DOI: 10.31648/sp.6615

Maciej Nawacki
Uniwersytet Warmińsko-Mazurski w Olsztynie
ORCID: 0000-0003-0082-7609
wanam1@gmail.com

Kryminalizacja naruszenia ochrony danych osobowych

Wejście w życie przepisów rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych)[1] w 2016 r. i pełne ich stosowanie, począwszy od 25 maja 2018 r., skupiło uwagę opinii publicznej i doktryny prawa[2] na problematyce ochrony danych osobowych. Jednym z aspektów tej ochrony, obok uregulowań prawa administracyjnego, cywilnoprawnej drogi dochodzenia roszczeń przez osoby, których dane osobowe dotyczą, jest karnoprawna reakcja na naruszenie ochrony danych osobowych. Przepis art. 84 RODO nie wymaga kryminalizacji naruszenia danych osobowych, pozostawiając w tym zakresie swobodę państwom członkowskim Unii Europejskiej. Zawiera natomiast nakaz przyjęcia skutecznych sankcji za naruszenia RODO, w szczególności za delikty niepodlegające dotkliwym administracyjnym karom pieniężnym. Zdarzenia skutkujące naruszeniami praw i wolności nawet tysięcy osób związane z wyciekiem danych osobowych, z ich nielegalnym przetwarzaniem czynią jednak zasadnym pytanie o konieczność i zakres kryminalizacji naruszenia zasad przetwarzania danych osobowych.

Wprowadzenie szerszego systemu ochrony danych osobowych, w tym kryminalizacja naruszeń ochrony danych osobowych, stanowi niewątpliwie wyraz ochrony godności ludzkiej w jednym z jej podstawowych aspektów, którym jest

[1] Ogólne rozporządzenie o ochronie danych – Dz. Urz. UE L 119 z 4 maja 2016 r., s. 1 ze zm. (dalej jako RODO).

[2] Konsekwencję wejścia w życie nowych regulacji jest również konieczność wypracowania praktyki ochrony danych osobowych i nadzoru nad ich przetwarzaniem przez specjalne organy w systemie wymiaru sprawiedliwości w rozumieniu motywu 20 RODO, z których wiodącym organem nadzoru jest Krajowa Rada Sądownictwa. Organy te w przeszłości nie rozpoznawały skarg na naruszenia ochrony danych osobowych.

prawo do prywatności[3]. W literaturze RODO przesadnie jest określane nawet jako *Magna Carta* ochrony prywatności[4]. Kryminalizacja naruszeń ochrony danych osobowych jawi się tym samym jako typizacja czynu godzącego w takie dobra chronione, jak cześć, dobre imię, wolność człowieka, co stawia przepisy przewidujące odpowiedzialność prawnokarną za naruszenia RODO w jednym rzędzie z typizacją zniesławienia (art. 212 k.k.), znieważenia (art. 216 k.k.), gróźb karalnych (art. 190 § 1 k.k.), czy utrwalania wizerunku osoby w trakcie czynności seksualnej (art. 191a § 1 k.k.).

Jeden z największych ostatnich wycieków danych osobowych (dane 50 283 osób z bazy danych Krajowej Szkoły Sądownictwa i Prokuratury z siedzibą w Krakowie[5]) stanowi nie tylko niewątpliwe naruszenie praw i wolności osób, których dane dotyczą, ale również godzi w podstawy bezpieczeństwa publicznego. Ujawnienie danych osobowych dotyczy bowiem sędziów, prokuratorów, kuratorów zawodowych, urzędników sądów i prokuratury. Dane te stały się przedmiotem nielegalnego handlu – bezprawnego przetwarzania, w efekcie dostęp do danych (w tym danym adresowych, prywatnych numerów telefonów, adresów poczty elektronicznej) uzyskała bliżej nieokreślona grupa ludzi, a tym samym dane te mogą być wykorzystane przez zorganizowaną przestępczość. Przepisy typizujące naruszenia RODO winny zatem uwzględniać w swojej konstrukcji także dalszy przedmiot ochrony, którym jest bezpieczeństwo publiczne.

Informacja to „ropa XXI wieku", nie dziwi zatem fakt, iż dane osobowe, ich zbiory mają wymierną wartość handlową, przetwarzanie danych stanowi zaś jeden z elementów działalności gospodarczej. Przepisy kryminalizujące naruszenia ochrony danych osobowych zbliżone są tym samym do typizacji przestępstw godzących w obrót gospodarczy i jednocześnie przestępstw przeciwko bezpieczeństwu informacji.

Wieloaspektowość systemu ochrony danych osobowych, rzutująca na konstrukcję przepisów karnych, typizujących naruszenia RODO, współwystępowanie różnych przedmiotów ochrony, charakterystycznych dla różnych rodzajów przestępstw, w tym dla prawa karnego gospodarczego, uzasadnia bliższą analizę zakresu i sposobu kryminalizacji naruszeń ochrony danych osobowych.

---

[3] Zob. M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej*, Warszawa 2014, s. 36 i nast.; M. Sakowska-Baryła, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018, s. 49.

[4] Zob. J. Kühling, J. Raab, [w:] J. Kühling, B. Buchner (red.), *Dattenschutz-Grundverordnung. Bundesdatenschutzgesetz. Kommentar*, München 2020, s. 3, 4.

[5] Decyzja Prezesa Urzędu Ochrony Danych Osobowych z 11 lutego 2021 r., sygn. akt DKN.5130.2024.2020, publ. https://www.uodo.gov.pl/decyzje/DKN.5130.2024.2020 (data dostępu: 18.03.2021). Decyzją tą nałożono na KSSIP karę administracyjną 100 000 zł m.in. za niezastosowanie odpowiednich środków technicznych i organizacyjnych, mających zapewnić zdolność do ciągłego zapewnienia poufności usług przetwarzania, brak przetestowania i oceny skuteczności środków technicznych i organizacyjnych, mających na celu zapewnienie bezpieczeństwa danych osobowych znajdujących się w kopii bazy danych platformy szkoleniowej KSSIP, a tym samym niewłaściwe uwzględnienie ryzyka związanego ze zmianami w procesie przetwarzania.

Kluczowym przepisem kryminalizującym naruszenia RODO jest art. 107 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[6], który w typie podstawowym przewiduje odpowiedzialność osoby, która przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest ona uprawniona (art. 107 ust. 1 UODO). Przestępstwo to jest zagrożone karą grzywny, ograniczenia wolności lub pozbawienia wolności do lat dwóch. Typ kwalifikowany (art. 107 ust. 2 UODO), zagrożony karą grzywny, ograniczenia wolności lub pozbawienia wolności do lat trzech przy tożsamej czynności sprawczej dotyczy danych osobowych wrażliwych (sensytywnych) – 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. Art. 108 UODO chroni natomiast samo postępowanie kontrolne zmierzające do ustalenia przestrzegania przepisów o ochronie danych osobowych, penalizując udaremnianie lub utrudnianie przeprowadzenia kontroli kontrolującemu oraz niedostarczanie niezbędnych danych pozwalających na ustalenie podstaw i wysokości karny administracyjnej. Bliźniaczy przepis do art. 107 UODO został zamieszczony w ustawie z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[7], która w art. 54 przewiduje odpowiedzialność karną za tożsame czynności sprawcze, których przedmiotem są dane osobowe, o których mowa w przepisach o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Desygnaty pojęciowe terminu *dane osobowe* są tożsame, niezależnie od podstaw legalnego przetwarzania tych danych ujętych w RODO lub wskazanych w dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW[8]. Wprowadzenie odrębnego typu przestępstwa nielegalnego przetwarzania danych osobowych na potrzeby w związku z zapobieganiem i zwalczaniem przestępczości, przy identycznym zagrożeniu karami pozbawienia wolności, w typie podstawowym do dwóch lat, w typie kwalifikowanymi z uwagi na dane wrażliwe do trzech lat, nie znajduje uzasadnienia.

[6] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz.U. z 2019 r., poz. 1781), dalej jako UODO.

[7] Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r., poz. 125).

[8] Dz.U. UE L 119 z 4 maja 2016 r., s. 89 ze zm. W odniesieniu do przywołanej dyrektywy powszechnie używa się skrótu DODO.

Blankietowy charakter przepisu typizującego przestępstwo nielegalnego przetwarzania danych osobowych

Odczytanie znamion charakteryzujących zakres bezprawności i karalności zachowań określonych w art. 107 OUDO niewątpliwie utrudnione jest blankietowością tego przepisu[9]. Zawarty w nim opis karalnych zachowań ma charakter generalny i niezupełny, prawidłowa rekonstrukcja znamion wymaga odwołania się w pierwszej kolejności nawet nie do przepisów UODO, która to ustawa ma charakter niesamodzielny i wykonawczy, a do stosowanych bezpośrednio przepisów RODO[10]. Od wykładni przepisów RODO, prawidłowego odkodowania norm w nim zawartych zależy zatem odczytanie zakresu kryminalizacji, a w praktyce możliwość pociągnięcia do odpowiedzialności karnej sprawy naruszenia ochrony danych osobowych. Ta funkcjonalna zależność od przepisów regulacyjnych powoduje, że przepis art. 107 UODO nie określa autonomicznie i w sposób zupełny płaszczyzny bezprawności postępowania oraz znamion typu czynu. Może to nasuwać wątpliwości co do zgodności przyjętej konstrukcji przepisu z postulatem jasnej typizacji[11].

Blankietowy charakter przepisu prowadzi do błędnych rozstrzygnięć co do biegu postępowań karnych, sprzyja oportunizmowi organów ochrony prawnej[12]. Przykładem może być postanowienie z 29 lipca 2020 r. w sprawie Prokuratury Okręgowej w Warszawie o sygn. PO I DS. 147/2020 o odmowie wszczęcia postępowania[13], gdzie w uzasadnieniu zawarto tezę, iż przetwarzanie danych osobowych poza pierwotnym celem przez administratora danych, któ-

[9] Wskazany sposób typizacji przy zastosowaniu przepisów blankietowych charakterystyczny jest dla pozakodeksowego prawa karnego. Zob. J. Skorupka, [w:] M. Bojarski (red.), *Szczególne dziedziny prawa karnego. Prawo karne wojskowe, skarbowe i pozakodeksowe*, seria: *System prawa karnego*, t. 11, Warszawa 2014, s. 535, 536.

[10] Por. P. Barta, [w:] P. Litwiński (red.), *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, s. 309.

[11] „Reguła określoności wskazana w art. 42 Konstytucji RP wyznacza dopuszczalność i zakres stosowania norm prawa karnego o charakterze blankietowym; nakazuje ona ustawodawcy takie wskazanie czynu zabronionego (jego znamion), aby nie budziło wątpliwości zarówno adresata normy prawnokarnej, jak i organów stosujących prawo i dokonujących »odkodowania« treści regulacji w drodze wykładni normy prawa karnego to, czy określone zachowanie in concreto wypełnia te znamiona; »zakaz« powinien być zawsze dokładnie i w sposób niebudzący wątpliwości oznaczony w ustawie karnej" – wyrok Trybunału Konstytucyjnego z 13 maja 2008 r., sygn. akt P 50/07, OTK ZU Nr 4/A/2008, poz. 58.

[12] Występowanie oportunizmu organów ochrony prawnej potwierdzali twórcy projektu ustawy o ochronie danych osobowych, wskazując, że „wprowadzone do projektu regulacje nie są (…) kopią obecnych rozwiązań. 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" – uzasadnienie projektu ustawy o ochronie danych osobowych, druk sejmowy Sejmu VIII kadencji nr 2410, s. 46.

[13] Postanowienie niepublikowane, w zbiorach własnych autora.

ry bez jakiegokolwiek uprawnienia przewidzianego w przepisach prawa udostępnia osobie trzeciej dane osobowe np. swojego pracownika, nie wyczerpuje znamion występku z art. 107 § 1 UODO, o ile udostępnienie to służy dochodzeniu roszczeń na drodze cywilnej. Prokurator wyszedł z błędnego założenia, że skoro strona postępowania ma prawo, a nawet obowiązek wskazania adresu przeciwnej strony w procesie cywilnym, to sposób pozyskania tego adresu jest prawnie irrelewantny, nie wyczerpuje znamion przestępstwa. Otóż, ten sposób rozumowania wyklucza możliwość pociągnięcia do odpowiedzialności karnej za przestępstwa m.in. uzyskania dostępu do informacji bez uprawnienia (tzw. kradzież danych) – art. 267 § 1 k.k., ujawnienia informacji uzyskanych bezprawnie – art. 267 § 4 k.k. czy właśnie przetwarzania informacji przez jej udostępnienie bez uprawnienia art. 107 UODO, jeżeli ta informacja ma być wykorzystana na potrzeby procesu cywilnego. Przy przyjęciu tego swoistego kontratypu „wyższej potrzeby procesu cywilnego" dowolny pracodawca mógłby przekazywać dane swojego pracownika bez uprawnienia do przetwarzania w tym zakresie, nie ponosząc odpowiedzialności karnej. Podobnie dane mogłyby być swobodnie udostępniane przez innych administratorów – usługodawców, sklepy, a także instytucje i urzędy pod pretekstem procesu cywilnego.

Odczytanie zakresu kryminalizacji

Przytoczony przykład wskazuje, że odtworzenie zakresu kryminalizacji naruszeń RODO wymaga:

1. zakwalifikowania danego zachowania jako mieszczącego się w pojęciu naruszenia ochrony danych osobowych – stwierdzenia nielegalności działania lub zaniechania na gruncie przepisów RODO,
2. stwierdzenia, że ustalone naruszenie ochrony danych osobowych jednocześnie wyczerpuje znamiona strony przedmiotowej występku z art. 107 UODO i zachodzą okoliczności modalne czynu,
3. wykonania testu podwójnej karalności, czy naruszenie ochrony danych osobowych wyczerpujące znamiona występku z art. 107 UODO nie podlega karze administracyjnej, co zgodnie z zasadą *ne bis in idem* wyłączałoby dodatkową możliwość karania za przestępstwo, z uwagi na pierwszeństwo represji przewidzianej w prawie administracyjnym (zbieg z sankcją administracyjną).

Dopiero przejście powyższych etapów analizy pozwala na określenie zakresu kryminalizacji naruszenia przepisów RODO, a w odniesieniu do konkretnych czynów daje podstawę do analizy wyczerpania przez sprawcę znamion podmiotowych występku, jak również do ustalenia ewentualnej sytuacji rzeczywistego i pozornego zbiegu art. 107 UODO z przepisami typizującymi przestępstwa przeciwko ochronie informacji, w tym przestępstwo bezprawnego

uzyskania informacji (art. 267 §§ 1–3 k.k.), przestępstwa gospodarcze z rozdziału XXXVI Kodeksu karnego czy z ogólnych przestępstwem urzędniczym (art. 231 k.k.).

Istotą blankietowej konstrukcji przepisu art. 107 UODO jest to, że rekonstrukcja normy sankcjonowanej wymaga odwołania do przepisów pełniących funkcję regulacyjną zawartych w RODO. W oparciu o przepisy rozporządzenia odczytaniu podlegają desygnaty pojęciowe terminu *przetwarza*. Zgodnie z art. 4 pkt 2 RODO przetwarzanie oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie. Wyliczenie nie ma charakteru enumeratywnego, tym samym przetwarzanie będzie oznaczać jakąkolwiek operację na danych osobowych, przy czym wyczerpanie znamienia czasownikowego nastąpi już przy jednorazowej czynności przetwarzania, np. w sytuacji udostępnienia jednego rekordu. W odróżnieniu zatem od niektórych typów przestępstw o wieloczynowo określonych znamionach czasownikowych, dokonanie przestępstwa nie jest zależne od powtarzalności działań – od dokonania zestawu operacji przetwarzania.

Odtworzenie ekstensji terminu *przetwarza* nie prowadzi tym samym do wyraźnego zakreślenia pola kryminalizacji. Podobnie oznaczenie osób, które mogą dokonać przestępstwa z art. 107 UODO, nie pozwala na wyodrębnienie czynów zabronionych według kryterium podmiotowego. Nie budzi w doktrynie wątpliwości powszechny charakter przestępstwa[14], czynu mogą zatem dokonać zarówno osoby, które profesjonalnie przetwarzają dane osobowe jako administratorzy (art. 4 pkt 7 RODO), podmioty przetwarzające (art. 4 pkt 8 RODO), jak też jako osoby fizyczne, które nie mają żadnych uprawnień do przetwarzania danych w rozumieniu RODO, a które nie przetwarzają danych osobowych wyłącznie w ramach czynności o czysto osobistym lub domowym charakterze (wyłączenie z art. 2 ust. 2 lit. c RODO). Przetwarzanie danych osobowych, które stały się przedmiotem przestępstwa (np. nielegalnego upublicznienia przez osoby fizyczne w celach kolekcjonerskich, samo ich przechowanie na nośnikach w domu), nie będzie zatem wyczerpywało znamion przestępstwa, z uwagi na wskazaną przesłankę legalności przetwarzania.

[14] Por. P. Barta, [w:] P. Litwiński (red.), op. cit., s. 310.

Naruszenie ochrony danych osobowych

Przepis blankietowy nie pełni co do zasady funkcji regulacyjnej, a jedynie funkcję ochronną, wzmacniając skuteczność przepisów regulacyjnych, do których odsyła[15]. Punktem wyjścia analizy zakresu kryminalizacji jest zatem naruszenie przepisów RODO, określane jako naruszenie ochrony danych osobowych. Termin ten definiowany na gruncie prawa o ochronie danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych (art. 4 pkt 12 RODO). Pojęcie naruszenia ochrony danych osobowych jest zatem węższe od naruszenia rozporządzenia (RODO), które obejmuje wszelkie uchybienia przepisom regulującym przetwarzanie i ochronę danych osobowych. Jedynie naruszenia poważne godzące bezpośrednio w bezpieczeństwo danych, prowadzące do wymienionych wyżej skutków, podlegają rejestracji jako incydenty bezpieczeństwa danych w trybie art. 33 ust. 5 RODO. Administrator danych zobowiązany jest dokumentować wszelkie naruszenia ochrony danych osobowych, ich okoliczności, skutki oraz podjęte działania zaradcze. Zgłoszeniu organowi nadzoru nie podlega każde przekroczenie przepisów RODO, wyłącznie naruszenie ochrony danych osobowych, chyba że jest mało prawdopodobne, by tego rodzaju incydent bezpieczeństwa skutkował ryzykiem naruszenia praw lub wolności osób fizycznych (art. 33 ust. 1 RODO). W odniesieniu do takiego poważnego incydentu bezpieczeństwa, o ryzyku naruszenia praw lub wolności w stopniu wysokim administrator zobowiązany jest także zawiadomić o naruszeniu ochrony danych osobowych osobę, której dane osobowe dotyczą (art. 34 ust. 1 RODO).

Naruszenia rozporządzenia, w tym naruszenia ochrony danych osobowych, stanowią przesłankę odpowiedzialności administracyjnej, określonej w art. 58 ust. 2 RODO (uprawnienia naprawcze organu nadzoru) i art. 83 RODO (administracyjne kary pieniężne), a także cywilnej art. 82 RODO (odszkodowanie za poniesioną szkodę majątkową lub niemajątkową). Trybunał Konstytucyjny w wyroku z 9 października 2001 roku, w sprawie o sygn. SK 8/2000 stwierdził: „Wolność ustawodawcy (…) nie ma charakteru absolutnego. Spoczywający na nim obowiązek dostatecznej ochrony wartości konstytucyjnych obliguje go do ustanowienia odpowiednich uregulowań, a ponadto – takich środków ochrony, które stworzą wystarczające gwarancje ich przestrzegania i egzekwowania. Gwarancje te zaś mogą mieć rozmaity charakter – cywilny, administracyjny, w ostateczności zaś również i karny (…) prawo karne w zwalczaniu zachowań społecznie niepożądanych musi stanowić *ultima ratio*. Oznacza to, że sięganie

[15] Ibidem – patrz przypis 9.

do instrumentów prawnokarnych uzasadnione jest wtedy tylko, gdy pożądanego celu nie można osiągnąć w żaden inny sposób. Z punktu widzenia uregulowań zawartych w Konstytucji ustanowiona ochrona musi być proporcjonalna, adekwatna do wagi chronionych praw i wolności”[16]. Ochrona praw i wolności może być zatem w pierwszej kolejności zapewniona na gruncie prawa administracyjnego czy też cywilnego. Kryminalizacja nie zakreśla także granic patologii, przeciwnie – to granice patologii zakreślają dopuszczalne w państwie prawa granice kryminalizacji.

Odpowiedzialność karna co do zasady zatem dotyczy patologii przetwarzania danych osobowych, tj. naruszeń RODO na tyle poważnych i powszechnych, że sankcje administracyjne (od uprawnień naprawczych organu nadzoru do kar pieniężnych włącznie), sankcje na gruncie prawa cywilnego nie są wystarczające lub niemożliwe do zastosowania wobec osób odpowiedzialnych za przekroczenie przepisów. Ogranicza to represję karną właśnie do najpoważniejszych naruszeń ochrony danych osobowych. Jeżeli naruszenie RODO nie jest na tyle poważne, że nie narusza bezpieczeństwa danych osobowych, nie skutkuje wysokim ryzykiem naruszenia praw i wolności człowieka, którego dane dotyczą, nie wymaga nawet zgłoszenia jako incydentu bezpieczeństwa, tym bardziej nie może stanowić czynu podlegającego kryminalizacji. Teza ta znajduje potwierdzenie w motywie 148 RODO, który wskazuje na pierwszeństwo represji administracyjnej, stwierdzając, że aby egzekwowanie przepisów niniejszego rozporządzenia było skuteczniejsze, należy za jego naruszenie nakładać sankcje, w tym administracyjne kary pieniężne – oprócz lub zamiast odpowiednich środków nakładanych na mocy niniejszego rozporządzenia przez organ nadzorczy. Jeżeli naruszenie jest niewielkie lub jeżeli grożąca kara pieniężna stanowiłaby dla osoby fizycznej nieproporcjonalne obciążenie, można zamiast tego udzielić upomnienia. Dopiero w motywie 149 RODO i w art. 84 RODO przewiduje, że państwa członkowskie powinny mieć możliwość ustanowienia sankcji karnych za naruszenie RODO, w tym za naruszenie krajowych przepisów przyjętych na jego mocy i w jego granicach, szczególnie za naruszenia niepodlegające administracyjnym karom pieniężnym, sankcji proporcjonalnych, odstraszających i skutecznych. Prawodawca zastosował zatem stopniowanie zakresu odpowiedzialności za naruszenie przepisów RODO – od środków naprawczych, przez upomnienie, administracyjne kary pieniężne, aż po sankcje karne. Naruszenia drobne wymagające co najwyżej środków naprawczych, upomnienia, jak również administracyjnych kar pieniężnych nie podlegają kryminalizacji.

Także porównanie zakresu kryminalizacji art. 107 i 108 UODO z przepisami karnymi poprzednio obowiązującej ustawy z dnia 29 sierpnia 1997 r.

---

[16] Wyrok Trybunału Konstytucyjnego z 9 października 2001 r., sygn. akt SK 8/2000, OTK ZU 2001/7, poz. 211.

o ochronie danych osobowych[17] wskazuje, że ustawodawca ograniczył się do penalizacji najpoważniejszych naruszeń RODO. Kryminalizacji nie podlega już samo przechowywanie danych osobowych niezgodnie z pierwotnym celem (złamanie zasad retencji danych), naruszenie nieumyślne obowiązku zabezpieczenia danych osobowych przed ich zabraniem przez osobę nieuprawnioną, niezgłoszenie do rejestru zbioru danych, niedopełnienie obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z przysługujących jej praw. Z zakresu czynów zabronionych jako przestępstwa godzących w zasady przetwarzania danych osobowych pozostały przestępstwa nielegalnego przetwarzania danych osobowych i utrudniania kontroli organowi nadzoru.

Powyższa analiza prowadzi do konkluzji, że zakres kryminalizacji art. 107 UODO ograniczony jest do najpoważniejszych naruszeń ochrony danych osobowych w rozumieniu art. 4 pkt 12 RODO i art. 33 ust. 1 RODO. Dany czyn wyczerpuje znamiona przestępstwa nielegalnego przetwarzania danych, o ile stanowi jednocześnie naruszenie ochrony danych osobowych. Działanie lub zaniechanie, które nie pociąga za sobą zagrożenia bezpieczeństwa danych, nie będzie tym samym stanowić nielegalnego przetwarzania danych. Nie jest wystarczające naruszenie podstaw przetwarzania danych przewidzianych w art. 6 ust. 1 RODO, jeżeli to nie zagraża bezpieczeństwu danych, a w konsekwencji nie pociąga za sobą ryzyka naruszenia praw i wolności osoby, której dany dotyczą. Z kręgu kryminalizacji wyłączone są tym samym zachowania nielegalnego przetwarzania, takie jak wyjście poza pierwotny cel przetwarzania danych bez dopełnienia wymogów przewidzianych w art. 13 ust 3 RODO i art. 14 ust. 4 RODO, naruszenie zasad retencji danych – przechowywanie wykraczające poza dopuszczalny prawem okres, szerzej zasady ograniczenia celu (art. 5 ust. 1lit. b RODO), naruszenie zasady minimalizacji danych, tj. samoograniczenia się administratora do danych niezbędnych stosownie do legalnego celu (art. 5 ust. 1 lit. c RODO). Także samo przetwarzanie bez uprawnienia w wyniku braku instrumentu powierzenia lub braku udokumentowanego polecenia administratora przez podmiot przetwarzający (procesor) lub dalszy podmiot przetwarzający (subprocesor) nie będzie wyczerpywało znamion występku, jeżeli podmioty te zapewniają zachowanie odpowiednich gwarancji, by przetwarzanie odpowiadało wymogom RODO. Podobnie nie jest kryminalizowane uchybienie innym obowiązkom administratora, takim jak przywołane wyżej obowiązki zgłoszenia incydentu bezpieczeństwa danych, prowadzenia rejestru naruszeń ochrony danych osobowych, powiadomienia osoby, której dane dotyczą o stwierdzonym wycieku danych. Przykładowo: nielegalne skopiowanie bazy danych osobowych kontrahentów, będących przedsiębiorcami, przez pracownika nie wejdzie w zakres kryminalizacji art. 107 UODO, nie ma

[17] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst pierwotny Dz.U. z 1997 r., Nr 133, poz. 883).

bowiem naruszenia bezpieczeństwa tych danych, podlegają one upublicznieniu w powszechnie dostępnej bazie Centralnej Ewidencji i Informacji o Działalności Gospodarczej[18]. Nadto zachodzi tu oczywisty brak ryzyka naruszenia praw i wolności osób, których dane dotyczą, na skutek oczywiście niezgodnego z RODO przetwarzania danych. Świadome i celowe wyniesienie danych osobowych przez pracownika na nośniku danych wbrew zakazowi administratora, by ułatwić sobie pracę zdalną w warunkach domowych, jeżeli nie prowadzi do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych, nie narusza tym samym bezpieczeństwa danych, nie stanowi istotnego incydentu bezpieczeństwa, a tym samym nie mieści się w zakresie kryminalizacji. Ujawnienie danych osobowych pracownika, w tym danych adresowych przez administratora – pracodawcę osobie trzeciej bez podstawy prawnej, a tym bardziej przez przypadkowego pracownika, który uzyskał poza swoimi uprawnieniami pracowniczymi dostęp do bazy danych osobowych, będzie stanowiło naruszenie ochrony danych osobowych. Ujawnienie takie mieści się zatem w zakresie kryminalizacji jako przetwarzanie, które nie jest prawnie dopuszczalne.

Odwołanie się do konstrukcji prawnej naruszenia ochrony danych osobowych w celu ustalenia normy sankcjonowanej prowadzi do wniosku, wbrew spotykanemu w doktrynie stanowisku, że przestępstwo art. 107 UODO jest przestępstwem formalnym[19], iż występek ten jest w rzeczywistości przestępstwem skutkowym. Występek nielegalnego przetwarzania danych osobowych stanowi przestępstwo konkretnego narażenia na niebezpieczeństwo[20] chronionego prawem dobra, którym są dane osobowe. Bez wystąpienia skutku w postaci narażenia, jak było to wcześniej analizowane, nie dochodzi do naruszenia ochrony danych osobowych na tyle istotnego, by podlegało ono zgłoszeniu jako incydent bezpieczeństwa, a tym samym by mogło być kwalifikowane jako przestępstwo. Nie jest wystarczające abstrakcyjne zagrożenie chronionego dobra, które nie prowadzi do wysokiego ryzyka naruszenia praw i wolności osób, których dane dotyczą.

---

[18] Oczywiście baza danych kontrahentów będzie chroniona jako tajemnica przedsiębiorstwa, jej naruszenie może skutkować pociągnięciem do odpowiedzialności karnej na podstawie art. 23 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j. Dz.U. z 2020 r., poz. 1913). Odmienny jest przedmiot ochrony wymienionego przepisu w porównaniu do art. 107 UODO. Przywołany przepis chroni tajemnicę przedsiębiorstwa, a tym samym prawnie uzasadniony interes przedsiębiorcy, zaś art. 107 UODO chroni dobra osobiste osób, których dane osobowe dotyczą.

[19] Por. P. Barta, [w:] P. Litwiński (red.), op. cit., s. 309–310.

[20] W zakresie rozumienia przestępstw skutkowych – konkretnego narażenia na niebezpieczeństwo patrz P. Nowak, *O skutkowości przestępstw formalnych*, „Zeszyty Prawnicze" 2014, t. 14, nr 1, passim.

Okoliczności modalne czynu

Stwierdzenie, że określone przetwarzanie danych stanowi naruszenie ochrony danych osobowych, skutkujące ryzykiem naruszenia praw i wolności, nie pozwala jeszcze na przyjęcie, iż działanie lub zaniechanie mieści się w zakresie kryminalizacji występku art. 107 UODO i na przejście do analizy znamion strony podmiotowej. Konieczna jest analiza okoliczności modalnych czynu – ustalenie, że ujawnione naruszenie ochrony danych osobowych jednocześnie mieści się w znamionach strony przedmiotowej z art. 107 UODO. Zachowania muszą zatem odpowiadać desygnatom pojęciowym terminów „przetwarzanie nie jest dopuszczalne" i „do których przetwarzania nie jest uprawniony".

Egzegeza tych terminów rodzi pewne trudności. Nie ma bowiem na gruncie przepisów RODO kategorii danych osobowych, których przetwarzanie zostało całkowicie wyłączone – nie jest dopuszczalne. Wszystkie dane osobowe można przetwarzać z poszanowaniem przepisów RODO, także dane sensytywne, dane o karalności. Niedopuszczalne jest zaś przetwarzanie danych, do których dany podmiot nie uzyskał uprawnienia do ich przetwarzania. Konieczne jest jednakże rozdzielenie zakresów pojęciowych terminów *przetwarzania danych niedopuszczalnego* i *przetwarzania bez uprawnienia*, którymi posłużył się ustawodawca. Przeciwne podejście stanowiłoby naruszenie zakazu wykładni synonimicznej i zakazu wykładni *per non est*[21]. Niedopuszczalne przetwarzanie danych osobowych należy tym samym wykładać jako działanie przez podmiot co do zasady uprawniony do określonych danych, będący ich legalnym administratorem lub podmiotem przetwarzającym, pracownikiem administratora lub podmiotu przetwarzającego, jednakże stanowiące operację przetwarzania, która wykracza poza formę i cel przetwarzania, określone granicami uprawnienia. Przykładem może być działanie administratora na etapie przetwarzania w ramach pierwotnego celu ograniczonego już tylko do celów archiwalnych, naukowych lub statystycznych (motyw 50 RODO i art. 89 RODO), który – wychodząc poza wskazany cel i formę przetwarzania – upublicznia dane osobowe. Oczywiście należy odróżniać przetwarzanie niedopuszczalne od przetwarzania dopuszczalnego po spełnieniu warunków RODO, np. po dokonania zawiadomienia o zamiarze zmiany sposobu przetwarzania w trybie art. 13 ust. 3 RODO i art. 14 ust. 4 RODO, po uzyskaniu polecenie od administratora przez podmiot przetwarzający. Należy w tym celu każdorazowo przeprowadzić test, czy w odniesieniu do określonych kategorii danych osobowych osoba dokonująca operacji przetwarzania mogłaby uzyskać takie upraw-

[21] Por. L. Morawski, *Zasady wykładni prawa*, Toruń 2006, s. 103–104, 106–107; R.A. Stefański, [w:] T. Bojarski (red.), *Źródła prawa karnego*, seria: *System prawa karnego*, t. 2, Warszawa 2011, s. 499–500.

nienie w zakresie celu i formy przetwarzania, jedynie ograniczając się do wypełnienia formalnych wymogów RODO.

Drugi termin, *przetwarzanie bez uprawnienia*, oznacza tym samym operację na danych osobowych, do których żadnych uprawnień sprawca nie posiada. Istotą czynności sprawczej jest w tej sytuacji nielegalne wejście w posiadanie informacji zawierających dane osobowe już stanowiące operację przetwarzania w rozumieniu art. 4 pkt 2 RODO. Oczywiście sprawca jednym działaniem może jednocześnie wyczerpywać znamiona niedopuszczalnego przetwarzania danych osobowych, jak i przetwarzania danych bez uprawnienia, jeżeli przedmiotem czynności sprawczej są zarówno legalnie posiadane przez niego do innych celów lub form przetwarzania i dane pozyskane nielegalnie.

Wzorzec kontroli legalności operacji przetwarzania danych osobowych podlega odtworzeniu w pierwszej kolejności w oparciu o przepisy RODO. Nielegalność przetwarzania danych rozumiana jako niedopuszczalność przedmiotowa lub brak uprawnienia podmiotowego wynika z braku umocowania podmiotu do przetwarzania w oparciu o warunki wymienione w art. 6 RODO [Zgodność przetwarzania z prawem] lub w granicach wyznaczonych przez art. 5 RODO [Zasady dotyczące przetwarzania danych osobowych]. W odniesieniu jednakże do kategorii podmiotów, w stosunku do których wyłączono przez ustawodawcę możliwość stosowania art. 5 RODO i art. 6 RODO, np. w stosunku do dziennikarzy, wzorzec kontroli musi opierać się głównie na przepisach krajowych, stanowiących o granicach legalności przetwarzania danych. Wyłączenie stosowania określonej grupy przepisów RODO nie wyłącza bowiem upoważnienia ustawodawcy do przyjęcia sankcji karnych (art. 84 ust. 1 RODO), a tym samym nie czyni przestępstwa z art. 107 UODO indywidualnym.

Pozostając przy przykładzie działalności polegającej na redagowaniu, przygotowywaniu, tworzeniu lub publikowaniu materiałów prasowych, w odniesieniu do której ustawodawca w art. 2 ust. UODO wyłączył stosowanie wskazanych przepisów RODO, legalność przetwarzania musi wynikać z przepisów ustawy z dnia 26 stycznia 1984 r. – Prawo prasowe[22] i z tej części przepisów RODO, która nie podlegała wyłączeniu. Ograniczeniu przetwarzania przez dziennikarza będą podlegały dane osobowe z art. 10 RODO, tj. dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa. Przetwarzanie w działalności prasowej danych osobowych polegające na upublicznieniu informacji o skazaniu osoby i jej danych indentyfikacyjnych – imienia i nazwiska, wizerunku bez zgody osoby, której dane osobowe dotyczą lub zgody sądu jako naruszające wskazany przepis art. 10 RODO i art. 13 ust. 2 Prawa prasowego, będzie nielegalne. Publikacja w tej sytuacji może być kwalifikowana jako opisane w art. 107 UODO przetwarzanie danych osobowych, choć ich przetwarzanie nie jest dopuszczalne.

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

Zbieg z sankcją administracyjną

Pierwszeństwo represji administracyjnej wynikające z motywu 148 RODO, zakładającego orzekanie sankcji administracyjnych, w tym kar pieniężnych jako preferowanego sposobu zabezpieczenia egzekwowania przepisów RODO, w praktyce może skutkować częstymi sytuacjami zbiegu spraw karnych z art. 107 UODO z postępowaniami prowadzonymi przez organy nadzoru. W motywie 149 RODO wprost wskazano, że nałożenie sankcji karnych za naruszenie RODO nie może prowadzić do naruszenia zasady *ne bis in idem*, zgodnie z wykładnią Trybunału Sprawiedliwości. Możliwość nałożenia administracyjnych kar pieniężnych za określone rodzaje operacji przetwarzania danych osobowych zdaje się zatem wykluczać zaliczenie naruszenia ochrony danych osobowych do katalogu czynów mieszczących się w zakresie kryminalizacji art. 107 UODO.

Administracyjne kary pieniężne nakładane są na administratorów, podmioty przetwarzające, którymi mogą być osoby prawne, organy administracji publicznej, ale którymi mogą być również osoby fizyczne – przedsiębiorcy. Osoba fizyczna nie może jednocześnie podlegać odpowiedzialności w postaci pieniężnej kary administracyjnej i karze grzywny czy surowszym karom przewidzianym za występek za tożsamy czyn. Nie jest dopuszczalna również interpretacja sytuacyjna, w której w przypadku naruszenia ochrony danych osobowych dokonanego w ramach operacji przetwarzania przez podmiot niebędący osobą fizyczną, względem tego podmiotu będzie stosowana sankcja administracyjna, wobec pracownika podmiotu zaś sankcja karna, w tożsamej zaś sytuacji dotyczącej przetwarzania przez podmiot – osobę fizyczną, ta będzie odpowiadać wyłącznie administracyjnie. Za występek z art. 107 UODO, jak dowodzi tego przeprowadzona analiza, nie odpowiada wyłącznie osoba, która nie jest uprawniona do przetwarzania danych osobowych – przestępstwo to ma charakter powszechny.

Zaliczenie przepisów prawa administracyjno-karnego do prawa karnego, nawet w znaczeniu najszerszym (*sensu largissimo*), jest sporne w doktrynie prawa karnego[23]. Bezpośrednie odwołanie się do zasady *ne bis in idem* w motywie 149 RODO, jak również orzecznictwo Trybunału Konstytucyjnego[24] i Trybunału Sprawiedliwości[25], które jako naruszenie zakazu wielokrotnego karania za ten sam czyn traktuje orzekanie sankcji administracyjno-karnych

---

[23] „Do prawa karnego (nawet *sensu largissimo*) nie można zaliczyć przepisów ustaw administracyjnych, przewidujących różnego typu sankcje finansowe, noszące najczęściej nazwę »kary pieniężne« nakładane na podmioty gospodarcze" – A. Marek, *Kodeks karny. Komentarz*, Warszawa 2007, s. 118.

[24] Wyrok Trybunału Konstytucyjnego z 18 listopada 2010 r., sygn. akt P. 29/2009, OTK ZU 2010/9A, poz. 104.

[25] „Zasada *ne bis in idem* (…) nie stoi na przeszkodzie stosowaniu przez państwo członkowskie kolejno sankcji podatkowej i sankcji karnej za ten sam czyn (…), pod warunkiem, że pierwsza z tych sankcji nie ma charakteru karnego" – wyrok Trybunału Sprawiedliwości Unii Europejskiej

i kar za przestępstwa stanowiące jednocześnie delikt administracyjny, przesądza o konieczności rozróżnienia naruszeń RODO stanowiących przesłankę wyłącznie wymierzenia administracyjnej kary pieniężnej od naruszeń ochrony danych osobowych mieszczących się w zakresie kryminalizacji art. 107 UODO. Także zastosowanie kryteriów engelowych, od nazwy sprawy Engel przeciwko Holandii[26], inaczej kryteriów aspektu karnego[27], w tym głównie uzależnienie nałożenia kary administracyjnej od stwierdzenia winy (art. 83 ust. 2 lit a, b, d, k RODO i motyw 148 RODO), warunku maksymalnej potencjalnej kary – nawet 20 000 000 euro, przemawia za koniecznością wyodrębnienia pola kryminalizacji występku.

Przyjęcie interpretacji, że kryminalizacja przewidziana przez przepis karny pokrywa się z zakresem naruszenia RODO sankcjonowanym administracyjnie, pociągałoby za sobą całkowitą zbędność regulacji karnomaterialnej i brak wykonania dyspozycji art. 84 ust. 1 RODO lub rezygnację z powszechnego charakteru występku nielegalnego przetwarzania danych osobowych, wbrew literalnej treści przepisu. Prawidłowe odczytanie normy sankcjonowanej, do której odsyła blankietowy w swojej istocie przepis art. 107 UODO, zakłada zatem wyłączenie przedmiotowe z zakresu tej normy zachowań sankcjonowanych przez art. 83 RODO, stanowiący ogólne warunki nakładania administracyjnych kar pieniężnych. Wyłączenie to będzie prowadziło także do umorzenia postępowania karnego za czyn sankcjonowany administracyjnie, nie z racji zaistnienia przesłanki powagi rzeczy osądzonej lub zawisłości sporu (art. 17 § 1 pkt 7 k.p.k.), a na podstawie przesłanki materialnej braku znamion przestępstwa (art. 17 § 1 pkt 2 k.p.k.). Czyni to bezprzedmiotowym spór o charakter przepisów karno-administracyjnych. Oczywiście wieloaspektowe operacje przetwarzania – w rozumieniu zespołów czynności i zaniechań wypełnienia obowiązków nakładanych przez RODO – mogą stanowić przesłanki pociągnięcia do odpowiedzialności administracyjnej obok odpowiedzialności karnej, jednakże za odrębne czyny.

Odrębność pola kryminalizacji art. 107 UODO od zachowań podlegających sankcji administracyjnej rozwiązuje również problem wynikający z zasady *one-stop-shop*[28] przy transgranicznym naruszeniu ochrony danych osobowych. Możliwość pociągnięcia sprawcy naruszenia do odpowiedzialności karnej nie będzie zależna od decyzji administracyjnej wiodącego organu nadzoru i od

---

z 26 lutego 2013 r. w sprawie C-617/10 Åklagaren przeciwko Hansowi Åkerbergowi Franssonowi, pkt 35, https://www.eur-lex.europa.eu (data dostępu: 1.03.2021).

[26] Engel i inni przeciwko Holandii, wyrok Europejskiego Trybunału Praw Człowieka z 8 czerwca 1976 r., seria A, nr 22.

[27] Patrz: Rada Europy/Europejski Trybunał Praw Człowieka*, Praktyczny przewodnik w sprawie kryteriów dopuszczalności*, 2014, s. 63–64, https://www.echr.coe.int (data dostępu: 1.03.2021).

[28] Patrz M. Gawroński, [w:] M. Gawroński (red.), *Ochrona danych osobowych. Przewodnik po ustawie i RODO z wzorami*, Warszawa 2018, s. 187.

spełnionego warunku podwójnej karalności[29]. Występek będzie popełniony w Polsce – w miejscu działania sprawcy, niezależnie od deliktu administracyjnego ściganego przez organ nadzoru innego europejskiego kraju.

Uprawnienia naprawcze

Wykładnia terminów składających się na nielegalne przetwarzanie danych osobowych w rozumieniu art. 107 UODO nie pozwala na wyodrębnienie pola kryminalizacji z zakresu zachowań sankcjonowanych administracyjnie. Konieczne jest zatem odwołanie się do konstrukcji uprawnień naprawczych (środków) określonych w art. 58 ust. 2 lit. a–h oraz j RODO. Karę administracyjną nakłada się bowiem na podstawie art. 83 ust. 2 RODO oprócz lub zamiast wymienionych środków. Zaistnienie przesłanek skorzystania przez organ nadzoru z uprawnień naprawczych względem danej osoby lub podmiotu, za którą osoba ta działa, jako pozwalające na wymierzenie administracyjnej kary pieniężnej, będzie wykluczało jednoczesne pociągnięcie do odpowiedzialności karnej tej osoby za występek nielegalnego przetwarzania danych osobowych.

Administracyjną karę pieniężną na podstawie art. 82 ust. 2 RODO można zatem orzec wobec administratora lub podmiotu przetwarzającego za naruszenie przepisów RODO w sytuacji kwalifikującej się do:

1. wydania ostrzeżenia dotyczącego możliwości naruszenia przepisów RODO przez planowane operacje przetwarzania (art. 58 ust. 2 lit. a RODO),
2. udzielenia upomnienia w przypadku naruszenia przepisów RODO przez operację przetwarzania (art. 58 ust. 2 lit. b RODO),
3. nakazania spełnienia żądania osoby, której dane dotyczą, wynikającego z praw przysługujących (art. 58 ust. 2 lit. c RODO),
4. nakazania dostosowania operacji przetwarzania do przepisów RODO wraz ze wskazaniem w stosownych przypadkach sposobu i terminu (art. 58 ust. 2 lit. d RODO),
5. nakazania administratorowi zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych (art. 58 ust. 2 lit. e RODO),
6. wprowadzenia czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania (art. 58 ust. 2 lit. f RODO),
7. nakazanie na mocy art. 16, 17 i 18 RODO sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania oraz nakazanie na mocy art. 17 ust. 2 i art. 19 RODO powiadomienia o tych czynnościach odbiorców, którym dane osobowe ujawniono (art. 58 ust. 2 lit. g RODO);

---

29 „Niespełnienie określonego w art. 111 § 1 k.k. warunku uznania za przestępstwo czynu popełnionego za granicą również przez ustawę obowiązującą w miejscu jego popełnienia, stanowi przeszkodę prowadzenia przed sądem polskim postępowania w kwestii odpowiedzialności karnej" – P. Gensikowski, [w:] D. Drajewicz (red.), *Kodeks postępowania karnego*, t. 1, *Komentarz. Art. 1–424*, Warszawa 2021, s. 85.

8. cofnięcia certyfikacji lub nakazania podmiotowi certyfikującemu cofnięcia certyfikacji udzielonej na mocy art. 42 lub 43 RODO lub nakazania podmiotowi certyfikującemu nieudzielania certyfikacji, jeżeli jej wymogi nie są spełnione lub przestały być spełniane (art. 58 ust. 2 lit. h RODO),

9. nakazanie zawieszenia przepływu danych do odbiorcy w państwie trzecim lub do organizacji międzynarodowej (art. 58 ust. 2 lit. j RODO).

Każda z wymienionych sytuacji, za wyjątkiem kwalifikowanej do upomnienia operacji przetwarzania danych, zawiera w sobie działania i zaniechania administratora lub podmiotu przetwarzającego dane na przedpolu naruszenia ochrony danych osobowych, tj. prowadzące do tego naruszenia, umożliwiające naruszenie, ułatwiające naruszenie lub działania i zaniechania występujące obok naruszenia ochrony danych osobowych lub polegające na niedopełnieniu obowiązkom wynikającym z zaistniałego naruszenia ochrony danych osobowych. Typy naruszeń skutkujące ostrzeżeniem, nakazaniem dostosowania operacji przetwarzania do wymogów RODO, cofnięciem certyfikacji, nakazaniem ograniczenia przetwarzania niewątpliwie godzą w bezpieczeństwo danych, nie stanowią jednakże o wysokim ryzyku naruszenia praw lub wolności osób fizycznych w rozumieniu art. 34 ust. 1 RODO, w konsekwencji wyłączone są z pola kryminalizacji art. 107 UODO. Stwierdzenie, w odniesieniu do danego czynu stanowiącego naruszenie przepisów ROOD, że realizuje on jedną z przesłanek określonych w art. 58 ust. 2 lit. a, c–h, j RODO kwalifikujących go jako delikt administracyjny, wyłączy zatem zastosowanie przepisu karnego.

Pozbawiona tej użyteczności jest natomiast przesłanka naruszenia przepisów RODO wprost przez operację przetwarzania danych osobowych (art. 58 ust. 2 lit. b RODO). Przesłanka ta odczytywana w oparciu reguły wykładni językowej nie prowadzi do rozróżnienia deliktu administracyjnego od występku. Naruszenie RODO przez operację przetwarzania danych może bowiem zawierać w sobie również przetwarzanie bez uprawnienia lub przetwarzanie, które nie jest dozwolone w rozumieniu art. 107 UODO. Na gruncie tak sformułowanej przesłanki zastosowania środka naprawczego i administracyjnej kary pieniężnej nie można wyodrębnić zachowań wyczerpujących wyłącznie znamiona występku. Pozostaje tym samym odwołanie się do omówionego już pojęcia naruszenia ochrony danych osobowych. Wykładnia systemowa prowadzi zatem do stopniowania naruszenia przepisów RODO przez operację przetwarzania danych od:

– deliktów administracyjnych niestanowiących naruszeń ochrony danych osobowych zagrożonych upomnieniem,

– przez delikty stanowiące naruszenia ochrony danych osobowych niezawierające w sobie ryzyka lub zawierające niewysokie ryzyko naruszenia praw i wolności osób, których dane osobowe dotyczą, zagrożone upomnieniem lub administracyjną karą pieniężną,

– po występki polegające na naruszeniu ochrony danych osobowych o wysokim ryzyku naruszenia praw i wolności osób, których dane osobowe dotyczą.

W sytuacji naruszenia ochrony danych osobowych o wysokim ryzyku naruszenia praw i wolności administrator i podmiot przetwarzający dane mogą zostać ukarani administracyjnie za towarzyszące przestępstwu inne naruszenia RODO.

Wnioski

1. Przepis art. 107 UODO typizujący występek nielegalnego przetwarzania danych osobowych ma charakter blankietowy – rekonstrukcja znamion wymaga odwołania się do przepisów RODO.

2. Art. 107 UODO kryminalizuje nielegalne przetwarzanie danych osobowych, ograniczone do naruszenia ochrony danych osobowych, skutkującego konkretnym narażeniem na niebezpieczeństwo chronionych dóbr, pociągające za sobą wysokie ryzyko naruszenia prawa i wolności osób, których dane osobowe dotyczą.

3. Naruszenia RODO stanowiące przesłanki zastosowania środków naprawczych lub administracyjnej kary pieniężnej, wymienione w art. art. 58 ust. 2 lit. a, c–h, j RODO, nie wchodzą w zakres kryminalizacji art. 107 UODO.

Wykaz literatury

Bojarski M. (red.), *Szczególne dziedziny prawa karnego. Prawo karne wojskowe, skarbowe i pozakodeksowe*, seria: *System prawa karnego*, t. 11, C.H. Beck, Warszawa 2014.

Bojarski T. (red.), *Źródła prawa karnego*, seria: *System prawa karnego*, t. 2, C.H. Beck, Warszawa 2011.

Drajewicz D. (red.), *Kodeks postępowania karnego*, t. 1, *Komentarz. Art. 1–424*, C.H. Beck, Warszawa 2021.

Gawroński M. (red.), *Ochrona danych osobowych. Przewodnik po ustawie i RODO z wzorami*, Wolters Kluwer, Warszawa 2018.

Krzysztofek M., *Ochrona danych osobowych w Unii Europejskiej*, Wolters Kluwer, Warszawa 2014.

Kühling J., Buchner B. (red.), *Dattenschutz-Grundverordnung. Bundesdatenschutzgesetz. Kommentar*, C.H. Beck, München 2020.

Litwiński P. (red.), *Ustawa o ochronie danych osobowych. Komentarz*, C.H. Beck, Warszawa 2018.

Marek A., *Kodeks karny. Komentarz*, Wolters Kluwer, Warszawa 2007.

Morawski L., *Zasady wykładni prawa*, Dom Organizatora TNOiK, Toruń 2006.

Nowak P., *O skutkowości przestępstw formalnych*, „Zeszyty Prawnicze" 2014, t. 14, nr 1.

Sakowska-Baryła M. (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, C.H. Beck, Warszawa 2018.

Summary

Criminalization of the personal data breach

Key words: criminal law, criminalization, personal data, personal data breach, the offence of illegal processing of personal data, administrative penalties.

The problem of the scope of criminalization under Art. 107 Act on Personal Data Protection is important when processing personal data or sets of personal data is common. It is not clear to what extent the provision of Art. 107 Act on PDP includes the criminalization of violation of the provisions of the General Data Protection Regulation. Moreover, the imposition of criminal sanctions for infringement of national data protection law and administrative sanctions should not lead to a breach of the principle of *ne bis in idem*. Undoubtedly, the more careful editing of Art. 107 Act on PDP would avoid many doubts about the interpretation of this provision. The article is concerned with the analysis of the personal data breach. The purpose of this study is to interpret the features of "non-permissible" and "unauthorized processing personal data". The key is to determine the meaning and mutual relationship between these terms and the personal data breach. The skilful use of interpretation rules that is known in criminal law and administrative law allows criminals to be held responsible for the most serious violations of the rules of personal data processing. The author draws attention to the relationship between general conditions for the corrective powers, imposing administrative fines and the personal data breach. The legal analysis indicates that the term of personal data breach determines the scope of criminalization of the crime of illegal processing of personal data.