Adam Szkurłat*

Kompetencje Prezesa UODO w zakresie cyberbezpieczeństwa w świetle polskich i unijnych regulacji prawnych

Spis treści

Streszczenie

W ramach niniejszego opracowania przedstawiono status i kompetencje organu nadzorczego powołanego w celu ochrony podstawowych praw i wolności osób fizycznych związanych z przetwarzaniem danych osobowych. Dokonana analiza przeprowadzona została z perspektywy przepisów prawa polskiego i unijnego, ze szczególnym uwzględnieniem RODO. Jednocześnie podjęto próbę określenia pozycji i kompetencji Prezesa UODO, działającego jako polski organ nadzorczy w sferze ochrony danych osobowych, w ramach krajowego systemu cyberbezpieczeństwa.

Słowa kluczowe: cyberbezpieczeństwo; RODO; organ nadzorczy; Prezes Urzędu Ochrony Danych Osobowych; krajowy system cyberbezpieczeństwa.

JEL: K23, K24, K33

I. Wstęp

Tematyka współpracy organów nadzoru oraz regulatorów rynku w odniesieniu do działań zapewniających cyberbezpieczeństwo jest zagadnieniem nabierającym coraz większego znaczenia. Wynika to nie tylko z popularyzacji i upowszechnienia elektronicznego obiegu danych i informacji oraz wykorzystywanych w tym celu narzędzi, lecz także jest efektem rozbudowania aparatu instytucjonalnego służącego do zapewnienia ochrony osobom fizycznym, w tym w szczególności konsumentom. Zróżnicowanie i mnogość dziedzin obrotu społecznego i gospodarczego, w których dochodzi do przynajmniej częściowego zautomatyzowania przetwarzania danych rodzi realne ryzyko naruszenia cyberbezpieczeństwa. Zastrzec przy tym należy, że w obiegu pojęcie „cyberbezpieczeństwa" w dużej mierze funkcjonuje w potocznym znaczeniu, zakładającym wszelkie działania, warunki i wymagania eliminujące stan zagrożenia w systemach informacyjnych

* Adwokat w Lubasz i Wspólnicy – Kancelarii Radców Prawnych sp. k.; absolwent studiów podyplomowych „Wykonywanie funkcji inspektora ochrony danych" w INP PAN w Warszawie; e-mail: adam.szkurlat@lubasziwspolnicy.pl.

i informatycznych, w szczególności w Internecie. Przeprowadzone niżej rozważania odrywają się od zwyczajowego rozumienia cyberbezpieczeństwa i obejmują analizę tej instytucji w normatywnym znaczeniu.

II. Pojęcie „cyberbezpieczeństwa" w kontekście przepisów RODO

Pojęcie cyberbezpieczeństwa od samego początku rodziło liczne wątpliwości w zakresie konkretnego znaczenia i nadania mu pewnych ram normatywnych. Podejmowane w literaturze przedmiotu próby definiowania cyberbezpieczeństwa nie miały kompleksowego charakteru, w zależności bowiem od dziedziny nauki uwypuklano aspekty informatyczne, społeczne, militarne czy funkcjonalne. Z tego też względu przedstawiciele doktryny podkreślali blankietowość tego terminu, przyjmując, że treść tego pojęcia jest zmienna, poddana ewolucji stosownie do zmian stosunków społecznych (Banasiński, 2018, s. 33). Takie stanowisko korespondowało z dynamicznymi zmianami zachodzącymi zwłaszcza w cyberprzestrzeni. Pomimo tych zmian, podjęta jednak została próba nadania znaczenia normatywnego. W polskim porządku prawnym znaczącym wyłomem w dookreślaniu pojęcia „cyberbezpieczeństwa" okazała się ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[1] (dalej: uksc). W art. 2 pkt 4) przywołanej ustawy polski prawodawca zawarł legalną definicję cyberbezpieczeństwa, przez które należy rozumieć

> *odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.*

Powyższa definicja zawiera szereg elementów, które umożliwiają powiązanie analizowanego pojęcia z tematyką ochrony danych osobowych i przepisami regulującymi tę problematykę. Wśród tych łączników należy wskazać na następujące terminy: poufność, integralność, dostępność, przetwarzanie. Co istotne, samo pojęcie „cyberbezpieczeństwa" wprost nie występuje w dwóch podstawowych aktach prawnych regulujących ochronę danych osobowych i działalność organu nadzorczego: RODO oraz ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (dalej: uodo). Warto jednak zwrócić uwagę, że w motywie 49 RODO europejski ustawodawca wykorzystuje pojęcia definiujące cyberbezpieczeństwo. Zgodnie z przywołanym motywem

> *przetwarzanie danych osobowych w zakresie bezwzględnie niezbędnym i proporcjonalnym do zapewnienia bezpieczeństwa sieci i informacji – tj. zapewnienia odporności sieci lub systemu informacyjnego na danym poziomie poufności na przypadkowe zdarzenia albo niezgodne z prawem lub nieprzyjazne działania naruszające* ***dostępność****, autentyczność,* ***integralność*** *i* ***poufność*** *przechowywanych lub przesyłanych danych osobowych – oraz bezpieczeństwa związanych z nimi usług oferowanych lub udostępnianych poprzez te sieci i systemy przez organy publiczne, zespoły reagowania na zagrożenia komputerowe, zespoły reagowania na komputerowe incydenty naruszające bezpieczeństwo, dostawców sieci i usług łączności elektronicznej oraz dostawców technologii i usług w zakresie bezpieczeństwa jest prawnie uzasadnionym interesem administratora, którego sprawa dotyczy.*

[1] DzU 2018, poz. 1560.

Co symptomatyczne, wspomniana w definicji cyberbezpieczeństwa triada wymagań dotyczących przetwarzanych danych pojawia się w RODO także w art. 32, regulującym obowiązki administratora w zakresie zapewnienia bezpieczeństwa przetwarzania. W ustępie 1 lit. b wspomnianego przepisu RODO unijny normodawca zobowiązuje administratora i podmiot przetwarzający do wdrożenia odpowiednich środków technicznych,

> *aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku (…) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania.*

Integralność i poufność mają w RODO dodatkowo status ogólnej zasady przetwarzania danych osobowych, która wymaga zapewnienia ochrony danych przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem (por. art. 5 ust. 1 lit f RODO).

W odniesieniu do cyberbezpieczeństwa wspomniane pojęcia „dostępności", „integralności" i „poufności" zawarte są także w szeregu norm standaryzujących systemy zarządzania bezpieczeństwem informacji, które mogą być zastosowane w celu realizacji przez administratora obowiązku wynikającego z art. 32 RODO. Powyższa uwaga dotyczy zwłaszcza norm ISO z serii ISO/IEC 27001, które – w myśl zasady *risk based approach* i w związku z obowiązkiem cyklicznych przeglądów – podlegają ciągłym zmianom warunkowanym postępem technologicznym (Lubasz, 2018, s. 701).

Osobne rozważania należy poświęcić wspólnemu dla RODO i uksc pojęciu „przetwarzania". Zasadniczo podzielić należy prezentowane w doktrynie stanowisko, że pojęcie to należy rozumieć

> *tak, jak przez ostatnie dwie dekady w ustawie z 29 sierpnia 1997 r. o ochronie danych osobowych (…), a obecnie w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) […]* (Szpor, 2019, s. 44).

Na gruncie 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".*

W literaturze przedmiotu podkreśla się nadto użycie przez ustawodawcę sformułowania „system informacyjny", a nie „system informatyczny", co ma istotne znaczenie z punktu widzenia stosowania przepisów nie tylko do kwestii związanych ze stosowanym sprzętem i oprogramowaniem (*hardware* i *software*), lecz także do przetwarzanych danych (*content*) (Szpor, 2019, s. 44).

Zbieżna nomenklatura stosowana w uksc i RODO oraz znaczenie cyberbezpieczeństwa dla przetwarzania danych osobowych determinują rozważania dotyczące roli organu nadzorczego

w odniesieniu do kontrolowania i nadzorowania przetwarzania danych w ramach działań stanowiących jednocześnie realizację wytycznych ustawodawcy w zakresie cyberbezpieczeństwa.

III. Organ nadzorczy – definicja i dualizm regulacji

Pojęcie „organu nadzorczego" zostało zdefiniowane w art. 4 pkt 21 RODO. W myśl tego przepisu oznacza ono „niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51" RODO. Przepis, do którego odsyła przytoczona definicja przewiduje zaś, że

> *każde państwo członkowskie zapewnia, by za monitorowanie stosowania (…) rozporządzenia odpowiadał co najmniej jeden niezależny organ publiczny w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii (dalej: organem nadzorczym).*

W sferze ochrony danych osobowych pozycja prawna organu nadzorczego została uregulowana dwojako: na poziomie unijnym oraz na szczeblu krajowym. W tym pierwszym wypadku zdecydowano się na unormowanie podstawowych kwestii, dotyczących m.in. gwarancji niezależności organu nadzorczego, zasad jego ustanawiania, zadań i uprawnień. *Ratio legis* takiego rozwiązania wynika z potrzeby unifikacji podstawowych zasad funkcjonowania ciał nadzorczych w poszczególnych krajach członkowskich. Wprowadzenie minimalnego standardu i jednolitego poziomu ochrony danych, obowiązujących we wszystkich państwach Unii Europejskiej, ma zapewnić pełną transparentność dla administratorów i podmiotów danych w zakresie ustalenia organów odpowiedzialnych za przestrzeganie przepisów o ochronie danych, ale będzie służyć również realizacji zasady swobodnego przepływu danych. Otwarty rynek i związane z tym możliwości świadczenia usług na terenie całej Unii Europejskiej wiążą się bowiem z transferami danych i ich transgranicznym przetwarzaniem, co z kolei rodzi ryzyko wystąpienia naruszeń w obszarze jurysdykcji innego państwa. Wychodząc naprzeciw tego rodzaju sytuacjom oraz chcąc zapełnić spójność w prowadzeniu postępowań i rozstrzyganiu spraw unijny ustawodawca zdecydował się uregulować w sposób szczególny zasady współpracy między organami nadzorczymi poszczególnych krajów. Wszystkie wspomniane wyżej okoliczności zadecydowały także o formie zastosowanego ostatecznie aktu prawa wspólnotowego, jakim jest rozporządzenie. Tylko taka postać regulacji gwarantuje wiążący charakter regulacji dla państw członkowskich. Zgodnie bowiem z art. 288 TFUE

> *rozporządzenie ma zasięg ogólny, wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.*

Wiążący charakter RODO jest jednakże łagodzony poprzez szereg postanowień RODO (m.in. art. 54 ust. 1, art. 58 ust. 5 i 6), które dają krajowym ustawodawcom pewien zakres swobody w kształtowaniu statusu organu nadzorczego.

W kontekście cyberbezpieczeństwa istotna wydaje się analiza przepisu art. 57, który statuuje zadania stawiane przed organem nadzorczym. Wyliczenie kompetencji zawarte w art. 57 ust. 1 RODO jest niezwykle rozbudowane, jednakże nie stanowi katalogu zamkniętego. Z jednej strony bowiem w początkowej części ww. przepisu zastrzeżono, że każdy organ nadzorczy

na swoim terytorium realizuje wymienione zadania bez uszczerbku dla innych zadań, z drugiej zaś – do zadań organu nadzorczego należy „wypełnienie innych zadań związanych z ochroną danych osobowych". W katalogu zadań organu nadzorczego mieści się natomiast tylko jedno działanie, które wprost może znaleźć przełożenie na cyberbezpieczeństwo – monitorowanie zmian w stosownych dziedzinach, o ile zmiany te mają wpływ na ochronę danych osobowych, w szczególności monitorowanie rozwoju technologii informacyjno-komunikacyjnych i praktyk handlowych. Z przepisów RODO nie wynika natomiast kompetencja organu nadzorczego do działania w innych obszarach niż problematyka dotycząca *stricte* przetwarzania danych osobowych.

Druga gałąź przepisów, które normują status organu nadzorczego, obejmuje przepisy prawa krajowego. W polskim porządku prawnym regulacje te znajdują się głównie w rozdziale 6 uodo, zatytułowanym „Prezes Urzędu". W tym miejscu należy poczynić wzmiankę, że w Polsce obowiązuje model jednego niezależnego organu nadzorczego w rozumieniu RODO. Rozwiązanie to stanowi kontynuację stosowanego dotychczas systemu, wprowadzonego w życie poprzednio obowiązującą ustawą o ochronie danych osobowych[2]. Wdrożenie unijnej reformy ochrony danych osobowych spowodowało przekształcenie dotychczasowego organu nadzorczego, tj. Generalnego Inspektora Ochrony Danych Osobowych w nowy, którym stał się Prezes Urzędu Ochrony Danych Osobowych (Fajgielski, 2018).

Określając status Prezesa UODO polski ustawodawca po pierwsze wskazał, że podmiot ten „jest organem właściwym w sprawie ochrony danych osobowych" (art. 34 ust. 1 uodo), po wtóre zaś wprost określił, że potwierdził, że

> *Prezes Urzędu jest organem nadzorczym w rozumieniu rozporządzenia 2016/679, w rozumieniu dyrektywy 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 (Dz. Urz. UE L 119 z 04.05.2016, s. 89) oraz w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępującego i uchylającego decyzje Rady […]* (art. 34 ust. 2 uodo).

Przepisy rozdziału 6 uodo zawierają szereg przepisów o charakterze ustrojowym, normujących kwestie formalne, takie jak: immunitet Prezesa UODO, procedurę pociągnięcia go do odpowiedzialności, obowiązek zachowania tajemnicy czy sprawozdawczość z prowadzonej działalności. Poza działaniami o charakterze informacyjno-edukacyjnym, opiniodawczym czy prewencyjnym brakuje natomiast w polskiej ustawie przepisów nakładających obowiązki czy precyzujących szczególne kompetencje Prezesa UODO (Chomiczewski, 2019, s. 239 i n.). Przepisy uodo nie zawierają przy tym postanowień, które wprost odnosiłyby się do kwestii cyberbezpieczeństwa.

[2] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (DzU 1997 Nr 133, poz. 883).

IV. Zadania Prezesa UODO w świetle uksc

Przepisy uksc zawierają szereg regulacji określających organy właściwe do spraw cyberbezpieczeństwa oraz zakres przypisanych im zadań. Normy z tego zakresu zawarte są w rozdziale 8 uksc, zatytułowanym „Organy właściwe do spraw cyberbezpieczeństwa". Wyliczenie zawarte w art. 41 uksc obejmuje poszczególne sektory oraz podmioty przypisane do każdego z nich. Wśród tych podmiotów znajdują się m.in. ministrowie właściwi do spraw przynależnych do danego sektora oraz Komisja Nadzoru Finansowego. Wspomniany przepis nie odwołuje się natomiast w żadnym miejscu do Prezesa UODO jako organu właściwego do spraw cyberbezpieczeństwa. Komentatorzy uksc wskazują przy tym, że za takim uregulowaniem przemawia

> *fakt, iż organy te dysponują odpowiednimi możliwościami prawnymi oraz zasobami niezbędnymi do skutecznej realizacji powierzonych zadań* (Prusak-Górniak i Silicki, 2019, s. 351).

Uprawnienia Prezesa UODO do działania w zakresie cyberbezpieczeństwa można natomiast wywodzić z treści art. 39 uksc, który reguluje problematykę przetwarzania danych przez Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego (tzw. CSIRT: CSIRT MON, CSIRT NASK i CSIRT GOV) oraz sektorowe zespoły cyberbezpieczeństwa. W ustępie 1 ww. przepisu wskazano, że w celu realizacji zadań określonych w przepisach art. 26 ust. 3 pkt 1–11, 14 i 15 i ust. 5–8 oraz art. 44 ust. 1–3 uksc ww. jednostki przetwarzają dane pozyskane w związku z incydentami i zagrożeniami cyberbezpieczeństwa, w tym dane osobowe, obejmujące także dane określone w art. 9 ust. 1 RODO. Zastosowanie ogólnego rozporządzenia o ochronie danych determinuje przy tym kognicję Prezesa UODO w zakresie monitorowania i egzekwowania stosowania RODO. W sposób pośredni zatem i tylko w odniesieniu do przetwarzania danych dotyczących incydentów i zagrożeń cyberbezpieczeństwa Prezes UODO jest uprawniony do ingerowania w proces przetwarzania danych. Ocena tego procesu może jednakże dotyczyć wyłącznie stosowania przepisów i wdrożenia wymagań przewidywanych przez RODO oraz przepisy uksc. W odniesieniu do przetwarzania danych szczególnych kategorii uksc nakłada na administratorów dodatkowy obowiązek prowadzenia analizy ryzyka, stosowania środków ochrony przed złośliwym oprogramowaniem, wprowadzenia mechanizmów kontroli dostępu oraz opracowania procedury bezpiecznej wymiany informacji. Również w tym zakresie Prezes UODO jest uprawniony do prowadzenia kontroli i weryfikacji prawidłowości przetwarzania danych w związku z obowiązkami określonymi w RODO.

V. Wnioski

Szczegółowa kwerenda przepisów uksc, RODO i uodo prowadzi do konkluzji, że Prezes UODO ma minimalną możliwość ingerowania w kwestie dotyczące cyberbezpieczeństwa. W istocie kompetencje polskiego organu nadzorczego ograniczają się do działania jedynie tam, gdzie bezpośrednie zastosowanie znajduje RODO. W przypadku krajowego systemu cyberbezpieczeństwa regulacja art. 39 uksc przewiduje zastosowanie RODO, a tym samym prerogatyw organu nadzorczego jedynie do przetwarzania danych związanych z incydentami i zagrożeniami cyberbezpieczeństwa. Prezes UODO nie został natomiast wprost uwzględniony w strukturze organów właściwych do spraw cyberbezpieczeństwa. Również uodo nie zawiera przepisów regulujących szczególne uprawnienia polskiego organu nadzorczego w zakresie ochrony danych osobowych,

chyba żeby uznać za takie monitorowanie rozwoju technologii informacyjno-komunikacyjnych, które miałyby wpływ na ochronę danych osobowych. Uprawnienie to nie wiąże się jednakże z możliwością bezpośredniego ingerowania w procesy przetwarzania danych i wpływania na poziom cyberbezpieczeństwa.

Relatywnie krótki okres obowiązywania wszystkich analizowanych aktów prawnych nie pozwala jeszcze na dokonanie kompletnej oceny czy narzędzia prawne, w które wyposażony został Prezes UODO są wystarczające do czuwania nad zapewnieniem cyberbezpieczeństwa w kontekście ochrony danych osobowych. Wydaje się, że dopiero prowadzone przez organ nadzorczy kontrole, zwłaszcza w odniesieniu do podmiotów ustawowo odpowiedzialnych za cyberbezpieczeństwo, pozwolą na precyzyjną i kompleksową oceną zaproponowanych przez ustawodawcę rozwiązań.

Bibliografia

Banasiński, C. (2018). Cyberbezpieczeństwo jako przedmiot badań. W: C. Banasiński (red.), *Cyberbezpieczeństwo, Zarys wykładu*. Warszawa: Wolters Kluwer.

Chomiczewski, W. (2019). Komentarz do art. 34 u.o.d.o. W: D. Lubasz (red.), *Ustawa o ochronie danych osobowych. Komentarz*. Warszawa: Wolters Kluwer.

Fajgielski, P. (2018). Komentarz do art. 51 RODO. W: P. Fajgierski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych*. Komentarz. Warszawa: Wolters Kluwer Polska.

Lubasz, D. (2018). Komentarz do art. 32 RODO. W: E. Bielak-Jomaa, D. Lubasz (red.), *RODO Ogólne Rozporządzenie o ochronie danych. Komentarz.* Warszawa: Wolters Kluwer.

Prusak-Górniak, K. i Silicki, K. (2019). Komentarz do art. 41 k.s.c. W: G. Szpor, A. Gryszczyńska, K. Czaplicki (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*. Warszawa: Wolters Kluwer.

Szpor, G. (2019). Komentarz do art. 2 k.s.c. W: G. Szpor, A. Gryszczyńska, K. Czaplicki (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*. Warszawa: Wolters Kluwer.