Czasopismo Prawa Karnego i Nauk Penalnych
Journal of Criminal Law and Penal Studies
ISSN: 1506-1817 Rok/Volume XXIV: 2020 Zeszyt/No. 1

Weronika Mincewicz-Podrecka[1]

Prawnokarna odpowiedzialność administratorów danych osobowych (w związku z RODO)

Criminal Liability of Personal Data Controllers (Analysis of Changes in the Legal Regulations on the Protection of Personal Data in the Context of the General Data Protection Regulation)

1. Wprowadzenie

Obserwowany w społeczeństwie określanym jako „informacyjne" czy „globalne społeczeństwo informatyczne"[2] wzrost znaczenia informacji nieuchronnie prowadzi do zwiększonego zagrożenia integralności oraz bezpieczeństwa danych osobowych. W tym kontekście za słusznością ochrony danych osobowych za pomocą instrumentów prawa publicznego przemawia waga chronionego dobra prawnego w postaci poufności informacji czy też prywatności jednostki[3]. Prawnokarne instrumenty reakcji na naruszenia ochrony danych osobowych stanowią jedynie pewien fragment całościowej struktury związanej z takimi naruszeniami[4], a ich celowość oraz skuteczność należy rozważać w kontekście innych możliwych do zastosowania rozwiązań. Analizując zagadnienia związane z ochroną danych osobowych, należy również zwrócić uwagę na zmiany związane z obowiązującym od 25 maja 2018 r. Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dn. 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych oraz uchylenia dyrektywy 95/46/WE[5].

[1] Weronika Mincewicz-Podrecka – ✉ weronika.mincewicz@student.uj.edu.pl.
[2] F. Radoniewicz, *Odpowiedzialność*..., s. 21–22.
[3] A. Adamski, *Prawo*..., s. 35 i n.
[4] E. Lederman, *Infocrime*..., s. 287.
[5] Dz. Urz. UE L 2016 r., nr 119, s. 1 i n., dalej: RODO.

Niniejszy artykuł ma na celu odpowiedź na pytanie, czy i w jakim zakresie zasadne jest wprowadzanie prawnokarnych sankcji w stosunku do administratorów danych osobowych. Rozpoczynam go od kluczowej dla zrozumienia omawianej problematyki analizy pojęć danych osobowych oraz administratora danych osobowych. W dalszej części przedstawiam rozważania na temat prawnokarnej odpowiedzialności administratorów danych osobowych, uwzględniając uprzedni oraz obecny stan prawny wraz z charakteryzującymi je różnicami. Kolejno omawiam alternatywę dla stosowania prawnokarnych środków reakcji w postaci sankcji administracyjnoprawnych i analizuję, w jakich sytuacjach jej zastosowanie jest uzasadnione.

2. Przedmiot ochrony

W związku z wejściem w życie RODO, zastępującego dyrektywę 95/46/WE[6], i uchyleniem wcześniej obowiązujących przepisów ustawy o ochronie danych osobowych[7], słuszne jest przyjęcie definicji danych osobowych zawartej w art. 4 pkt 1 rozporządzenia. RODO, jako akt obowiązujący bezpośrednio w państwach członkowskich UE, ma pierwszeństwo w stosowaniu wobec ustawodawstwa krajowego[8]. Normy zawarte w RODO mają też pierwszeństwo przed innymi regulacjami prawa UE, z wyjątkiem szczególnych obowiązków ochrony danych osobowych z dyrektywy 2002/58/WE[9]. Dlatego też pojęcia zdefiniowane w RODO, a w wśród nich pojęcie „danych osobowych", należy traktować jako adekwatne do jednolitego zastosowania na gruncie różnych gałęzi prawa.

Definicja legalna „danych osobowych" zawarta jest w art. 4 pkt 1 RODO, zgodnie z którym:

> „dane osobowe" oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośred-

---

[6] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobody przepływu tych danych, Dz. Urz. WE L 281/31 z 23 listopada 1995 r.

[7] Poza niektórymi artykułami, które zachowują moc jedynie w odniesieniu do postępowań związanych z wykrywaniem, zapobieganiem i zwalczaniem czynów zabronionych oraz wykonywaniem orzeczeń, kar porządkowych i środków przymusu w tych sprawach.

[8] P. Kowalik, D. Wociór, *Zastosowanie*..., s. 4.

[9] P. Litwiński, P. Barta, M. Kawecki, w: *Rozporządzenie*..., wprowadzenie, teza III 4.4.

> nio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

W świetle definicji RODO danymi osobowymi są **wszelkie informacje**, nie jest więc możliwe stworzenie wyczerpującego katalogu informacji, które miałyby mieć charakter danych osobowych[10]. Z punktu widzenia klasyfikacji informacji jako danych osobowych nie ma więc znaczenia sposób i forma ich wyrażania, ich prawdziwość czy zrozumiałość. Uznanie informacji za dane osobowe jest każdorazowo zależne od kontekstu, w którym występują[11]. Danymi osobowymi mogą być wyłącznie informacje związane z osobą fizyczną. W szczególności należy zaznaczyć, że pojęcie danych osobowych nie odnosi się do danych osób zmarłych (motyw 27 RODO) oraz osób prawnych (motyw 14 RODO).

Informacja stanowi dane osobowe w rozumieniu RODO jedynie, jeżeli istnieje możliwość powiązania jej ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Za osobę zidentyfikowaną należy uznać osobę, której tożsamość jest znana administratorowi danych w tym znaczeniu, że ma on obiektywną możliwość powiązania z nią konkretnej informacji bez konieczności realizacji dodatkowych aktywności[12]. W poprzednim stanie prawnym w literaturze oraz orzecznictwie występowały spory dotyczące interpretacji pojęcia „możliwej do zidentyfikowania osoby fizycznej", a w szczególności jego subiektywnego bądź obiektywnego charakteru[13]. Istotny w tej kwestii może okazać się motyw 26 RODO, który wskazuje na konieczność analizy uzasadnionego prawdopodobieństwa wykorzystania danego sposobu do zidentyfikowania danej osoby, biorąc pod uwagę: „wszelkie obiektywne czynniki, takie jak koszt i czas potrzebne do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny"[14]. Jak zauważają Litwiński, Barta i Kawecki w komentarzu do RODO[15],

---

10 D. Lubasz, w: *RODO*..., komentarz do art. 4 pkt 1, teza 10.

11 P. Litwiński, P. Barta, M. Kawecki, w: *Rozporządzenie*..., komentarz do art. 4, teza I 4.

12 D. Lubasz, w: *RODO*..., komentarz do art. 4 pkt 1, teza 13.

13 P. Litwiński, P. Barta, M. Kawecki, w: *Rozporządzenie*..., komentarz do art. 4, teza I 18–22.

14 D. Lubasz, *RODO*..., s. 20.

15 P. Litwiński, P. Barta, M. Kawecki, w: *Rozporządzenie*..., komentarz do art. 4, teza I 23.

wprowadzenie w rozporządzeniu nowego wymogu w postaci występowania „uzasadnionego prawdopodobieństwa" możliwości wykorzystania danego sposobu identyfikacji oznacza konieczność interpretacji przesłanki identyfikowalności osoby fizycznej w sposób subiektywny.

Ponadto art. 9 ust. 1 RODO wyodrębnia szczególne kategorie danych osobowych, które podlegają zwiększonej ochronie, a możliwość przetwarzania uzależniona jest od spełnienia dodatkowych przesłanek (art. 9 ust. 1 i ust. 2 RODO). Wyliczenie z art. 9 ust. 1 RODO ma charakter zamknięty i dotyczy: „danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby".

3. Administrator danych osobowych

W wielu przypadkach przyjęte powszechnie praktyki sprawiają, że jednostki udostępniają swoje dane osobowe nie mając pełnego obrazu związanych z tym konsekwencji oraz możliwości kontroli ich wykorzystania[16]. Dlatego też konieczne jest ustalenie kręgu podmiotów przechowujących i przetwarzających dane osobowe, odpowiedzialnych za ich bezpieczeństwo, oraz określenie zasad, zgodnie z którymi ma być ono zapewnione.

Za podmiot kluczowy z punktu widzenia analizy odpowiedzialności za bezpieczeństwo danych osobowych można z pewnością uznać administratora danych osobowych, a interpretacja tego pojęcia będzie miała szczególne znaczenie dla stosowania przepisów związanych z analizowaną tematyką[17]. Zgodnie z art. 4 pkt 7 RODO:

> „administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

---

16 P. Fajgielski, *Zgoda*…, s. 38.

17 D. Lubasz, w: *RODO*…, komentarz do art. 4 pkt 7, teza 2.

Definicja administratora nie uległa zasadniczej zmianie w stosunku do uprzednio obowiązujących przepisów[18].

Zakres podmiotowy pojęcia administratora obejmuje zarówno osoby fizyczne, jak i osoby prawne, organy publiczne oraz inne podmioty. Jest to katalog otwarty, który w szczególności nie wymaga posiadania przez administratora danych osobowości prawnej[19] oraz zawiera w sobie zarówno podmioty z sektora prywatnego, jak i publicznego[20]. Administratorami danych są więc przykładowo spółki osobowe, akcyjne albo z ograniczoną odpowiedzialnością, fundacje, stowarzyszenia, przedsiębiorstwa państwowe, związki wyznaniowe, partie polityczne czy związki zawodowe[21]. Status administratora danych mogą posiadać również oddziały przedsiębiorstw, terenowe jednostki organizacyjne stowarzyszeń, fundusze emerytalne[22] oraz operatorzy wyszukiwarek internetowych[23]. 5 czerwca 2018 r. Trybunał Sprawiedliwości Unii Europejskiej wydał wyrok[24], zgodnie z którym za administratora danych mogą być również uznane portale takie jak Facebook oraz podmioty zarządzające fanpage'ami z uwagi na fakt, iż biorą one udział w decydowaniu o celach oraz sposobach przetwarzania danych osobowych[25].

Administrator danych osobowych może przetwarzać je samodzielnie lub wspólnie z innymi podmiotami. Współudział w administrowaniu danymi osobowymi przybiera różne formy, od ścisłej współpracy do

---

18 D. Lubasz, w: *RODO…,* komentarz do art. 4 pkt 7, teza 3.

19 P. Litwiński, P. Barta, M. Kawecki, w: *Rozporządzenie*…, komentarz do art. 4, teza VII 13.

20 M. Sakowska-Baryła, *Prawo*…, s. 137.

21 D. Lubasz, w: *RODO…,* komentarz do art. 4 pkt 7, teza 4.

22 P. Litwiński, P. Barta, M. Kawecki, w: *Rozporządzenie*…, komentarz do art. 4, teza VII 4–6.

23 Patrz: wyrok TS z 13 maja 2014 r., C-131/12, < http://curia.europa.eu/juris/liste.jsf?language=pl&num=C-131/12 >, w którym za administratora uznany został operator wyszukiwarki internetowej w stosunku do informacji zawierających dane osobowe, które (informacje) są przez operatora lokalizowane, indeksowane w sposób automatyczny, czasowo przechowywane i udostępniane internautom w sposób uporządkowany, zgodnie z określonymi preferencjami.

24 Wyrok TS z 5 czerwca 2018 r., C-210/16, < http://curia.europa.eu/juris/liste.jsf?num=C-210/16&language=PL >.

25 Trybunał zauważył, że: „administrator fanpage'a prowadzonego na Facebooku, taki jak Wirtschaftsakademie, uczestniczy, podejmując działania polegające na ustaleniu parametrów zależnych w szczególności od jego użytkowników docelowych, jak również od celów w zakresie zarządzania lub promocji jego działalności, w określeniu celów i sposobów przetwarzania danych osobowych osób odwiedzających jego fanpage'a" – wyrok TS z 5 czerwca 2018 r., C-210/16, para. 39.

stosunkowo ograniczonego zakresu, związanego tylko z niektórymi celami przetwarzania[26]. Zasady działania i obowiązki współadministratorów danych zostały określone w art. 26 RODO. Przepis dotyczy sytuacji, w której co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania danych[27]. Ustalenia te powinny określać zakres odpowiedzialności związanej z wypełnianiem obowiązków wynikających z RODO, wyznaczać te obowiązki oraz relacje między współadministratorami i podmiotami, których dane dotyczą[28]. Swoboda w dokonywaniu uzgodnień będzie przy tym ograniczona, jeżeli obowiązki przypadające administratorom i ich zakres reguluje prawo UE lub odpowiedniego państwa członkowskiego (art. 26 pkt 3 zd. 2 RODO). Zgodnie z art. 26 pkt 2 zd. 2 RODO zasadnicza treść wyżej wymienionych uzgodnień ma być udostępniana podmiotom, których dane dotyczą. Dodatkowo uzgodnienia dokonane przez administratorów nie mogą wpływać na możliwość wykonywania przez osobę, której dane dotyczą, praw przyznanych jej przez RODO wobec każdego z administratorów.

Kluczową przesłanką konieczną do uznania podmiotu za administratora danych osobowych jest fakt ustalania przez niego celów i sposobów przetwarzania danych osobowych. Ten warunek musiał być również spełniony na gruncie wcześniejszego stanu prawnego, zgodnie ze stanowiskiem NSA, w którym uznał on że: „administratorem danych osobowych nie jest każdy dysponent tych danych, a tylko ten, kto decyduje o celach i środkach ich przetwarzania"[29]. Cele należy tutaj rozumieć jako wartości, do których dąży się poprzez przetwarzanie danych osobowych, a sposoby jako wybrane techniczne sposoby przetwarzania danych[30]. Administrator powinien podejmować decyzje o celach i sposobach przetwarzania danych osobowych samodzielnie, a fundamentalne znaczenie dla jego statusu będzie posiadanie kontroli nad tym przetwarzaniem[31]. Pojęcie administratora należy rozumieć w sposób funkcjonalny, biorąc pod uwagę jego faktyczną kontrolę nad procesem, a nie jedynie formalne ustalenia[32]. To właśnie faktyczne władztwo nad przetwarzanymi danymi

---

[26] D. Lubasz, w: *RODO…,* komentarz do art. 4 pkt 7, teza 6.
[27] P. Litwiński, P. Barta, M. Kawecki, w: *Rozporządzenie*…, komentarz do art 26, teza 1.
[28] P. Litwiński, P. Barta, M. Kawecki, w: *Rozporządzenie*…, komentarz do art 26, teza 2.
[29] Wyrok NSA z 30 stycznia 2002 r., II SA 1098/01.
[30] P. Litwiński, P. Barta, M. Kawecki, w: *Rozporządzenie*…, komentarz do art 4, teza VII 9.
[31] P. Litwiński, P. Barta, M. Kawecki, w: *Rozporządzenie*…, komentarz do art 4, teza VII 9.
[32] D. Lubasz, w: *RODO…,* komentarz do art. 4 pkt 7, teza 7.

osobowymi odróżnia administratora od podmiotu przetwarzającego, zdefiniowanego w art. 4 pkt 8 RODO[33]. Podmiot przetwarzający dane osobowe wykonuje bowiem czynności związane z przetwarzaniem danych osobowych w imieniu administratora i nie podejmuje samodzielnie decyzji na temat celów i sposobów tego przetwarzania[34]. Należy przy tym zaznaczyć, że określenie, jakie działanie stanowi decydowanie o środkach przetwarzania, może sprawiać w praktyce problemy i powinno być zawsze podejmowane w odniesieniu do konkretnej sytuacji[35]. Ustalenie, czy dany podmiot ma status administratora, czy też podmiotu przetwarzającego dane osobowe, będzie miało niewątpliwe znaczenie przy ustalaniu zakresu jego odpowiedzialności, również prawnokarnej.

Podsumowując, zgodnie z art. 4 pkt 7 RODO administrator danych to podmiot, który spełnia łącznie następujące przesłanki:

a) jest osobą fizyczną lub prawną, organem publicznym, jednostką lub innym podmiotem,
b) który samodzielnie lub wspólnie z innymi,
c) ustala cele i sposoby przetwarzania danych osobowych.

Znaczna kontrola, jaką sprawują administratorzy danych osobowych nad procesem ich przepływu, daje podstawę do ustalenia reguł ich odpowiedzialności dążących do realizacji wartości związanych z ochroną danych osobowych, prywatności oraz wolności wypowiedzi[36]. W związku z przetwarzaniem danych osobowych na ich administratorów nałożono szereg obowiązków, które zostały w znacznym stopniu zmodyfikowane przez przepisy RODO. Powinny być one realizowane w sposób zgodny z zasadami zgodności z prawem, rzetelności i przejrzystości, ograniczenia celu, minimalizacji danych, prawidłowości, ograniczenia przechowania oraz integralności i poufności danych wynikającymi z art. 5 RODO[37].

Do obowiązków administratora należy m.in. wdrożenie odpowiednich środków technicznych i organizacyjnych służących zgodności przetwarzania z rozporządzeniem (art. 24 RODO) oraz zapewnieniu

---

33 „«Podmiot przetwarzający» oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora".

34 P. Litwiński, P. Barta, M. Kawecki, w: *Rozporządzenie*..., komentarz do art 4, teza VII 12.

35 D. Lubasz, w: *RODO*..., komentarz do art. 4 pkt 7, teza 9; M. Sakowska-Baryła, *Prawo*..., s. 141.

36 D.C. Nunziato. *With*..., s. 63–64.

37 M. Krzysztofek, *Ochrona*..., s. 103 i n.

wymaganego standardu ochrony (art. 25 RODO). To do niego należy prowadzenie rejestru czynności przetwarzania danych, zgodnie z wymogami z art. 30 RODO. Administrator zobligowany jest również współpracować, w przypadku takiego ich żądania, z organami nadzorczymi w ramach wykonywanych przez nie zadań (art. 31 RODO).

Ponadto na administratorze ciążą obowiązki związane z zapewnieniem bezpieczeństwa przetwarzanych danych osobowych (art. 32 RODO). Stwierdzone naruszenia ochrony danych osobowych mają być przez niego zgłaszane właściwemu organowi nadzorczemu w ciągu 72 godzin po stwierdzeniu naruszenia, poza przypadkami, w których jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych (art. 33 RODO). Jeśli naruszenie ochrony danych osobowych w danej sytuacji może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator informuje o tym również osobę, której te dane dotyczą (art. 34 RODO). Gdy dany rodzaj przetwarzania z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator ma dodatkowo obowiązek dokonać oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych (art. 35 RODO). W pewnych sytuacjach konieczne będzie również wyznaczenie Inspektora Danych Osobowych.

Poza wyżej wymienionymi obowiązkami administrator danych jest również zobligowany do podejmowania czynności związanych z wykonywaniem praw przyznanych osobom, których dane dotyczą, przez RODO. Są one związane przede wszystkim z udzielaniem informacji na temat zbierania i przetwarzania danych oraz z kontrolą jednostki nad dotyczącymi jej danymi osobowymi.

4. Prawnokarne podstawy odpowiedzialności administratorów danych osobowych

Biorąc pod uwagę szczególną rolę administratorów danych osobowych, sam fakt ich odpowiedzialności za prawidłowe przetwarzanie danych osobowych oraz ich bezpieczeństwo nie budzi wątpliwości. Należy jednak postawić sobie pytanie, w jakim zakresie i na jakiej podstawie ta odpowiedzialność ma lub powinna mieć prawnokarny charakter. Zastosowanie regulacji prawa karnego jest uzasadnione wyłącznie w tych

przypadkach, w których nastąpił atak na dobro prawne dzierżyciela[38]. Dodatkowo należy pamiętać o subsydiarnym charakterze prawa karnego i zasadzie traktowania jego instrumentów jako *ultima ratio*[39].

W niektórych przypadkach o wypełnieniu znamion czynu zabronionego lub jego prawnych konsekwencjach decydują szczególne właściwości administratora danych. Po pierwsze, może to nastąpić w sytuacji, w której karane jest działanie administratora danych, a o popełnieniu lub wyższej/niższej karalności czynu zabronionego decydują szczególne cechy tego podmiotu[40] (odpowiednio przestępstwa indywidualne właściwe i niewłaściwe). Przykładem takiego przestępstwa był czyn z art. 51[41] Ustawy z dn. 28 sierpnia 1997 r. o ochronie danych osobowych[42], który mógł być popełniony w formie działania wyłącznie przez podmiot administrujący zbiorem danych lub zobowiązany do ochrony danych osobowych[43].

Po drugie, możemy mieć do czynienia z sytuacją, w której administrator danych, jako szczególny gwarant ich ochrony, poniesie odpowiedzialność za czyn popełniony w formie zaniechania. Zgodnie z art. 2 Kodeksu karnego z 6 czerwca 1997 r.:[44] „Odpowiedzialności karnej za przestępstwo skutkowe popełnione przez zaniechanie podlega ten tylko, na kim ciążył prawny, szczególny obowiązek zapobiegnięcia skutkowi". Należy pamiętać, że przepis ten odnosi się do przestępstw skutkowych (materialnych), a więc wyłącznie w ich przypadku możemy mówić o popełnieniu czynu zabronionego w formie zaniechania[45]. Zaniechanie należy przy tym rozumieć jako niepodjęcie niezbędnych działań mających zapobiec opisanemu w ustawie skutkowi[46]. Dany podmiot ponosi prawnokarną odpowiedzialność za zaniechanie tylko, jeżeli w stosunku do dobra chronionego przez normę znajdował się w pozycji gwaranta

---

38 A. Zoll, *Ochrona*..., s. 223.

39 A. Zoll, *Ochrona*..., s. 223.

40 L. Gardocki, *Pojęcie*..., s. 39.

41 „Art. 51. 1. Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. 2. Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku".

42 Dz.U. 2016, poz. 922.

43 P. Barta, P. Litwiński, *Ustawa*..., komentarz do art. 51, tezy 2–3.

44 Dz.U. 1997, nr 88, poz. 553, dalej: k.k.

45 A. Zoll, w: *Kodeks*..., komentarz do art. 2, teza 3.

46 A. Zoll, w: *Kodeks*..., komentarz do art. 2, teza 7.

zapobiegnięcia wystąpienia tego skutku i miał obowiązek podjęcia w tym kierunku odpowiednich działań[47]. Taki obowiązek musi mieć prawny charakter[48]. Istotny przy tym jest rodzaj chronionych przez gwaranta dóbr oraz charakter występującego dla nich zagrożenia[49]. Należy pamiętać, iż wykonanie czynności zapobiegających wystąpieniu danego skutku musi być co do zasady w zasięgu możliwości gwaranta[50]. Jeżeli chodzi o przypisanie skutku zaniechania, to może być ono oparte wyłącznie na płaszczyźnie normatywnej[51]. Kluczowym dla zdeterminowania odpowiedzialności prawnokarnej administratora danych za przestępstwo popełnione w formie zaniechania jest więc ustalenie istnienia tego szczególnego obowiązku, któremu on podlega, oraz jego aktualizacji.

Już przed analizą poszczególnych przepisów warto zasygnalizować, że problematyka popełnienia przestępstwa w formie zaniechania przez administratora danych ma istotne znaczenie przy rozważaniu jego odpowiedzialności za naruszenia popełnione przez podmioty, którym powierza on przetwarzanie danych[52]. Ustalenie tej odpowiedzialności jest przy tym każdorazowo zależne od treści oraz zakresu obowiązku gwaranta, jego relacji z podmiotem przetwarzającym dane oraz od sytuacji, w której obowiązek został zaktualizowany[53].

Zarówno w przypadku przestępstw, które administratorzy danych osobowych mogą popełnić w formie działania, jak i tych w formie zaniechania należy zwrócić uwagę na skuteczność oraz celowość wprowadzenia prawnokarnych rozwiązań[54]. Jest kwestią sporną, czy i w jakim zakresie przetwarzanie danych osobowych powinno być regulowane przez przepisy prawa karnego[55]. Ich skuteczność jest niejednokrotnie kwestionowana i podnosi się możliwość regulacji tych zagadnień za pomocą narzędzi charakterystycznych dla innych dziedzin prawa np. kar administracyjnych[56].

---

47 A. Zoll, w: *Kodeks…,* komentarz do art. 2, teza 13.
48 A. Zoll, w: *Kodeks…,* komentarz do art. 2, teza 15.
49 A. Zoll, w: *Kodeks…,* komentarz do art. 2, tezy 12–13.
50 A. Zoll, w: *Kodeks…,* komentarz do art. 2, teza 25.
51 A. Zoll, w: *Kodeks…,* komentarz do art. 2, teza 8.
52 Na gruncie RODO będą to podmioty przetwarzające zdefiniowane w art. 4 pkt 8 rozporządzenia.
53 G. Karp, *Analiza*…, s. 211–213.
54 A. Lach, *Problem*…, s. 1191.
55 A. Lach, *Problem…,* s. 1193.
56 A. Lach, *Problem*…, s. 1195.

5. Wcześniejsze regulacje

W związku z wejściem w życie RODO została uchylona Ustawa z dn. 28 sierpnia 1997 r. o ochronie danych osobowych, a na jej miejsce uchwalono Ustawę z dn. 10 maja 2018 r. o ochronie danych osobowych[57]. Na mocy art. 175 OchrDanychU utraciły moc przepisy m.in. rozdziału 8 poprzedniej ustawy, zawierające regulacje prawnokarne. Jak podkreślano już wcześniej w doktrynie[58], obowiązujący w Polsce system wprowadzania za naruszenia związane z danymi osobowymi wyłącznie sankcji karnych, przy braku administracyjnych kar pieniężnych, był rozwiązaniem wyjątkowym na tle praktyki innych państw Unii Europejskiej. System przepisów karnych ustawy był wielokrotnie oceniany jako nieefektywny[59]. Liczba zawiadomień o podejrzeniu popełnionego przestępstwa skierowanych przez Generalnego Inspektora Ochrony Danych Osobowych utrzymywała się na niskim poziomie[60] (jedynie 45 takich przypadków w 2017 r.). Wyroki skazujące za przestępstwa zapadały stosunkowo rzadko – liczba prawomocnie skazanych osób wynosiła odpowiednio: w 2011 r. – 9, w 2012 r. – 16, w 2013 r.– 9, w 2014 r. – 20, w 2015 r. – 9, w 2016 r. – 12[61]. Nie odpowiadało to z pewnością skali występujących w praktyce naruszeń i pojawiały się propozycje zmian funkcjonowania systemu ochrony danych osobowych poprzez wzrost znaczenia instrumentów prawa administracyjnego[62].

6. Obecny stan prawny

Administratorzy danych osobowych mogą ponosić prawnokarną odpowiedzialność na podstawie przepisów zawartych w OchrDanychU,

---

57 Dz.U. 2018, poz. 1000, dalej: OchrDanychU.

58 P. Barta, P. Litwiński, *Ustawa*..., Rozdział 8. Przepisy karne, Wprowadzenie, teza 3.

59 Tak m.in. A. Lach, *Problem*..., s. 1192.

60 Statystyki za lata 2016–2018 r.: < https://giodo.gov.pl/pl/1520114/9175 >, statystyki za lata 2011–2015 r.: < https://giodo.gov.pl/pl/1520114/4583 >.

61 Patrz: Skazania prawomocne – dorośli – wg rodzajów przestępstw i wymiaru kary w latach 2008–2016, < https://isws.ms.gov.pl/pl/baza-statystyczna/opracowania-wieloletnie/ >.

62 K. Buczkowski, *Prawnokarna*..., s. 57–58; P. Barta, P. Litwiński, *Ustawa*..., Rozdział 8. Przepisy karne, Wprowadzenie, teza 5.

przepisów k.k. oraz innych ustaw szczególnych. Zgodnie z art. 116 k.k.[63] w każdym z tych przypadków mają zastosowanie ogólne zasady odpowiedzialności prawa karnego dotyczące m.in. form sprawstwa, kar i środków karnych czy okresów przedawnienia[64]. Ten rodzaj odpowiedzialności na podstawie prawa karnego mogą ponosić wyłącznie osoby fizyczne[65].

Zgodnie z art. 84 ust. 1 RODO: „Państwa członkowskie przyjmują przepisy określające inne sankcje za naruszenia niniejszego rozporządzenia, w szczególności za naruszenia niepodlegające administracyjnym karom pieniężnym na mocy art. 83, oraz podejmują wszelkie środki niezbędne do ich wykonania. Sankcje te muszą być skuteczne, proporcjonalne i odstraszające".

Motyw (149) Preambuły RODO dodatkowo wskazuje, że:

> Państwa członkowskie powinny mieć 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. Jednak nałożenie sankcji karnych za naruszenie takich krajowych przepisów oraz nałożenie sankcji administracyjnych nie powinno prowadzić do naruszenia zasady ne bis in idem, zgodnie z wykładnią Trybunału Sprawiedliwości.

Przy zachowaniu odpowiednich warunków państwa członkowskie UE mogą więc wprowadzać dodatkowe sankcje karne za naruszenie przepisów RODO[66]. Mają być one przy tym skuteczne, proporcjonalne i odstraszające[67], a w przypadku ich zastosowania należy zawsze pamiętać o respektowaniu zasady *ne bis in idem*[68].

Polski ustawodawca na podstawie omówionego powyżej upoważnienia wprowadził w OchrDanychU dwie kategorie czynów zabronionych:

---

63 „Art. 116. Przepisy części ogólnej tego kodeksu stosuje się do innych ustaw przewidujących odpowiedzialność karną, chyba że ustawy te wyraźnie wyłączają ich zastosowanie".

64 K. Buczkowski, *Prawnokarna…,* s. 5–6.

65 K. Buczkowski, *Prawnokarna…,* s. 6.

66 P. Litwiński, P. Barta, w: *Rozporządzenie*…, komentarz do art. 85, teza 1.

67 Mimo problemów z określonością użytych kryteriów należy pamiętać, że ulegają one obiektywizacji poprzez orzecznictwo Trybunału Sprawiedliwości UE oraz ogólne zasady prawa UE – tak: N. Zawadzka, w: *RODO*…, komentarz do art. 85, teza 5.

68 P. Litwiński, P. Barta, w: *Rozporządzenie*…, komentarz do art. 85, teza 2.

a) pierwszą, dotyczącą przetwarzania danych osobowych w sytuacji, w której jest to niedopuszczalne lub przy braku uprawnień (art. 107 OchrDanychU),
b) drugą, polegającą na udaremnianiu lub utrudnianiu kontrolującemu prowadzenia kontroli przestrzegania przepisów o ochronie danych (art. 108 OchrDanychU).

Art. 107 ust. 1 OchrDanychU[69] wprowadza odpowiedzialność karną za zachowanie polegające na przetwarzaniu danych osobowych w sytuacji, w której nie jest to dopuszczalne lub w której ktoś dokonuje przetwarzania danych osobowych mimo braku odpowiednich uprawnień. Przepis ten jest w wielu aspektach podobny do art. 49 ust. 1 uprzednio obowiązującej ustawy. Przedmiotem ochrony jest w tym przypadku prywatność, a dokładniej związana z nią zasada legalności i bezpieczeństwa przetwarzania danych osobowych[70]. Art. 107 ust. 1 OchrDanychU jest przepisem odsyłającym[71], a realizacja znamion opisanego w nim czynu zależna będzie od analizy stanu faktycznego pod względem spełnienia przesłanek dopuszczalności przetwarzania danych osobowych[72]. W obecnym stanie prawnym przesłanki te wymienione są w art. 6 ust. 1 RODO, państwa członkowskie mogą wprowadzać też bardziej szczegółowe regulacje w tym zakresie (art. 6 ust. 2 RODO). Jeżeli przesłanki dopuszczalności przetwarzania danych nie zostaną spełnione, to należy stwierdzić, że zachowanie sprawcy było niezgodne z wymaganiami koniecznymi do legalnego przetwarzania danych osobowych i przy spełnieniu dodatkowych kryteriów będzie możliwe przypisanie mu odpowiedzialności prawnokarnej.

Przestępstwo określone w art. 107 ust. 1 OchrDanychU to przestępstwo powszechne[73] i w związku z tym może być popełnione przez każdy podmiot zdolny do ponoszenia odpowiedzialności karnej, w tym również administratora danych osobowych. Jednak, jak zauważa P. Barta:

> sprawca przestępstwa przetwarzania danych osobowych w sytuacji, gdy przetwarzanie takie jest niedopuszczalne, albo gdy do ich przetwarzania nie jest uprawniony, przez sam fakt podjęcia decyzji o rozpoczęciu przetwarzania danych staje się

69 „Art. 107. 1. Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch".
70 A. Adamski, *Prawo*..., s. 149.
71 A. Adamski, *Prawo*..., s. 147.
72 P. Barta, w: *Ustawa*..., komentarz do art. 107, teza 8.
73 K. Buczkowski, *Prawnokarna*..., s. 9.

administratorem tych danych (jeżeli przetwarza dane we własnym imieniu) albo występuje jako osoba działająca w imieniu administratora danych (jeżeli przetwarza dane w imieniu innego podmiotu, w szczególności osoby prawnej)[74].

Przepis ten wprowadza więc odpowiedzialność prawnokarną za faktyczne podjęcie działań charakterystycznych dla administratora danych osobowych, w szczególności posiadania kontroli nad decyzją o przetwarzaniu danych osobowych. Można ją ponieść w sytuacji, w której samo przetwarzanie danych nie jest dopuszczalne lub w przypadku przetwarzania danych osobowych bez odpowiedniego uprawnienia[75].

Przestępstwo z art. 107 ust. 1 OchrDanychU jest przestępstwem formalnym[76] i w związku z tym nie może być popełnione przez zaniechanie[77]. W konsekwencji nie popełnia wyżej wymienionego przestępstwa administrator danych pozwalający osobie nieuprawnionej na ich przetwarzanie[78]. Jest to przestępstwo umyślne[79]. Przepis wprowadza prawnokarną odpowiedzialność za przetwarzanie danych osobowych w przeciwieństwie do przetwarzania danych osobowych w zbiorze, jak określone to było w uprzednio obowiązującej ustawie[80].

Dodatkowo art. 107 ust. 2 OchrDanychU określa znamiona typu kwalifikowanego, ze względu na przedmiot przestępstwa w postaci szczególnych kategorii danych osobowych[81]. Możliwy wymiar kary za popełnienie przestępstw z art. 107 ust. 1 i ust. 2 to odpowiednio kara grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2 i kara grzywny, ograniczenia wolności albo pozbawienia wolności do lat 3. Na koniec można wspomnieć, że w doktrynie pojawiały się głosy[82]

---

74 P. Barta, w: *Ustawa*..., komentarz do art. 107, teza 10.

75 K. Buczkowski, *Prawnokarna*..., s. 6–7.

76 P. Barta, w: *Ustawa*..., komentarz do art. 107, teza 9.

77 G. Karp, *Analiza*..., s. 214.

78 P. Barta, w: *Ustawa*..., komentarz do art. 107, teza 13.

79 P. Barta, w: *Ustawa*..., komentarz do art. 107, teza 14.

80 Ustawa wprowadzała odpowiedzialność karną za przetwarzanie zbiorów danych, za które – zgodnie z art. 7 pkt 1 – uznawało się: „każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie".

81 Dotyczy on: „danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej".

82 A. Lach, *Problem...,* s. 1195.

przeciwko kryminalizacji nieuprawnionego przetwarzania danych osobowych ze względu na wystarczającą skuteczność sankcji administracyjnych w tym zakresie.

Drugi z przepisów karnych OchrDanychU ma na celu penalizację udaremnienia lub utrudniania kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych (art. 108 OchrDanychU[83]). Zakresowo zbliżony jest on do art. 54a wcześniejszej ustawy, posługuje się jednak innymi terminami[84]. Przedmiotem ochrony omawianego przepisu jest możliwość prowadzenia kontroli bez zakłóceń wywołanych przez podmioty zewnętrzne[85].

Przestępstwo z art. 108 OchrDanychU może być popełnione przez działanie lub zaniechanie[86]. W przypadku formy działania jest to przestępstwo powszechne, którego znamiona mogą być spełnione przez każdego, nie tylko podmioty zobowiązane do współpracy czy ułatwienia kontroli[87]. Do przypisania prawnokarnej odpowiedzialności za analizowany czyn zabroniony w formie zaniechania konieczne jest wykazanie istnienia prawnego szczególnego obowiązku podmiotu. W przypadku administratora danych obowiązek ten musi tworzyć zobowiązanie do podjęcia przez niego odpowiednich czynności mających zapobiec skutkowi w postaci udaremnienia lub utrudnienia prowadzenia kontroli. Na czynności te w przypadku kontroli wskazują przepisy Rozdziału 9 OchrDanychU[88]. Znamię udaremnienia prowadzenia kontroli należy w tym kontekście rozumieć jako całkowite uniemożliwienie jej wykonania, a utrudnianie jako zachowanie faktycznie zakłócające jej prowadzenie[89]. Przestępstwo z art. 108 OchrDanychU może zostać popełnione wyłącznie umyślnie, w zamiarze bezpośrednim oraz ewentualnym[90].

---

83 „Art. 108. Kto udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch".

84 „Art. 54a. Kto inspektorowi udaremnia lub utrudnia wykonanie czynności kontrolnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2".

85 K. Buczkowski, *Prawnokarna*..., s. 18.

86 P. Barta, w: *Ustawa*..., komentarz do art. 108, teza 4.

87 P. Barta, w: *Ustawa*..., komentarz do art. 108, teza 1.

88 Np. stanowiąc w art. 84 ust. 2 OchrDanychU, iż: „Kontrolowany zapewnia kontrolującemu oraz osobom upoważnionym do udziału w kontroli warunki i środki niezbędne do sprawnego przeprowadzenia kontroli".

89 P. Barta, w: *Ustawa*..., komentarz do art. 108, tezy 5–6.

90 K. Buczkowski, *Prawnokarna*..., s. 20.

Za jego popełnienie grozi kara grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2.

Omówione wyżej przepisy stanowiły jedynie część obowiązujących wcześniej prawnokarnych regulacji, które zostały uchylone wraz z wejściem w życie RODO oraz OchrDanychU. Jak już wspominano wyżej, stosowany model ochrony prawnokarnej danych osobowych nie był skuteczny i wystarczający do zapewnienia ich ochrony[91]. Biorąc pod uwagę taką sytuację, ustawodawca zdecydował się na rezygnację z niektórych z przepisów karnych. Jak to określono w projekcie ustawy:[92] „Odpowiedzialność karna ma być jednak wyjątkiem przewidzianym wyłącznie dla najcięższych naruszeń przepisów. Będzie stanowiła uzupełnienie dla szeroko uregulowanej odpowiedzialności administracyjnej i cywilnej, a nie główną oś gwarancji przestrzegania przepisów, jak obecnie". Przestały więc obowiązywać następujące przepisy Ustawy z dn. 28 sierpnia 1997 r. o ochronie danych osobowych:

1) art. 51, penalizujący udostępnianie danych osobom nieuprawnionym;
2) art. 52, dotyczący odpowiedzialności karnej za naruszenie obowiązku zabezpieczenia danych;
3) art. 53, wprowadzający odpowiedzialność karną za niezgłoszenie danych do rejestru;
4) art. 54, penalizujący niedopełnienie obowiązku poinformowania osoby, której dane dotyczą, o jej prawach.

W projekcie podkreślono dodatkowo fakt, iż naruszenie związane z ochroną danych osobowych może stanowić podstawę do poniesienia odpowiedzialności zgodnie z przepisami Kodeksu karnego np. w ramach rozdziału XXXIII Przestępstwa przeciwko ochronie informacji[93].

Z uwagi na krótki okres, który upłynął od wprowadzonych zmian, nie można jeszcze jednoznacznie stwierdzić, czy nowe podejście do ochrony danych osobowych, ograniczające stosowanie prawnokarnych regulacji, będzie w tym zakresie skuteczne. W doktrynie częściowa rezygnacja z kryminalizacji na rzecz sankcji administracyjnoprawnych

---

91 K. Buczkowski, *Prawnokarna*..., s. 53.

92 Projekt ustawy – ochronie danych osobowych z projektami aktów wykonawczych, druk nr 2410, Sejm VIII kadencji, s. 46, < http://www.sejm.gov.pl/Sejm8.nsf/druk.xsp?nr=2410 >.

93 K. Buczkowski, *Prawnokarna*..., s. 47.

oceniana jest najczęściej pozytywnie[94]. Niektórzy autorzy postulowali jednak utrzymanie kryminalizacji udostępniania danych osobowych osobom nieuprawnionym przez osobę, która zobowiązana jest do ich ochrony, z uwagi na szkodliwość społeczną takich czynów połączoną z brakiem możliwości ich penalizacji w formie współsprawstwa czy pomocnictwa do przestępstwa osoby, która w ten sposób uzyskała dostęp do danych osobowych[95].

W tym miejscu nie można również zapomnieć o ochronie danych osobowych w ramach przepisów kodeksu karnego i zakresie, w jakim dotyczyć będzie ona odpowiedzialności prawnokarnej administratorów danych osobowych. Mimo niewątpliwych różnic w znaczeniu pojęcia danych i pojęcia informacji[96] należy zaobserwować, iż przepisy chroniące informacje niejednokrotnie służą równocześnie ochronie danych osobowych. W tym ujęciu dane powinny być rozumiane jako pewnego rodzaju nośnik informacji[97], a dane osobowe jako szczególny, kwalifikowany rodzaj tych danych. Ochronie informacji poświęcony jest rozdział XXXIII Kodeksu karnego, inne przepisy tego kodeksu oraz ustaw pozakodeksowych. Kryminalizacja obejmuje m.in. nieuprawniony dostęp do informacji (art. 267 § 1 k.k.), nieuprawnione ujawnienie informacji (art. 266 k.k.) czy kradzież tożsamości (art. 190a § 2 k.k.).

Z perspektywy kodeksowej odpowiedzialności prawnokarnej możemy mieć więc do czynienia z sytuacjami, w której status administratora danych stanowi przesłankę do stwierdzenia jego uprawnienia do podejmowania określonych, niedozwolonych dla innych podmiotów czynności związanych informacjami (w tym danymi osobowymi). Jest tak np. w przypadku przestępstwa z art. 268 k.k., którego podmiotem może być każda osoba zdolna odpowiadać karnie (przestępstwo powszechne)[98], a klauzula normatywna uprawnienia administratora danych do podejmowania określonych czynności związanych z ich przetwarzaniem sprawia, że nie można przypisać mu odpowiedzialności za ten czyn zabroniony, pod warunkiem, że działa on w zakresie przyznanych

---

94 K. Buczkowski, *Prawnokarna*..., s. 54; P. Barta, P. Litwiński, *Ustawa*..., Rozdział 8. Przepisy karne, Wprowadzenie, teza 5.

95 A. Lach, *Problem*..., s. 1195.

96 A. Adamski, *Prawo*..., s. 38–39.

97 P. Kardas, *Prawnokarna*..., s. 59–60.

98 P. Kardas, *Prawnokarna*..., s. 90–91.

mu uprawnień. Z kolei w innych przypadkach szczególny status administratora danych i jego prawne obowiązki (określone przede wszystkim w RODO oraz OchrDanychU) stanowią podstawę rozszerzonej odpowiedzialności, ze względu na uznanie go za gwaranta nienastąpienia skutku[99]. Przykładem prawnego, szczególnego obowiązku administratora danych może być zapewnienie odpowiedniego stopnia bezpieczeństwa danych osobowych, o którym mówi art. 32 RODO. W większości przypadków z treści takiego obowiązku nie jest możliwe wyprowadzenie odpowiedzialności prawnokarnej na podstawie kodeksu karnego, z uwagi na konstrukcję treściową omawianych przepisów, czy też wymagania związane ze stroną podmiotową w przypadku pomocnictwa[100]. W przypadku pomocnictwa w formie zaniechania konieczne jest wykazanie, że na podmiocie, który nie podjął określonych działań, ciążył w danym kontekście szczególny prawny obowiązek podjęcia działań służących niedopuszczeniu do popełnienia czynu zabronionego i nie został on zrealizowany[101]. Taka sytuacja może mieć miejsce, jeżeli administrator danych, będąc w pozycji gwaranta nienastąpienia skutku, dopuścił się zaniedbania pewnych czynności związanych z zapewnieniem bezpieczeństwa danych osobowych przy jednoczesnym zamiarze, aby ten brak podjętych czynności prowadził do popełnienia przez inną osobę czynu zabronionego np. w postaci uzyskania dostępu do informacji (art. 267 § 1 k.k.).

Na marginesie zauważyć można, że administrator nie ponosi prawnokarnej odpowiedzialności wyłącznie za bezpieczeństwo danych osobowych, ale również za treść przetwarzanych informacji[102] (które niejednokrotnie zawierać będą również dane osobowe). W przypadku, w którym mamy do czynienia z informacjami sprzecznymi z prawem, można się zastanawiać nad zasadnością odpowiedzialności administratora danych, na którego w danej sytuacji nałożony jest szczególny prawny obowiązek kontroli lub nadzorowania przetwarzanych informacji, za pomocnictwo przez zaniechanie do rozpowszechniania przez inne osoby treści zakazanej przez prawo[103]. Jest to koncepcja kontrowersyjna, niemniej jednak demonstruje znaczenie i skalę decyzji podejmowanych

99 A. Zoll, w: *Kodeks*..., komentarz do art. 2, teza 13.
100 P. Kardas, w: *Kodeks*..., komentarz do art. 18, teza 187.
101 P. Kardas, w: *Kodeks*..., komentarz do art. 18, teza 179.
102 M. Siwicki, *Nielegalna*..., s. 227 i n.
103 M. Siwicki, *Nielegalna*..., s. 245.

przez administratora danych w ramach ich przetwarzania[104]. W tym kontekście należy przypomnieć, że zgodnie z obecnym kierunkiem orzecznictwa za administratorów danych uznaje się szerokie spektrum podmiotów, w tym m.in. operatorów wyszukiwarek internetowych[105], administratorów fanpage'ów czy portale społecznościowe[106].

Przy ocenie zachowań administratorów danych osobowych należy pamiętać o wyznaczanych konstytucyjnie fundamentach ochrony danych osobowych, możliwych konfliktach związanych z nimi wartości oraz konstytucyjnych zasadach odpowiedzialności karnej[107]. Będą bowiem one wyznaczać granice przypisania prawnokarnej odpowiedzialności tym podmiotom[108].

7. Regulacje administracyjnoprawne

Zarówno w międzynarodowych, jak i krajowych regulacjach dotyczących ochrony danych osobowych można zaobserwować tendencje do rezygnacji z wprowadzenia przepisów karnych na rzecz przepisów charakterystycznych dla innych gałęzi prawa[109]. Należy stwierdzić, że – pod warunkiem skuteczności tych ostatnich – jest to zgodne z zasadą *ultima ratio* prawa karnego[110].

Z punktu widzenia analizy odpowiedzialności prawnokarnej, a w szczególności związanych z nią zmian wprowadzonych w przepisach RODO oraz OchrDanychU, najistotniejsze będą normy administracyjnoprawne oraz ich relacja z normami prawa karnego. Już podczas obowiązywania poprzedniej ustawy powtarzały się postulaty *de lege ferenda* uchylenia niektórych prawnokarnych przepisów związanych z naruszeniami ochrony danych osobowych i zastąpienia ich sankcjami o charakterze administracyjnoprawnym[111]. Ten kierunek przyjęła reforma ochrony danych osobowych wprowadzana przez przepisy RODO

---

104 D.C. Nunziato, *With*..., s. 64.
105 Taka sytuacja wystąpi przy spełnieniu przez nich pewnych warunków. Więcej: wyrok TS z 13 maja 2014 r., C-131/12.
106 Wyrok TS z 5 czerwca 2018 r., C-210/16.
107 P. Kardas, *Prawnokarna*..., s. 41–42.
108 B. Marcinkowski, *Dane*..., s. 124 i n.
109 A. Lach, *Problem*..., s. 1191 i n.
110 A. Zoll, *Ochrona*..., s. 223.
111 P. Barta, w: *Ustawa*..., komentarz do art. 107, teza 3.

i OchrDanychU, zwiększając zakres odpowiedzialności administracyjnoprawnej administratorów danych i jednocześnie rezygnując z części obowiązujących uprzednio sankcji prawnokarnych.

Przy analizie administracyjnoprawnych regulacji wprowadzających odpowiedzialność administratorów danych osobowych za ich bezpieczeństwo największe znaczenie w aktualnym stanie prawnym mają przepisy RODO oraz OchrDanychU. Należy więc pamiętać o ogólnych zasadach wyprowadzanych z rozporządzenia i zgodnie z nimi stosować sankcje administracyjnoprawne. Obowiązki administratorów danych, takie jak zapewnienie bezpieczeństwa przetwarzania danych osobowych, informowanie o związanych z nimi naruszeniach czy wymagane w niektórych przypadkach uprzednie konsultacje, nie są abstrakcyjnym standardem[112], ale mogą stanowić podstawę ich odpowiedzialności prawnej. Sprawia to, że administratorzy danych faktycznie mają obowiązek podjęcia szeregu działań związanych z kwestiami ochrony danych osobowych, a ich niedopełnienie, w kontekście sankcji administracyjnoprawnych, może skutkować prawną reakcją podjętą przez organy nadzorcze lub przedsięwziętą na drodze sądowej[113].

Art. 51 ust. 1 RODO zobowiązuje państwa członkowskie do ustanowienia publicznego, niezależnego (art. 52 RODO) organu nadzorczego, którego zadaniem jest monitorowanie stosowania przepisów rozporządzenia. W Polsce taką funkcję pełni Urząd Ochrony Danych Osobowych (dalej: UODO). Zadania realizowane przez ten organ oraz jego kompetencje są zbliżone do tych wykonywanych wcześniej przez Generalnego Inspektora Ochrony Danych Osobowych. UODO ma wykonywać szereg zadań związanych z ochroną danych osobowych (art. 57 RODO), a postępowania w sprawie naruszeń przepisów o ochronie danych osobowych prowadzone są przez Prezesa UODO (art. 60 OchrDanychU). Prezes UODO jest również podmiotem, który w drodze decyzji nakłada administracyjne kary pieniężne za naruszenie przepisów RODO (art. 101 OchrDanychU).

W zakresie zadań realizowanych przez UODO szczególnie istotna z perspektywy publicznoprawnej odpowiedzialności administratorów danych osobowych oraz jej zasadności będzie kwestia rodzaju i skutecz-

112 W.G. Voss, *European*..., s. 226 i n.
113 M. Krzysztofek, *Ochrona*..., s. 197–198.

ności potencjalnych sankcji nakładanych przez organ oraz ich porównania ze środkami reakcji prawnokarnej. RODO, w stosunku do uprzednio obowiązującego stanu prawnego, wprowadza bowiem znacznie dotkliwsze administracyjne kary pieniężne.

Administracyjne kary pieniężne nakładane na podstawie RODO muszą być skuteczne, proporcjonalne i odstraszające (art. 83 ust. 1 RODO). Kryteria te powinny być oceniane w każdym przypadku indywidualnie[114] przez organ nadzorczy nakładający taką karę. Administracyjne kary pieniężne mogą być stosowane razem lub zamiast innych środków dostępnych dla organów nadzorczych[115]. Organ musi przy tym brać pod uwagę szereg okoliczności[116], których przykładowy katalog zawiera art. 83 ust. 2 RODO.

Rozporządzenie przewiduje dwie wysokości administracyjnoprawnych kar pieniężnych:[117]

1) administracyjne kary pieniężne do wysokości 10 000 000 EUR, a w przypadku przedsiębiorstwa w wysokości do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego (przy czym zastosowanie ma kwota wyższa) za naruszenia wymienione w art. 83 ust. 4 RODO,
2) administracyjne kary pieniężne do wysokości 20 000 000 EUR, a w przypadku przedsiębiorstwa w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego (przy czym zastosowanie ma kwota wyższa) za naruszenia wymienione w art. 83 ust. 5 i 6 RODO.

Mogą być one nakładane zarówno na osoby fizyczne, jak i na przedsiębiorstwa[118]. Jeżeli system krajowy nie przewiduje administracyjnych kar pieniężnych nakładanych przez organ nadzorczy, to w takim wypadku będą one mogły być nakładane przez właściwe sądy krajowe (art. 83 ust. 9 RODO). Dodatkowo państwa członkowskie mogą, pod warunkiem zawiadomienia Komisji Europejskiej, przyjmować przepisy określające inne sankcje (art. 84 RODO). Na podstawie art. 84 RODO możliwe będzie przyjęcie innych sankcji niż administracyjne kary pieniężne do

---

114 P. Litwiński, P. Barta, M. Kawecki, w: *Rozporządzenie*..., komentarz do art. 83, teza 2.
115 P. Litwiński, P. Barta, M. Kawecki, w: *Rozporządzenie*..., komentarz do art. 83, teza 3.
116 J. Łuczak, w: *RODO*..., komentarz do art. 83, teza 5.
117 A. Lach, *Problem*..., s. 1192.
118 P. Litwiński, P. Barta, M. Kawecki, w: *Rozporządzenie*..., komentarz do art. 83, teza 10.

tych samych naruszeń, które są podstawą administracyjnych kar pieniężnych, oraz innych naruszeń, przy zachowaniu zasady *ne bis in idem*[119].

Należy stwierdzić, że ze względu na dotkliwy charakter administracyjnych kar pieniężnych można się spodziewać, iż będą one w znacznym zakresie skuteczne i zmuszą administratorów danych do dostosowania się do regulacji RODO.

W polskim systemie prawnym zasady stosowania administracyjnych kar pieniężnych sprecyzowane są w rozdziale 11 OchrDanychU. Organem uprawnionym do ich nakładania jest Prezes UODO, który wymierza je w drodze decyzji administracyjnej (art. 101 i art. 102 OchrDanychU). Wiąże się to z koniecznością zachowania wymogów związanych ze stosowaniem tego instrumentu prawnego, jak chociażby uzasadnienie decyzji[120]. Administracyjne kary pieniężne mają być w każdym przypadku skuteczne, proporcjonalne i odstraszające[121], a od decyzji Prezesa UODO stronom przysługuje skarga do sądu administracyjnego[122].

Jak wynika z powyższej analizy, naruszenie obowiązków nałożonych na administratorów danych przez przepisy RODO czy OchrDanychU może skutkować poważnymi konsekwencjami. W tym kontekście słuszny wydaje się postulat precyzyjnego określenia tych obowiązków, który niestety nie jest w zupełności zrealizowany[123]. Zwraca się uwagę na brak jasności języka RODO, który może prowadzić do problemów w interpretacji rozporządzenia[124]. W takiej sytuacji prawdopodobne jest, że z uwagi na obawę przed wysokimi karami administracyjnymi oraz niejasność obowiązujących przepisów[125], stosowanie RODO przez podmioty przetwarzające dane osobowe może nie przynosić zamierzonych efektów dla zapewnienia praw osób, których te dane dotyczą.

8. Podsumowanie

System sankcji karnych oraz administracyjnych za naruszenia ochrony danych osobowych ma służyć przede wszystkim ich skutecznej ochro-

119 J. Łuczak, w: *RODO*..., komentarz do art. 84, teza 6.
120 O. Legat, w: *Ustawa*..., komentarz do art. 101, teza 8.
121 P. Barta, w: *Ustawa*..., komentarz do art. art. 101, teza 4.
122 O. Legat, w: *Ustawa*..., komentarz do art. 101, teza 8.
123 M. Hintze, *Data*..., s. 2 i n.
124 D. Keller, *The Right*..., s. 30–31.
125 D. Keller, *The Right*..., s. 31.

nie i dlatego konieczne jest zachowanie odpowiedniego balansu w zastosowaniu instrumentów charakterystycznych dla tych gałęzi prawa w celu zapewnienia jego sprawnego funkcjonowania. Mimo słuszności stosowania prawnokarnych środków reakcji w pewnych przypadkach[126], należy przyznać rację twierdzeniu, że w praktyce wielokrotnie okazywały się one nieskuteczne. W takiej sytuacji, ze względu na postulat celowości przyjmowanych regulacji, znacznie lepszym rozwiązaniem jest wprowadzenie sankcji administracyjnoprawnych[127] (oczywiście pod warunkiem ich skuteczności).

Systemy ochrony danych osobowych charakteryzujące się położeniem nacisku na sankcje administracyjnoprawne zamiast środków prawnokarnych były już przed wprowadzeniem RODO dominujące w większości krajów członkowskich UE[128]. Nowe regulacje, w szczególności te wprowadzane przez RODO, mają służyć przede wszystkim zapewnieniu wyższego poziomu bezpieczeństwa danych osobowych i pod tym względem konieczne jest zastosowanie tego typu publicznoprawnych środków, które realnie wpłyną na przestrzeganie przepisów w tym zakresie. Środki administracyjnoprawne są w tej sytuacji w wielu przypadkach rozwiązaniem bardziej zasadnym niż teoretycznie obowiązujące w systemie prawnym, ale praktycznie nieczęsto stosowane tradycyjne sankcje karne. Słuszność wprowadzenia tego typu rozwiązań w ustawodawstwie europejskim oraz krajowym potwierdzają wcześniejsze sprawdzenie się systemu kar administracyjnych w innych państwach[129] oraz ogólna ocena surowości wprowadzonych kar administracyjnoprawnych, która sugeruje, że administratorzy danych (oraz inne relewantne podmioty) będą mieli silną motywację finansową do ich stosowania. Nie oznacza to, że powinno się w całości zrezygnować w tej kwestii z zastosowania sankcji prawnokarnych, jednak powinny mieć one ograniczony zakres i dotyczyć najpoważniejszych naruszeń, dla których nie są wystarczające instrumenty reakcji zapewniane przez prawo administracyjne[130].

Nie należy przy tym zapominać, że również rozwiązania opierające się na sankcjach administracyjnoprawnych będą mieć istotny wpływ na

---

126 M. Sakowska-Baryła, *Prawo*..., s. 420.
127 K. Buczkowski, *Prawnokarna*..., s. 54.
128 P. Barta, P. Litwiński, *Ustawa*..., Rozdział 8. Przepisy karne, Wprowadzenie, teza 3.
129 P. Barta, P. Litwiński, *Ustawa*..., Rozdział 8. Przepisy karne, Wprowadzenie, teza 3.
130 A. Lach, *Problem*..., s. 1196.

sposób i zakres przetwarzania danych osobowych oraz innych informacji i ich nadmierna eskalacja może prowadzić do naruszenia wartości związanych z dostępem do informacji i transparentnością[131]. Dlatego też przy zastosowaniu instrumentów każdej z gałęzi prawa, nie tylko prawa karnego, konieczne jest zachowanie balansu pomiędzy ochroną prywatności danych osobowych a wolnością dostępu do informacji czy też wolnością wypowiedzi.

Summary

The subject of this article is to analyze the criminal liability of data controllers in the context of the function they perform in connection with the processing of personal data. The paper answers the question in which situations special obligations should be placed upon data controllers in relation to providing safety of personal data, and to what extent the lack of fulfillment of those obligations may result in violating criminal law provisions. The analysis of these provisions is presented in the context of changes introduced by the General Data Protection Regulation. The relevant regulations are assessed in terms of their effectiveness, proportionality, and purposefulness in protecting the privacy of individuals.

Keywords

data controller, personal data, privacy, General Data Protection Regulation (GDPR), pecuniary administrative sanctions, processing of personal data

Bibliography

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

Barta P., w: *Ustawa o ochronie danych osobowych. Komentarz*, red. P. Litwiński, Warszawa 2018.

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

Buczkowski K., *Prawnokarna problematyka ochrony danych osobowych*, Warszawa 2015.

Fajgielski P., *Zgoda na przetwarzanie danych osobowych udzielana w Internecie*, w: *Internet. Ochrona wolności, własności i bezpieczeństwa*, red. G. Szpor, Warszawa 2011.

Gardocki L., *Pojęcie przestępstwa i podziały przestępstw w polskim prawie karnym*, „Annales Universitatis Mariae Curie-Skłodowska" 2013, sectio G, vol. LX 2.

Hintze M., *Data Controllers, Data Processors, and the Growing Use of Connected Products in the Enterprise: Managing Risks, Understanding Benefits, and Complying with the GDPR*, 2018, < https://ssrn.com/abstract=3192721 > lub < http://dx.doi.org/10.2139/ssrn.3192721 >.

[131] D. Keller, *The Right*..., s. 75.

Kardas P., w: *Kodeks karny. Część ogólna. Tom I. Część I. Komentarz do art. 1–52*, red. W. Wróbel, A. Zoll, Warszawa 2016.

Kardas P., *Prawnokarna ochrona informacji w polskim prawie karnym z perspektywy przestępstw komputerowych. Analiza dogmatyczna i strukturalna w świetle aktualnie obowiązującego stanu prawnego*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2000, nr 1.

Karp G., *Analiza prawnokarnej odpowiedzialności administratora danych jako gwaranta nienastąpienia skutku za przestępstwa materialne popełnione przez zaniechanie*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2009, nr 2.

Keller D., *The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation*, 2017, < https://ssrn.com/abstract=2914684 > lub < http://dx.doi.org/10.2139/ssrn.2914684 >.

Kowalik P., Wociór D., *Zastosowanie przepisów o ochronie danych osobowych w jednostkach sektora publicznego*, w: *Ochrona danych osobowych w sektorze publicznym z uwzględnieniem rozporządzenia unijnego*, red. A. Balicki, Warszawa 2016.

Krzysztofek M., *Ochrona danych osobowych w Unii Europejskiej: transfer danych osobowych z Unii Europejskiej, ze szczególnym uwzględnieniem transferu do Stanów Zjednoczonych, w obecnym i nadchodzącym stanie prawnym*, Warszawa 2014.

Lach A., *Problem kryminalizacji naruszenia przepisów rozporządzenia ogólnego w sprawie danych osobowych*, „Monitor Prawniczy" 2017, nr 22.

Lederman E., *Infocrime: protecting information through criminal law*, Cheltenham – Northampton, MA 2016.

Legat O., w: *Ustawa o ochronie danych osobowych. Komentarz*, red. B. Marcinkowski, Warszawa 2018.

Litwiński P., Barta P., w: *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, red. P. Litwiński, Warszawa 2018.

Litwiński P., Barta P., Kawecki M., w: *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, red. P. Litwiński, Warszawa 2018.

Lubasz D., w: *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018.

Lubasz D., *RODO. Zmiany w zakresie ochrony danych osobowych. Porównanie przepisów. Praktyczne uwagi*, Warszawa 2018.

Łuczak J., w: *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018.

Marcinkowski B., *Dane osobowe: Polska – UE – USA. Współczesne wyzwania. Administracyjnoprawne zagadnienia odpowiedzialności poziomu ochrony danych osobowych na przykładzie amerykańskiego prawa federalnego*, Warszawa 2018.

Nunziato D.C., *With Great Power Comes Great Responsibility: Proposed Principles of Digital Due Process for ICT Companies*, w: *Protection of Information and the Right to Privacy – A New Equilibrium?*, red. L. Floridi, New York 2014.

Radoniewicz F., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016.

Sakowska-Baryła M., *Prawo do ochrony danych osobowych*, Wrocław 2015.