nowej uodo argumentacją, optującą za obszerną dekryminalizacją naruszeń przepisów ochrony danych osobowych, stwierdzającą, iż „obowiązujące dziś przepisy wskazują wiele czynów zabronionych, ale jednocześnie zbyt ogólnie opisują znamiona poszczególnych z nich. W konsekwencji prokuratorzy i sądy niechętnie sięgają do tych regulacji, co z kolei przekłada się na niewielką liczbę prowadzonych postępowań", co, zdaniem autorów projektu, tłumaczy „nierozbudowywanie przepisów karnych i ich ograniczenie do niezbędnych z punktu widzenia systemu ochrony danych osobowych"[63] w projekcie nowej ustawy.

W niniejszym opracowaniu wykazano, iż typy czynów zabronionych z obecnej uodo nie nastręczają trudności w zakresie ich wykładni, a już z całą pewnością nie jest zasadny zarzut o zbyt ogólnej i nieprecyzyjnej konstrukcji ich znamion. Ponadto, autorzy projektu całkowicie mylnie uzależniają skuteczność regulacji od ilości prowadzonych postępowań karnych, pomijając zupełnie ich rolę w kształtowaniu prewencji generalnej. Co więcej, nietrafnie implikują, iż „niewielka"

[62] Dostęp online: https://legislacja.rcl.gov.pl/projekt/12302950/katalog/12457652#12457652.

[63] Uzasadnienie projektu ustawy o ochronie danych osobowych z dnia 14.09.2017 r., s. 43. Dostęp online: https://legislacja.rcl.gov.pl/docs//2/12302950/12457652/12457653/dokument308352.pdf.

liczba postępowań prowadzonych na podstawie przepisów karnych uodo wynika z niechęci do wszczynania na tej podstawie postępowań przez organy ścigania. Przyczyny tego zjawiska należałoby się raczej doszukiwać w, po pierwsze, niskiej świadomości społecznej odnośnie do istnienia regulacji karnych chroniących jednostkę przed naruszeniami regulacji dotyczących ochrony danych osobowych i wynikającej z tego możliwości zawiadamiania organów ścigania o możliwości popełnienia przestępstwa (czy nawet występowania w charakterze oskarżyciela posiłkowego subsydiarnego), a po drugie, w zbyt bojaźliwej działalności GIODO, który to, jako naczelny organ kontrolny, zbyt rzadko uznawał za zasadne kierowanie spraw odnoszących się do naruszeń ochrony danych osobowych na drogę karną, nawet, gdy były ku temu powody[64]. Same sankcje administracyjne, jakkolwiek dla podmiotu naruszającego mogą być niezwykle dotkliwe, nie zapewniają wystarczającego stopnia ochrony i możliwości otrzymania rekompensaty przez podmiot pokrzywdzony za naruszenie prawa do prywatności, co z kolei umożliwia prawo karne podczas realizowania funkcji restytucyjnej (art. 46 k.k.) (oczywiście i w tym zakresie prawo karne powinno pełnić jedynie rolę subsydiarną w stosunku do prawa cywilnego i znajdować zastosowanie jedynie w sytuacjach, w których wyrządzeniu krzywdy/szkody towarzyszyłby większy niż znikomy (a najczęściej bardzo wysoki) stopień społecznej szkodliwości, jednakże regulacje prawnokarne „dodatkowo" zabezpieczające jednostkę są, z punktu widzenia rangi chronionego dobra, niezbędne).

Wreszcie, zmniejszenie prawnokarnej ochrony danych osobowych w sposób istotny mogłoby ograniczać możliwość „osobistego" dochodzenia sprawiedliwości przez pokrzywdzoną jednostkę, bowiem, jakkolwiek na mocy GDPR jednostka mogłaby kierować do organu nadzorczego (PUODO) skargę na naruszenie przepisów rozporządzenia[65], to nie oznacza to w żadnej mierze, iż skarga jednostki spowodowałyby czy to wszczęcie postępowania kontrolnego, czy to wydanie decyzji nakładającej na podmiot naruszający sankcję administracyjną. Sytuacji nie poprawi znacząco przyznane jednostce prawo do zaskarżania do sądu wydanych na podstawie wniesienia skargi decyzji, gdyż samo złożenie skargi nie musi implikować wszczęcia postępowania jurysdykcyjnego zakończonego decyzją. Doskonałą egzemplifikacją ukazującą rozbieżność między liczbą skarg wniesionych do organu nadzorczego a liczbą przeprowadzonych postępowań kontrolnych i wydanych decyzji jest relacja liczby skarg złożonych do GIODO

[64] Będzie o tym mowa poniżej przy okazji przytaczania statystyk dotyczących działalności GIODO.

[65] Prawo do wniesienia skargi do organu nadzorczego w przypadku, gdy podmiot twierdzi, że przetwarzanie danych osobowych narusza GDPR, statuuje art. 77 ust. 1 rozporządzenia.

w latach 2011-2015 do liczby przeprowadzonych kontroli i liczby wydanych decyzji, w szczególności przez Departament Orzecznictwa, Legislacji i Skarg oraz Departament Inspekcji[66]. Stale rosnąca liczba wniesionych do GIODO skarg (w 2011 r. było ich 1272, zaś w 2015 r. już 2256) nie przełożyła się na wzrost liczby postępowań kontrolnych, a nawet postępowań tych było coraz mniej (199 w 2011 r. i 175 w roku 2015), nie mówiąc już o liczbie decyzji wydawanych przez Departament Orzecznictwa, Legislacji i Skarg (tu odnotowano nieznaczny, aczkolwiek ewidentnie nieproporcjonalny do liczby skarg wzrost, bowiem w 2011 r. wydano 539 decyzji, zaś w 2015 r. – 647), czy przez Departament Inspekcji (tu liczba decyzji spadła niemal o połowę, z 104 w 2011 r. do 57 w 2015). Świadczy to jednoznacznie o tym, że ochrona administracyjnoprawna (realizowana przez organ nadzorczy), a także ochrona cywilnoprawna, mogąca zapewniać jedynie możliwość dochodzenia zadośćuczynienia za krzywdę/naprawienia szkody i usunięcia skutków naruszenia prawa, są zdecydowanie niewystarczające. Z uwagi na rangę dobra podlegającego ochronie na mocy przepisów dotyczących ochrony danych osobowych (prawo do prywatności), a także gwarancje konstytucyjne i międzynarodowe, abrogację przepisów karnych dotyczących tej problematyki z systemu prawa uznać należy za niedopuszczalną.

Absurdalność tej abrogacji uwidacznia się tym wyraźniej na tle tego, że „skarga", o której mowa art. 77 w zw. z pkt. 141 preambuły GDPR nie jest tożsama z „wnioskiem", o którym mowa w art. 18 ust. 1 obecnej uodo w zw. z art. 61 § 1 k.p.a.[67]. W związku z tym złożenie przez podmiot, który uważa, że naruszono przepisy rozporządzenia, skargi do organu nadzorczego, nie musi być tożsame z wszczęciem postępowania jurysdykcyjnego, zakończonego wydaniem decyzji administracyjnej, co w praktyce, mając na uwadze statystyki dotyczące liczby skarg i liczby wszczętych na ich podstawie postępowań na gruncie obecnego stanu prawnego, oznaczałoby, że istotnie osłabiona zostałaby administracyjnoprawna ochrona przed naruszeniami danych osobowych w stosunku do stanu obecnego, mimo że obecnie ochrona ta i tak jest zbyt słaba.

Wniosków tych nie zmienia nawet ten fakt, że, stosownie do art. 78 rozporządzenia GDPR, podmiot, który twierdziłby, że naruszono przepisy rozporządzenia, miałby możliwość kwestionowania decyzji organu nadzorczego przed sądem (sądem administracyjnym). Po pierwsze, możliwość zakwestionowania

[66] Statystyki rodzajów działalności podejmowanych przez GIODO w latach 2011-2015, źródło: http://www.giodo.gov.pl/541/id_art/4583/j/pl.

[67] Warto nadmienić, że w projektowanej uodo próżno szukać podobnej regulacji. Tryb „skargowy" z GDPR byłby zatem jedynym sposobem do ewentualnego zainicjowania postępowania administracyjnego przez stronę, która uważałaby, że naruszono jej prawa.

postępowania organu nadzorczego przed sądem dotyczy tylko takiego postępowania, które zakończone zostałoby w formie ostatecznej decyzji, a zatem jedynie postępowania jurysdykcyjnego, co, jak wspomniano powyżej, wcale nie musiałoby być przypadkiem częstym. Po drugie, jednostka, całkowicie niezależnie od postępowania administracyjnego (i sądowoadministracyjnego), może (i będzie mogła) dochodzić swoich praw na drodze cywilnoprawnej przed sądem powszechnym (na gruncie obecnego stanu prawnego – art. 23 k.c., na gruncie projektowanej uodo – art. 78-81, pośrednio także art. 23 k.c.). W związku zatem z tym, że obszar ochrony cywilnoprawnej pozostanie niezmieniony (w pewnym zakresie zmieni się tylko jego podstawa prawna), natomiast obszar ochrony administracyjnoprawnej zostanie *de facto* ograniczony, tak drastyczne ograniczenie ochrony prawnokarnej, jakie zaproponowano w projektowanej uodo, ocenione zostać musi jednoznacznie negatywnie.

Równie negatywnie ocenić należy fakt, iż projektodawcy nowej uodo odpowiedzialność karną za bezprawne przetwarzanie danych osobowych ograniczyli jedynie do tzw. danych szczególnych/wrażliwych (art. 9 GDPR). Ograniczenie takie w jedynym przepisie karnym *sensu stricto* w projektowanej uodo uznać należy za całkowicie nieuzasadnione. Nie można zgodzić się z przytoczoną w uzasadnieniu projektu (s. 44) argumentacją, iż kryminalizowanie naruszenia tej kategorii danych jest konieczne ze względu na „wagę naruszenia", co *a contrario* sugeruje, że kryminalizowanie naruszenia innych kategorii danych nie jest konieczne ze względu na niewielką, zdaniem projektodawców, wagę owego naruszenia. Przyjęcie założenia, że naruszenie „zwykłych" kategorii danych osobowych jest *ex ante* mniej „poważne" niż naruszenie danych wrażliwych jest nie tylko bezpodstawne, ale niejednokrotnie także kontrfaktyczne. Oceny „wagi" naruszenia dokonywać można bowiem dopiero *ex post*, albowiem naruszenie jakiejkolwiek kategorii danych osobowych – czy to danych wrażliwych, czy „niewrażliwych", narusza przecież to samo dobro prawne – prawo do prywatności. Dopiero zatem *post factum* możliwa jest ocena, czy dane naruszenie jest naruszeniem „poważnym". W efekcie, projektowany przepis uznać należy za całkowicie nierozważny.

Jedyną racjonalną zmianą zaproponowaną przez projektodawców jest przesunięcie odpowiedzialności za udaremnienie/utrudnienie przeprowadzającemu kontrolę przeprowadzenie czynności ze sfery prawa karnego do sfery prawa wykroczeń (obecny art. 54a, projektowany art. 89 uodo). Mając na uwadze rangę dobra prawnego chronionego przez ten typ czynu zabronionego (niezależność GIODO/PUODO, prawidłowość czynności kontrolnych), należy z aprobatą odnieść się do projektu takiej zmiany. Dobro chronione nie jest bowiem tak

istotne, jak prawo do prywatności jednostki, które chronione jest przez inne przepisy karne uodo (z wyjątkiem art. 53 uodo) i z kryminalnopolitycznego punktu widzenia zasadne jest pozbawienie tego przepisu jego przestępnego charakteru. Podobnie ustawodawca powinien postąpić z normą wyrażoną przez obecny art. 53 uodo, regulację tę (przy uwzględnieniu wskazanych w opracowaniu zmian) „przesuwając" ze sfery prawa karnego do sfery prawa wykroczeń.

Konkludując, należy stwierdzić, iż nietrafne i niezwykle niepokojące są plany projektodawcy nowej uodo, mające na celu ograniczenie sfery prawnokarnej ochrony danych osobowych poprzez przesunięcie, niemal w całości, tej ochrony do sfery prawa administracyjnego i cywilnego. Z uwagi na charakter dóbr podlegających ochronie (prawo do prywatności, prawo do nieujawniania innych niż wymagane przez prawo danych o sobie, itd.), a także regulacje najwyższej rangi (Konstytucja RP, wiążące Rzeczpospolitą prawo międzynarodowe) należy stwierdzić, iż spektrum ochrony karnej powinno zostać w projektowanej ustawie, w stosunku do obecnego stanu prawnego, rozszerzone, a nie zawężone.

Nie ma tu znaczenia fakt liczby postępowań wszczynanych na podstawie przepisów karnych uodo, bo nie chodzi o to, by jak najczęściej karać, a o to, by zapewnić jednostce jak najpełniejszą ochronę jednej z najistotniejszych sfer ludzkiej egzystencji. W związku z tym optować należy za maksymalizacją ilości mechanizmów stanowiących właściwą reakcję na naruszenia praw jednostki. Słuszność tego postulatu uwidacznia się tym wyraźniej w świetle tego, że wbrew intencjom ustawodawcy unijnego, na gruncie prawa polskiego ochrona jednostki przed naruszeniami danych osobowych, zarówno w sferze prawa cywilnego, jak i prawa administracyjnego pod rządami GDPR, wcale nie będzie szersza niż na gruncie obecnego stanu prawnego.

Bibliografia

Akty prawne

Act of Privacy 1974.

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997, Nr 78, poz. 483, ze zm.).

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 1997, Nr 133, poz. 883, ze zm.).

Konwencja Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu dnia 28 stycznia 1981 r. (Dz.U. z 2003, Nr 3, poz. 25).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem

danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119 z 2016 r.).

Karta Praw Podstawowych UE (Dz.Urz.UE C 202 z 2016 r.).

Rezolucja 45/95 Zgromadzenia Ogólnego ONZ z 1985 r. (ogłoszona w dniu 14 grudnia 1990 r.).

Ustawa z dnia 26 czerwca 2003 r. o ochronie prawnej odmian roślin (Dz.U. z 2003, Nr 137, poz. 1300, ze zm.).

Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (Dz.U. z 2001, Nr 128, poz. 1402, ze zm.).

Literatura

Adamski A., *Prawo karne komputerowe*, Warszawa 2000.

Barczak-Oplustil A., *Komentarz do art. 225*, (w:) A. Zoll (red.), *Kodeks karny. Część szczególna. Tom II. Komentarz do art. 117-277 k.k.*, Warszawa 2013.

Barta J., Fajgielski P., Markiewicz R., *Ochrona danych osobowych. Komentarz*, Warszawa 2015.

Barta P., Litwiński P., *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2016.

Bignami F., *The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens*, Bruksela 2015.

Bieniak M., *Odpowiedzialność karna menedżerów*, Warszawa 2015.

Błachnio-Parzych A., *Prawnokarna ochrona inspektora ochrony danych osobowych – przestępstwo udaremnienia lub utrudnienia kontroli przestrzegania przepisów o ochronie danych osobowych*, Dodatek Specjalny do Monitora Prawniczego 2011, nr 3.

Borecka J., *Geneza prawnej ochrony danych osobowych i pojęcie danych osobowych*, Zeszyty Naukowe Instytutu Administracji Akademii im. Jana Długosza w Częstochowie, IV/2006.

Drozd A., *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy*, Warszawa 2004 r.

Giezek J., *Komentarz do art. 225*, (w:) J. Giezek (red.), *Kodeks karny. Część szczególna. Komentarz*, Warszawa 2014.

Herzog A., *Glosa do postanowienia SN z dnia 21 listopada 2007 r. IV KK 376/07*, „Prokuratura i Prawo" 2008, nr 11.

Jagielski M., *Prawo do ochrony danych osobowych. Standardy europejskie*, Warszawa 2010.

Kulesza W., *Ochrona danych osobowych a nowa kodyfikacja prawa karnego w Polsce*, (w:) M. Wyrzykowski (red.), *Ochrona danych osobowych*, Warszawa 1999.

Kuner C., *European data privacy law and online business*, Oksford-NowyJork 2003.

Kurzępa B., *Przestępstwa z ustawy o ochronie danych osobowych*, „Prokuratura i Prawo" 1999, nr 6.

Organiściak M., Zakrzewski R., *Ochrona danych osobowych – przepisy karne*, „Przegląd Ustawodawstwa Gospodarczego"2002, nr 8.

Raglewski J., *Komentarz do art. 116*, (w:) D. Flisak (red.), *Prawo autorskie i prawa pokrewne. Komentarz*, Warszawa 2015.

Sakowicz A., *Prawnokarne gwarancje prywatności*, Kraków 2006.

Sibiga G., *Dostosowywanie prawa polskiego do ogólnego rozporządzenia o ochronie danych*, Warszawa 2016.

Szpor G., *Pojęcie informacji a zakres danych osobowych*, (w:) P. Fajgielski (red.), *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, Lublin 2008.

Westin A., *Privacy and freedom*, Nowy York 1967.

Witczak D., *Prawnokarna ochrona danych osobowych zawartych w oświadczeniu majątkowym funkcjonariusza pożarnictwa*, „Zeszyty Naukowe SGSP", nr 58 (tom 1)/2/2016.

Wociór D., *Ochrona danych osobowych i informacji niejawnych z uwzględnieniem ogólnego rozporządzenia unijnego*, Warszawa 2016.

Woś T., *Postępowanie administracyjne*, Warszawa 2015.

Orzecznictwo

Postanowieniu Sądu Najwyższego z dnia 11 grudnia 2000 r., II KKN 438/00, OSNKW 2001, nr 3-4, poz. 33.

Postanowienie Sądu Najwyższego z dnia 21 listopada 2007 r., IV KK 376/07, KZS 2008 nr 11, poz. 47, Legalis.

Wyrok Trybunału Konstytucyjnego z dnia 12 listopada 2002 r., SK 40/01,OTK Seria A 2002 nr 6, poz. 81.

Źródła internetowe

Słownik języka polskiego PWN online: https://sjp.pwn.pl/.

Projekt nowej ustawy o ochronie danych osobowych - https://legislacja.rcl.gov.pl/projekt/12302950/katalog/12457652#12457652.

Uzasadnienie projektu ustawy o ochronie danych osobowych z dnia 14.09.2017 r. - https://legislacja.rcl.gov.pl/docs//2/12302950/12457652/12457653/dokument308352.pdf.

Statystyki rodzajów działalności podejmowanych przez GIODO w latach 2011-2015 - http://www.giodo.gov.pl/541/id_art/4583/j/pl.

Streszczenie

Artykułu poświęcony jest analizie przepisów karnych ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych zarówno w kontekście obecnie istniejącego stanu prawnego, jak i standardów wyznaczanych przez ogólne rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. o ochronie danych (RODO/GDPR) (stosowane od dnia 25 maja 2018 r.), w celu udzielenia odpowiedzi na pytanie, czy w projektowanej „nowej" ustawie o ochronie danych osobowych, której uchwalenie jest konieczne ze względu na istotne zmiany normatywne wprowadzane przez GDPR, ustawodawca powinien zdecydować się na recepcję dotychczasowych uregulowań w zakresie prawnokarnej ochrony danych osobowych (z uwzględnieniem odpowiednich zmian wynikających ze specyfiki rozporządzenia GDPR), czy też sferę tę powinien zmodyfikować, a to zarówno poprzez znaczącą dekryminalizację pewnych naruszeń bądź przeciwnie –kryminalizację deliktów, które na gruncie obecnego stanu prawnego znajdują się poza spektrum normowania prawa karnego. W opracowaniu dokonano kompleksowej analizy typów czynów zabronionych obecnie obowiązującej ustawy, badając je zarówno w perspektywie ich *ratio legis*, jak też w perspektywie katalogu chronionych przez nie dóbr prawnych oraz również w perspektywie konstrukcyjnych i wykładniczych aspektów typologicznych. Następnie, analizie poddano każdy z tak zbadanych typów czynów zabronionych ustawy w perspektywie uregulowań GDPR, udzielając twierdzącej odpowiedzi na pytanie o ewentualną możliwość recepcji przepisów karnych ustawy o ochronie danych osobowych w obecnym kształcie do ustawy „nowej". W artykule skomentowano także rozwiązania projektowane w „nowej" ustawie o ochronie danych osobowych, poddając je krytyce oraz postulując, z uwzględnieniem odpowiednich modyfikacji koniecznych tak w kontekście rozporządzenia GDPR, jak i ze względu na koherentność systemu prawnokarnej ochrony danych osobowych, recepcję dotychczasowych rozwiązań na grunt nowej ustawy.

SŁOWA KLUCZOWE: prawnokarna ochrona danych osobowych, RODO, GDPR, nowa ustawa o ochronie danych osobowych

Summary

The article presents analysis of criminal offences of Polish ustawa o ochronie danych osobowych 1997 in the perspective of current legal status on personal data protection and also standards set by General Data Protection Regulation 2016, in order to settle whether the projected „new" regulation on personal data protection, which ought to adapt Polish internal law to the requirements foreseen in Union legislation, should or should not adapt the existing criminal regulations itself (obviously, taking into account specific changes due to the GDPR), and if not - should the criminal sphere of personal

data protection be modified either through significant decriminalization of some infringements or, on the contrary - through criminalization of some infringements, which are currently outside the scope of criminal offences on personal data protection. The study provides a comprehensive analysis of all types of crimes from the currently binding act, examined in the perspective of their *ratio legis*, as well as in the perspective of the catalog of legal goods protected by them and also in the perspective of structural and interpretative typological aspects. Then, each crime analysed that way has been also examined in the perspective of the GDPR, which provided an affirmative answer on possibility of reception of criminal infringements from the „old" statute to the „new" one. In the article there is also a commentary on solutions projected in the "new" ustawa o ochronie danych osobowych, as well as some postulates on the reception of existing solutions to the ground of the „new" statute.

KEY WORDS: criminal protection of personal data, GDPR, new ustawa o ochronie danych osobowych, new Polish personal data protection act

Nota o autorze

Adrian Romkowski, student V roku prawa na Wydziale Prawa i Administracji Uniwersytetu Jagiellońskiego w Krakowie; zainteresowania badawcze: obszary styku norm prawa karnego i cywilnego, teorie kar, formy popełnienia przestępstwa, prawo karne procesowe.