Roczniki Administracji i Prawa nr XIX(2), s. 179-192

Oryginalny artykuł naukowy
Original article

Data wpływu/Received: **12.07.2019**
Data recenzji/Accepted: **16.11.2019**
Data publikacji/Published: **30.12.2019**

Źródła finansowania publikacji: Wyższa Szkoła Humanitas

DOI: 10.5604/01.3001.0014.0435

Authors' Contribution:
(A) Study Design (projekt badania)
(B) **Data Collection (zbieranie danych)**
(C) Statistical Analysis (analiza statystyczna)
(D) **Data Interpretation (interpretacja danych)**
(E) **Manuscript Preparation (redagowanie opracowania)**
(F) Literature Search (badania literaturowe)

Tomasz Miłkowski*
Nr ORCID: 0000-0003-2465-4423

NOWE ZASADY GROMADZENIA I OCHRONY DANYCH OSOBOWYCH PRZEZ SŁUŻBY POLICYJNE

Problematyka gromadzenia i ochrony danych przez służby policyjne jest jedną z podstawowych kwestii związanych z gromadzeniem informacji w ogóle. Obejmuje ona bowiem nie tylko dane, do których dostęp może być stosunkowo szeroki, jak np. rejestr skazanych, dane adresowe, ewidencja kierujących i punktów karnych itp., ale także te, które są niejawne, a do tego pochodzą – w niektórych przypadkach – z niesprawdzonych źródeł. Powoduje to, że z formalnego punktu widzenia część z nich mogłaby mieć charakter pomówień czy wręcz bezpodstawnych oskarżeń. Nie jest tak głównie dlatego, że dane operacyjno-rozpoznawcze, bo o takich przede wszystkim jest tutaj mowa, nie są upubliczniane czy udostępniane, nawet osobom,

* dr; Wyższa Szkoła Humanitas, Instytut Nauk Prawnych.

których potencjalnie dotyczą. Konsekwencje więc „wycieku" czy też niewłaściwej ochrony takich danych mogłyby być poważne. Chodzi zresztą nie tylko o fałszywe oskarżenia, ale i informacje prawdziwe[1], które wpływać mogą na postrzeganie konkretnej osoby. Widać to zresztą doskonale po upublicznianych przypadkach włamań do baz danych podmiotów gospodarczych, których skutki są z finansowego czy wizerunkowego punktu widzenia bardzo poważne. Podmioty publiczne muszą zaś chronić dane obywateli również i dlatego, że gromadzą je i przetwarzają często niezależnie od ich woli. Co więcej, poprzez działalność legislacyjną nierzadko nie pozostawiają żadnego wyboru, „zmuszając" obywateli do przekazywania takich danych. W zamian jednak muszą zagwarantować, że nikt nieupoważniony nie pozna ich treści. Prawa do ochrony prywatności, tajemnicy korespondencji czy wolności od naruszenia miru domowego są bowiem standardem demokratycznego państwa prawa. Wynika to zarówno z reguł konstytucyjnych, jak i obszernego dorobku legislacyjnego Unii Europejskiej. Dane gromadzone w obszarze bezpieczeństwa są zaś niczym innym jak częścią informacji, w posiadaniu których są podmioty publiczne.

Znaczenie takich danych widoczne jest szczególnie w przypadku gromadzenia danych przez służby ochrony i porządku publicznego, do których zaliczyć możemy: Policję, Straż Graniczną (SG), Służbę Ochrony Państwa (SOP), Żandarmerię Wojskową (ŻW), Krajową Administrację Skarbową (KAS), Centralne Biuro Antykorupcyjne (CBA), Agencję Bezpieczeństwa Wewnętrznego (ABW), Agencję Wywiadu (AW), Służbę Kontrwywiadu Wojskowego (SKW) i Służbę Wywiadu Wojskowego (SWW). Są to bowiem – co wypada jeszcze raz podkreślić – w wielu wypadkach informacje, których ujawnienie może wpływać w istotny sposób na postrzeganie danej osoby. Mogą przecież dotyczyć one materii dosyć łatwych do zweryfikowania, ale czasem jest inaczej, szczególnie w przypadku wiedzy operacyjno-rozpoznawczej. Nie zawsze muszą być one prawdziwe, tak w części, jak i jako całość. Specyfika pracy tych służb nie pozwala jednak na to, by jedynie przy braku możliwości ich jednoznacznej weryfikacji je odrzucać lub usuwać. Podejrzenia, prawdopodobieństwo, wskazanie na możliwy związek czy utrzymywanie kontaktu z grupami przestępczymi itp. są czymś „naturalnym" w działaniach tych służb. Czymś, co trzeba sprawdzić, ale zanim tak się stanie, jedynym właściwie obostrzeniem jest zakaz „użycia" takiej wiedzy wobec danej osoby. Nawet jednak w takim wypadku jak wykluczenie prawdziwości, informacja nie musi „zniknąć" z rejestrów (katalogów) danych operacyjno-rozpoznawczych. Może służyć choćby pracy analitycznej.

Kwestia ta wymaga jednak, chociażby z punktu widzenia gwarancji praw i wolności jednostki, by spojrzeć na nią szerzej. Na gruncie Konstytucji Rzeczypospolitej Polskiej z 1997 r.[2] możemy w tym wypadku przywołać chociażby jej art. 2, art. 47, art. 49, art. 50 i art. 51. Pierwszy z nich, wskazujący, że Rzeczpospolita jest demokra-

[1] Jak np. dane o popełnionych wykroczeniach, podejrzeniach przemocy domowej itd.
[2] Dz.U. nr 78, poz. 483, ze zm. – dalej: Konstytucja.

tycznym państwem prawnym, stanowi swoiste preludium dla rozwinięcia omawianego zagadnienia w dalszych przepisach. Art. 47 Konstytucji, gwarantujący każdemu prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym, kładzie nacisk na aspekt wewnętrzny funkcjonowania osoby w społeczeństwie. Dwa kolejne z przywołanych, odnoszące się do wolności i ochrony tajemnicy komunikowania się (art. 49) oraz nienaruszalności mieszkania (art. 50), których (w obu wypadkach) ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony, kierowane są już w pierwszym rzędzie do tych, którzy chcieliby to prawo do intymności życia prywatnego naruszyć. Także gdy to „naruszenie" ma swoje oparcie w legalnych działaniach władzy. Z oczywistych względów dotyczy to bowiem również instytucji oraz organów publicznych (państwowych), które w określonych prawem przypadkach mogą wkroczyć w tak określone prawo (wolność). Rodzi to jednocześnie po stronie tych podmiotów potencjalnie dwojakiego rodzaju odpowiedzialność. Po pierwsze, z tytułu naruszenia reguł stanowiących podstawę do ingerencji w te prawa, a po drugie z tytułu dopuszczenia do wejścia w posiadanie takich informacji przez osoby nieuprawnione, nawet jeśli ich pozyskanie było legalne. Jak stanowi art. 30 Konstytucji, przyrodzona i niezbywalna godność człowieka jest źródłem wolności oraz praw człowieka i obywatela. Stąd tak istotne jest, by organy władzy respektowały ją w każdym jej przejawie i kształcie i wyraźne podkreślenie, że jest ona nienaruszalna, a jej poszanowanie i ochrona jest wręcz obowiązkiem władz publicznych. W tym właśnie kontekście należy odczytywać treść art. 51 Konstytucji, stanowiącego swoisty łącznik pomiędzy prawem do prywatności a obowiązkami wynikającymi z życia jednostki w szerszym aspekcie – społecznym i państwowym. Jest on również pewnym „objaśnieniem" rozumienia godności z punktu widzenia funkcjonowania jednostki w społeczeństwie informacyjnym. Ustanawia on w tym względzie kilka reguł, a mianowicie:

1) nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji go dotyczących;

2) władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym;

3) każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych (choć ustawa może określić ograniczenie tego prawa);

4) każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą;

5) zasady i tryb gromadzenia oraz udostępniania informacji określać musi ustawa.

Jak już wspomniano, powyższe regulacje są jednocześnie inspiracją i zobowiązaniem dla ustawodawcy. Każdy przepis i każda norma odnosząca się do prawa do prywatności i jej obrony przed dostępem osób trzecich musi znajdować swoje oparcie w powyższych regulacjach.

Pierwszym widocznym tego przejawem było uchwalenie 29 sierpnia 1997 r. ustawy *o ochronie danych osobowych*[3]. Jednocześnie jednak mieliśmy do czynienia z dwoma kierunkami aktywności legislacyjnej. Obok powyżej wspomnianej ustawy (i kolejnych aktów) związanej z powszechnym dostępem i ogólnymi zasadami ochrony informacji, w dziedzinie szeroko rozumianego bezpieczeństwa i porządku publicznego regulacje te opierały się w pierwszym rzędzie na treści ustaw służb policyjnych i specjalnych, w których zwarto dosyć skąpe przepisy związane z prawem do gromadzenia danych, a jednocześnie regułami ich ochrony i udostępniania. Ustawa „ogólna", jaką była ustawa o ochronie danych osobowych, w tej mierze ustanawiała jedynie pewne podstawowe zasady tworzenia, rejestrowania i kontrolowania prawidłowości gospodarowania bazami danych. W praktyce ochrona tych danych polegała głównie na pozostawieniu ich w zawiadywaniu rzeczonych służb i „domniemanej zgodzie" na ich gromadzenie bez możliwości wglądu z zewnątrz. Z tego też punktu widzenia ochrona tych informacji była o tyle „łatwiejsza", że i problematyka dostępu do informacji publicznej nie musiała uwzględniać możliwości wglądu w takie dane[4]. Nie musiała, gdyż dostęp ten był z założenia praktycznie wykluczony.

Obok samych ustaw kształtujących ustrój służb policyjnych i specjalnych mieliśmy oczywiście do czynienia i z innymi aktami, które za przedmiot regulacji miały zagadnienia gromadzenia, przetwarzania lub przekazywania informacji kryminalnych. Były to i są jednak zawsze ustawy kształtujące jedynie wycinek tej problematyki. Co ciekawe, niektóre z nich obejmują swoim zakresem zarówno materię rozwiązań krajowych, jak i europejskich. Wśród takich ustaw możemy wymienić chociażby takie, jak: z 6 lipca 2001 r. *o przetwarzaniu informacji kryminalnych*[5], z 16 września 2011 r. *o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi*[6] czy z 10 czerwca 2016 r. *o działaniach antyterrorystycznych*[7]. Wszystkie one odnoszą się do kwestii przetwarzania danych o szczególnym znaczeniu, a więc danych kryminalnych, policyjnych czy traktujących o problematyce bezpieczeństwa. Nie regulują one jednak problematyki dostępu do nich osób, których te dane dotyczą, a głównie możliwości ich pozyskiwania, przekazywania i wykorzystywania w ramach zadań poszczególnych służb i instytucji.

[3] Tekst jedn. Dz.U. z 2016 r., poz. 922.

[4] Art. 5 ustawy z 1997 r. stanowił, że jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ich ochronę, niż wynika to z niniejszej ustawy, stosuje się przepisy tych ustaw. Każda zaś z ustaw dotyczących służb policyjnych i specjalnych zawiera normy wyraźnie chroniące formy, metody i środki pracy, w tym źródeł informacji oraz samych informacji. Nie wspominając już o ochronie informacji niejawnych, do których należą praktycznie wszystkie pozyskiwane w ramach czynności operacyjno-rozpoznawczych.

[5] Tekst jedn. Dz.U. z 2019 r., poz. 44.

[6] Tekst jedn. Dz.U. z 2018 r., poz. 484.

[7] Tekst jedn. Dz. U. z 2019 r., poz. 904.

Na gruncie europejskim ten dualizm sposobu regulacji był być może nawet jeszcze bardziej czytelny, gdyż obowiązujący do traktatu z Lizbony podział prawodawstwa unijnego na trzy filary[8] przesądzał, że zagadnienie współpracy policyjnej było domeną stosunków międzyrządowych, a więc jedynym aktem, który mógł skłaniać do koordynacji w tym względzie, były decyzje ramowe. To zaś powodowało, że dynamiczny rozwój regulacji chroniących dane osobowe i ograniczający możliwość ich pozyskiwania z pozycji całej Unii Europejskiej nie obejmował *de facto* kwestii uprawnień służb policyjnych.

Reasumując powyższe i odnosząc się do problematyki wpływu rozwiązań normatywnych na poziomie europejskim na krajowe, wskazać należy, że wspomniana już ustawa o ochronie danych osobowych z 1997 r. czerpała w dużym stopniu z rozwiązań przewidzianych w dyrektywie 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. *w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych*[9]. Kwestia ochrony danych gromadzonych przez służby policyjne, ze wszystkimi wspomnianym ograniczeniami formalnymi, korespondowała zaś z tymi, które zawarto w decyzji ramowej Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. *w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych*[10]. Oba akty zostały jednak uchylone.

Ten przywołany stan rzeczy uległ bowiem istotnej zmianie na przestrzeni ostatnich trzech lat. Stało się tak zarówno w przypadku regulacji ogólnych, jak i tych kierowanych do służb policyjnych.

Po pierwsze, ogólne zasady ochrony danych stały się treścią 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*[11], a tym samym rozwiązania krajowe – tam gdzie je przyjęto – dotyczą głównie (ewentualnego) wyższego poziomu ochrony lub kwestii technicznych czy też rozwiązań ściśle związanych ze specyfiką danego państwa[12]. Po drugie zaś, w dziedzinie ochrony porządku i bezpieczeństwa podstawowe zasady określono 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*[13]. Choć pierwszy z tych aktów nie wymagał – co do zasady – uchwale-

[8] Choć samo pojęcie nie jest ściśle prawne, przyjęło się je używać jako najlepiej oddające istotę problemu.
[9] Dz.Urz.UE. L 1995 nr 281, s. 31.
[10] CELEX : 32008F0977.
[11] Tzw. ogólne rozporządzenie o ochronie danych (RODO), Dz.Urz.UE. L 2016 nr 119, s. 1.
[12] Przykładem jest choćby nazwa i umiejscowienie urzędu właściwego dla ochrony danych.
[13] Dz. Urz. UE L z 2016 nr 119, s. 89 – dyrektywa 2016/680.

nia specjalnie dedykowanego tej tematyce jednego aktu rangi ustawowej, jako że rozporządzenie unijne jest stosowane bezpośrednio w każdym z krajów Unii Europejskiej, 10 maja 2018 r. uchwalono nową ustawę *o ochronie danych osobowych*[14], jednocześnie czasowo w mocy zachowując te przepisy, które w szerokim znaczeniu wiązały się z ochroną danych gromadzonych przez służby[15]. W materii ochrony danych „policyjnych" wymagane bowiem było uchwalenie ustawy, która zawierałyby rozwiązania przewidziane w dyrektywie i dostosowywała je do naszego porządku prawnego. Rzecz jasna w tym wypadku można było rozważać kilka sposobów aktywności legislacyjnej, jak chociażby odpowiednie nowelizacje każdej z ustaw służb ochrony i porządku. Zdecydowano jednak uczynić to jednym aktem, a mianowicie na mocy ustawy z 14 grudnia 2018 r. *o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości*[16]. Na marginesie tylko należy wspomnieć, że przywołane powyżej utrzymanie w mocy przepisów „starej" ustawy o ochronie danych osobowych wynikało tylko z tego, że nie zdołano uchwalić rzeczonej ustawy w przewidzianym w dyrektywie terminie, a więc do 6 maja 2018 r. Ostatnie zdanie art. 175 ustawy o ochronie danych osobowych stanowi bowiem, że przepisy tam wymienione[17] zachowują wprawdzie moc, ale jedynie „w terminie do dnia wejścia w życie przepisów wdrażających dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680. W związku z tym od lutego 2019 r. znajdujemy się w nowej i zupełnie zmienionej rzeczywistości normatywnej. Wynika to również z tego, że zagadnienia współpracy policyjnej stały się integralną częścią prawodawstwa unijnego, po odejściu od podziału na tzw. filary. Obowiązują wprawdzie w tym wypadku rozleglejsze wyjątki, w znacznie szerszym stopniu daje się państwom członkowskim Unii Europejskiej pole do podejmowania indywidualnych rozstrzygnięć, niemniej nie jest to już dziedzina regulacji międzyrządowych – ze wszystkimi tego konsekwencjami. Do podstawowych zaś należy obowiązek dostosowania prawodawstwa krajowego do treści aktów normatywnych[18], które będąc podstawowym instrumentem kreowania rozwiązań normatywnych z tego poziomu, wytyczają kierunki aktywności legislacyjnej każdego z państw członkowskich. Pamiętać należy również, że do np. wydania dyrektywy wystarcza poparcie określonej ilości państw. Tym samym nie zawsze każda z norm w niej zawartych odpowiada w pełni władzom krajowym, co jednak nie powinno mieć wpływu na wynik finalny, a więc implementację dyrektywy w danym kraju.

[14] Dz.U. poz. 1000.

[15] Art. 175 ustawy o ochronie danych osobowych z 2018 r. stanowił, że traci (wprawdzie) moc ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, z wyjątkiem (jednak) art. 1, art. 2, art. 3 ust. 1, art. 4-7, art. 14-22, art. 23-28, art. 31 oraz rozdziałów 4, 5 i 7, które zachowują moc w odniesieniu do przetwarzania danych osobowych w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, prowadzenia postępowań w sprawach dotyczących tych czynów oraz wykonywania orzeczeń w nich wydanych, kar porządkowych i środków przymusu w zakresie określonym w przepisach stanowiących podstawę działania służb i organów uprawnionych do realizacji zadań w tym zakresie.

[16] Dz.U. z 2019 r. poz. 125 – dalej: ustawa.

[17] Patrz przypis 15.

[18] Przypomnijmy, że rozporządzenia mogą być wydawane w przypadku polityki (dziedziny) leżącej całkowicie w gestii unijnej. Tam gdzie wymaga to ścisłej kooperacji z krajami członkowskimi, wyda się dyrektywy.

Dyrektywa 2016/680 – jak już wspomniano – powinna była zostać wdrożona do 6 maja 2018 r. W realiach Polski oznaczało to uchwalenie – zgodnie z decyzją Rządu – osobnej ustawy poświęconej tej tematyce. Jak wiadomo, do tej daty tak się nie stało, co w praktyce nie powinno jednak rodzić żadnych konsekwencji. Dla ich wystąpienia musiałoby bowiem dojść do zdarzenia, w którym konkretna osoba zostałaby pokrzywdzona przez brak odpowiedniej normy w krajowym porządku prawnym. Drugą możliwością jest wszczęcie – z uwagi na bierność danego kraju – procedury wyjaśniającej z uwagi na uchybienia zobowiązaniom państwa członkowskiego przez Komisję Europejską. Nie doszło do tego do wejścia w życie ustawy, a więc 6 lutego 2019 r.

Sama dyrektywa 2016/680 w swoim wstępie zawiera również wyjaśnienie powodów i celów wydania takiego aktu[19]. W motywie 10. podnosi się, że w deklaracji nr 21 w sprawie ochrony danych osobowych w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej (załączonej do Aktu końcowego konferencji międzyrządowej, która przyjęła traktat z Lizbony) uznano, że ze względu na szczególny charakter współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej konieczne może okazać się przyjęcie (na podstawie art. 16 TFUE) szczególnych przepisów o ochronie danych osobowych i swobodnym przepływie danych osobowych w tych dziedzinach. I dalej (motyw 11), że należy zatem odnieść się do tych dziedzin w odrębnej dyrektywie, która stanowi szczególne przepisy o ochronie 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 tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, z zachowaniem szczególnego charakteru takich czynności. Przy czym, jeżeli taki organ lub podmiot przetwarza dane osobowe do celów innych niż cele dyrektywy, zastosowanie ma RODO. W motywie 14. wzmiankowano również, że czynności w zakresie bezpieczeństwa narodowego, czynności agencji lub jednostek zajmujących się bezpieczeństwem narodowym, czy też przetwarzania danych osobowych przez państwa członkowskie podczas takich czynności nie wchodzą w zakres niniejszej dyrektywy i nie są nią objęte.

Osobne miejsce poświęcono problematyce ochrony danych, a także dostępu do nich, w szczególności przez osoby, których dotyczą, a także osoby trzecie. Osoba zatem, której dane dotyczą, powinna mieć prawo do tego, by nie stosowano względem niej decyzji analizującej jej cechy osobiste, opierającej się wyłącznie na przetwarzaniu automatycznym, jeśli ma ona niekorzystne skutki prawne dla takiej osoby lub poważnie na nią wpływa. Przetwarzanie takie powinno zawsze podlegać odpowiednim zabezpieczeniom, wraz z konkretną informacją dla osoby, której dane dotyczą, i prawem do uzyskania interwencji ludzkiej, a zwłaszcza prawem do wyrażenia własnego stanowiska, uzyskania wyjaśnienia decyzji wydanej wskutek takiej analizy lub zaskarżenia tej decyzji (motyw 38). Niezależ-

[19] Treść tę określa się jako motywy.

nie od tego, każda osoba fizyczna powinna mieć prawo dostępu do zebranych danych jej dotyczących oraz powinna mieć możliwość łatwego wykonywania tego prawa w rozsądnych odstępach czasu, by mieć świadomość przetwarzania danych i móc zweryfikować jego zgodność z prawem. Dlatego każda osoba, której dane dotyczą, powinna mieć prawo do poznania i uzyskania informacji na temat celów przetwarzania danych, okresu ich przetwarzania oraz odbiorców danych, także w państwach trzecich. Jeśli takie informacje obejmują informacje o pochodzeniu danych osobowych, nie powinny one ujawniać tożsamości osób fizycznych, w szczególności poufnych źródeł informacji. Dla realizacji tego prawa wystarczy zaś przekazać osobie, której dane dotyczą, pełne podsumowanie tych danych w zrozumiałej formie. Takie podsumowanie może mieć formę kopii przetwarzanych danych osobowych (motyw 43)[20]. Jednocześnie każda osoba fizyczna powinna mieć prawo (motyw 47) do uzyskania sprostowania dotyczących jej nieprawidłowych danych osobowych, zwłaszcza danych dotyczących faktów, oraz prawo do usunięcia danych. Każda osoba fizyczna powinna mieć również prawo do ograniczenia przetwarzania

[20] Przy czym informacje takie mogą (przez określony czas) być „ukryte" przed daną osobą, o czym stanowi art. 13 dyrektywy.
1. Państwa członkowskie zapewniają, by administrator udostępniał osobie, której dane dotyczą, przynajmniej następujące informacje:
a) tożsamość i dane kontaktowe administratora;
b) dane kontaktowe inspektora ochrony danych, w razie potrzeby;
c) cele przetwarzania, do których mają posłużyć dane osobowe;
d) informacje o prawie do wniesienia skargi do organu nadzorczego oraz dane kontaktowe organu nadzorczego;
e) informacje o prawie żądania od administratora dostępu do danych osobowych, sprostowania lub usunięcia danych osobowych lub ograniczenia przetwarzania danych osobowych odnoszącego się do osoby, której dane dotyczą.
2. Państwa członkowskie zapewniają, by oprócz informacji, o których mowa w ust. 1, w konkretnych przypadkach administrator przekazywał osobie, której dane dotyczą, następujące dalsze informacje umożliwiające wykonywanie przysługujących jej praw:
a) podstawa prawna przetwarzania;
b) okres przechowywania danych osobowych lub, gdy nie jest to możliwe, kryteria służące określeniu tego okresu;
c) w stosownym przypadku kategorie odbiorców danych osobowych, w tym odbiorców w państwach trzecich lub organizacjach międzynarodowych;
d) w razie potrzeby dalsze informacje, zwłaszcza gdy dane osobowe są zbierane bez wiedzy osoby, której dotyczą.
3. Państwa członkowskie mogą przyjąć akty prawne pozwalające opóźnić, ograniczyć lub pominąć informowanie osoby, której dane dotyczą, przewidziane w ust. 2 w takim zakresie i przez taki czas, w jakim odnośny środek jest działaniem koniecznym i proporcjonalnym w społeczeństwie demokratycznym, z należytym uwzględnieniem praw podstawowych i uzasadnionych interesów danej osoby fizycznej, aby:
a) uniemożliwić utrudnianie czynności postępowań urzędowych lub sądowych, postępowań przygotowawczych lub procedur;
b) uniemożliwić zakłócanie zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu i ściganiu czynów zabronionych i wykonywaniu kar;
c) chronić bezpieczeństwo publiczne;
d) chronić bezpieczeństwo narodowe;
e) chronić prawa i wolności innych osób.
4. Państwa członkowskie mogą przyjąć akty prawne dla określenia kategorii przetwarzania, które w całości lub części wchodzą w zakres stosowania środków wskazanych w którejkolwiek z liter ust. 3.

danych osobowych, gdy kwestionuje ona ich prawidłowość, której nie da się potwierdzić, lub gdy dane osobowe muszą zostać zachowane do celów dowodowych. W szczególności należy ograniczyć przetwarzanie danych osobowych (zamiast ich usuwania), jeżeli w konkretnym przypadku uzasadnione przesłanki sugerują, że usunięcie mogłoby wpłynąć na uprawnione interesy osoby, której dane dotyczą.

Jeśli zaś chodzi o kwestie dostępu do tego typu danych, to (motyw 44), państwa członkowskie powinny mieć możliwość przyjmowania aktów prawnych pozwalających opóźnić, ograniczyć lub pominąć informowanie osób, których dane dotyczą, lub ograniczyć, w całości lub w części, dostęp tych osób do ich własnych danych osobowych w takim zakresie i przez taki czas, w jakim odnośny środek jest działaniem niezbędnym i proporcjonalnym w społeczeństwie demokratycznym – przy należytym uwzględnieniu praw podstawowych i uzasadnionych interesów danej osoby fizycznej – tak aby uniemożliwić zakłócanie czynności postępowań urzędowych lub sądowych, postępowań przygotowawczych lub czynności procesowych, aby uniemożliwić zakłócanie zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, aby chronić bezpieczeństwo publiczne lub narodowe lub aby chronić prawa i wolności innych osób. Oceny – badając konkretnie i indywidualnie każdy przypadek, czy prawo dostępu powinno zostać częściowo lub całkowicie ograniczone – powinien dokonywać tu administrator.

Jeśli chodzi o problematykę nadzoru, bez którego trudno sobie wyobrazić prawidłową realizację dyrektywy, dyrektywa pozwala na powierzenie tego zadania organom ustanowionych na podstawie RODO (motyw 76), choć może to być więcej niż jeden organ, jeśli wynika to z charakteru, doświadczeń lub przyczyn historycznych (motyw 77). W przypadku rozwiązań krajowych art. 1 ustawy wskazuje, że określa on:

1) zasady i warunki ochrony danych osobowych przetwarzanych przez właściwe organy w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, w tym zagrożeń dla bezpieczeństwa i porządku publicznego, a także wykonywania tymczasowego aresztowania, kar, kar porządkowych i środków przymusu skutkujących pozbawieniem wolności;

2) prawa osób, których dane osobowe są przetwarzane przez właściwe organy w celach, o których mowa w pkt 1, oraz środki ochrony prawnej przysługujące tym osobom;

3) sposób prowadzenia nadzoru nad ochroną danych osobowych przetwarzanych przez właściwe organy w celach, o których mowa w pkt 1, z wyłączeniem danych osobowych przetwarzanych przez prokuraturę i sądy;

4) zadania organu nadzorczego oraz formy i sposób ich wykonania;

5) obowiązki administratora i podmiotu przetwarzającego oraz inspektora ochrony danych i tryb jego wyznaczania;

6) sposób zabezpieczenia danych osobowych;

7) tryb współpracy z organami nadzorczymi w innych państwach Unii Europejskiej;

8) odpowiedzialność karną za naruszenie przepisów niniejszej ustawy.

Już na wstępie (art. 3) znajdujemy jednak dwa wyłączenia (natury systemowej) spod regulacji przewidzianych omawianym aktem. Po pierwsze, ochrona w niej przewidziana nie dotyczy danych osobowych znajdujących się w aktach spraw, m.in.: postępowania w sprawach nieletnich, karnych, karnych skarbowych, wykroczeniowych, czy prokuratorskich. Po drugie jednak, wszystkich danych przetwarzanych w związku z zapewnieniem bezpieczeństwa narodowego, w tym w ramach realizacji zadań ustawowych ABW, AW, SKW, SWW oraz CBA. To drugie wyłączenie zdaje się być poczynione na wyrost. Z formalnego punktu widzenia dyskusyjne jest ono w zestawieniu z treścią art. 13 ust. 3 i art. 15 dyrektywy[21]. Wydaje się natomiast, że da się ono pogodzić z treścią powyżej przywołanego motywu 14 dyrektywy 2016/680[22]. Kłopot w tym wypadku polega bowiem na tym, że o pozbawieniu dostępu do danych w ten sposób gromadzonych powinna przesądzać wyłącznie treść informacji. Przyjęte rozwiązanie nie do końca więc odpowiada normie unijnej. Nie przesądzając, jak w konsekwencji stosowania ustawy rozwiązanie to może zostać ocenione[23], na chwilę obecną wszystkie wymienione służby specjalne nie muszą jednak stosować się do regulacji ustawowej, nawet gdyby zdołano wykazać, że część gromadzonych przez nie informacji (danych) nie jest bezpośrednio związana z zapewnieniem bezpieczeństwa narodowego.

Art. 13 i art. 14 ustawy wyznaczają podstawowe granice dla gromadzenia danych osobowych. Zgodnie z art. 13 ustawy właściwe organy[24] przetwarzają dane osobowe wyłącznie w zakresie niezbędnym dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Oznacza to, że w każdym przypadku

[21] Art. 15 dyrektywy.
1. Państwa członkowskie mogą przyjąć akty prawne pozwalające ograniczyć w całości lub w części prawo dostępu osoby, której dane dotyczą, w takim stopniu i przez taki okres, w jakim takie częściowe lub całkowite ograniczenie jest działaniem niezbędnym i proporcjonalnym w społeczeństwie demokratycznym, z należytym uwzględnieniem praw podstawowych i uzasadnionych interesów danej osoby fizycznej, aby:
a) uniemożliwić utrudnianie czynności postępowań urzędowych lub sądowych, postępowań przygotowawczych lub procedur;
b) uniemożliwić zakłócanie zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar;
c) chronić bezpieczeństwo publiczne;
d) chronić bezpieczeństwo narodowe;
e) chronić prawa i wolności innych osób.
2. Państwa członkowskie mogą przyjąć akty prawne, aby ustalić kategorie przetwarzania, które w całości lub części wchodzą w zakres stosowania ust. 1 lit. a)–e).
3. W przypadkach, o których mowa w ust. 1 i 2, państwa członkowskie zapewniają, by administrator bez zbędnej zwłoki informował pisemnie osobę, której dane dotyczą, o każdej odmowie lub o każdym ograniczeniu dostępu i o przyczynach tej odmowy lub tego ograniczenia. Informacje takie można pominąć, jeżeli ich udzielenie godziłoby w którykolwiek z celów, o których mowa w ust. 1. Państwa członkowskie zapewniają, by administrator informował osobę, której dane dotyczą, o możliwości wniesienia skargi do organu nadzorczego lub środka prawnego do sądu.
4. Państwa członkowskie zapewniają, by administrator dokumentował faktyczne lub prawne powody, na jakich opiera się decyzja. Informacje te udostępnia się organom nadzorczym.

[22] Dyskusyjne jest, na ile powinno to mieć wpływ na ocenę całości regulacji.

[23] Nie można wykluczyć, że w przyszłości może to zostać zweryfikowane na drodze orzecznictwa sądowego i trybunalskiego.

[24] Zgodnie z art. 4 pkt 16 rozumie się przez to organ władzy publicznej, jednostkę organizacyjną lub inny podmiot uprawniony na podstawie odrębnych przepisów do przetwarzania danych osobowych.

organ musi udowodnić, że posiadanie takiej informacji jest niezbędne dla jego działania. Przypomnieć należy, że oznaczać to może również działanie mające na celu:

1) rozpoznawanie, zapobieganie, wykrywanie i zwalczanie czynów zabronionych (w tym zagrożeń dla bezpieczeństwa i porządku publicznego) lub

2) wykonywanie tymczasowego aresztowania, kar, kar porządkowych i środków przymusu skutkujących pozbawieniem wolności.

Ustawodawca dopuszcza jednak przetwarzanie danych osobowych zebranych pierwotnie w jednym z powyższych celów, w innym (nowym) celu, o ile:

1) administratorowi[25] wolno przetwarzać takie dane osobowe na mocy odrębnych przepisów;

2) przetwarzanie jest niezbędne i proporcjonalne na mocy odrębnych przepisów;

3) przepisy prawa zezwalają na ich przetwarzanie;

4) mieści się to w zakresie niezbędnym do ich archiwizacji w interesie publicznym oraz

5) do celów naukowych, statystycznych lub historycznych.

Art. 14 ustawy wyraźnie wskazuje natomiast, że niedopuszczalne jest przetwarzanie danych osobowych ujawniających pochodzenie rasowe, etniczne, poglądy polityczne, przekonania religijne, światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, danych dotyczących seksualności i orientacji seksualnej osoby fizycznej. Są to tzw. dane wrażliwe, które można jednak przetwarzać, jeżeli:

1) przepisy prawa zezwalają na ich przetwarzanie lub

2) jest to niezbędne dla ochrony życia, zdrowia lub interesów osoby, której dane dotyczą, lub innej osoby, lub

3) dane takie zostały upublicznione przez osobę, której dotyczą.

Co ważne, administrator zobowiązany jest nie rzadziej niż co 10 lat dokonywać weryfikacji wszystkich danych osobowych, jeżeli przepisy szczególne tej kwestii nie regulują inaczej (art. 16). Przy czym weryfikacja polegać winna na ocenie, czy dalsze przechowywanie konkretnej informacji jest zbędne. Niezależnie od powyższego, administrator – o ile nie jest to dalece utrudnione lub niemożliwe – przetwarza[26] posiadane dane tak, aby można było rozróżnić, które z nich dotyczą[27]:

[25] Zgodnie z art. 4 pkt 1 rozumie się przez to właściwy organ, który samodzielnie lub wspólnie z innym właściwym organem lub właściwymi organami ustala cele i sposoby przetwarzania danych osobowych, podmiot wskazany przez ustawę jako administrator, jeżeli cele i sposoby przetwarzania danych osobowych są określone w ustawie, albo podmiot wskazany przez prawo Unii Europejskiej albo prawo państwa członkowskiego Unii Europejskiej lub podmiot wyznaczony zgodnie z kryteriami określonymi w prawie tego państwa.

[26] Zgodnie z art. 4 pkt 14 przetwarzanie oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie przez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

[27] Art. 19 ustawy.

1) osób, w stosunku do których istnieją poważne podstawy, aby przypuszczać, że popełniły lub zamierzają popełnić czyn zabroniony;

2) osób skazanych za czyn zabroniony;

3) pokrzywdzonych czynem zabronionym lub osób, w przypadku których określone fakty wskazują, że mogą stać się ofiarami czynu zabronionego;

4) innych osób związanych z czynem zabronionym, takich jak osoby, które mogą zostać wezwane do złożenia zeznań w sprawie czynu zabronionego lub na dalszych etapach postępowania, osoby, które mogą dostarczyć informacji o czynach zabronionych, lub osoby, które mają kontakty lub powiązania z jedną z osób, o których mowa w pkt 1 i 2.

Co istotne, administrator winien również tak przetwarzać dane osobowe, aby można było rozróżnić, które z nich mają swe źródło w faktach, a które w indywidualnych ocenach (art. 20). Intencją tego rozróżnienia jest właśnie materia wiarygodności danych. Szczególnie w obszarze czynności operacyjno-rozpoznawczych jest to często kwestia trudna do jednoznacznego wskazania. Ponieważ jednak z tego typu informacji wyciąga się często dalej idące wnioski, ma to duże znaczenie. Podobnie w przypadku, gdy osoba chciałaby sprostować lub usunąć dane na swój temat, podnosząc argument ich nieprawdziwości. Jeśli dotyczyłoby to danych opartych na faktach (np. rejestrach), inaczej wyglądać będzie droga do ich sprostowania niż w przypadku, gdy są to informacje zasłyszane lub pochodzące z niesprawdzonych źródeł.

Rozdział 4 ustawy, poświęcony prawom osób, na temat których dane są gromadzone i przetwarzane, stanowi w dużej mierze odniesienie wprost do regulacji unijnej. Art. 22 wskazuje na zakres informacji, które administrator przekazuje w razie otrzymania takiego wniosku, a art. 23 reguluje mechanizm dostępu do danych. Z kolei art. 24 i art. 25 odnoszą się do sprostowania, usunięcia lub czasowego ograniczenia przetwarzania danych, jeśli ich prawdziwość jest kwestionowana. Jest to niewątpliwie zmiana jakościowa, bowiem dotychczas nie było klarownych procedur podważania danych gromadzonych przez służby policyjne.

Należy jednak pamiętać, że tak skonstruowane mechanizmy gwarancyjne ulegają znacznemu osłabieniu na mocy art. 26 ustawy, który stanowi, że nie przekazuje się informacji, o których mowa w przepisach niniejszego rozdziału, oraz nie udostępnia się danych osobowych, jeżeli mogłoby to powodować:

1) ujawnienie informacji uzyskanych w wyniku czynności operacyjno-rozpoznawczych;

2) utrudnienie lub uniemożliwienie rozpoznawania, zapobiegania, wykrywania lub zwalczania czynów zabronionych;

3) utrudnienie prowadzenia postępowania karnego, karnego wykonawczego, karnego skarbowego lub w sprawach o wykroczenia lub wykroczenia skarbowe;

4) zagrożenie życia, zdrowia ludzkiego lub bezpieczeństwa i porządku publicznego;

5) zagrożenie bezpieczeństwa narodowego, w tym obronności lub bezpieczeństwa oraz ekonomicznych podstaw funkcjonowania państwa;

6) istotne naruszenie dóbr osobistych innych osób.

Przy czym administrator może przekazać osobie, której dane dotyczą, powyższe informacje w przypadku, gdy ich ujawnienie byłoby niezbędne do ochrony życia lub zdrowia ludzkiego. Mając na względzie kształt wspomnianych przesłanek, widać, że część decyzji o dostępie do danych zależeć będzie od oceny samych funkcjonariuszy. Z drugiej jednak strony ustawa dosyć szeroko odnosi się do kwestii odpowiedzialności administratora za prawidłowość realizacji zadań wynikających z uprawnienia do gromadzenia i przetwarzania tak wrażliwych danych. Poświęcony jest temu zagadnieniu rozdział 5, który kształtując obowiązki administratora (art. 31-38), traktuje także o zasadach zabezpieczania danych (art. 39-45), a wreszcie o wymaganiach i obowiązkach inspektora ochrony danych (art. 46-47), którego administrator musi wyznaczyć. Do zadań inspektora ochrony danych należy:

1) informowanie administratora oraz osób zajmujących się przetwarzaniem o obowiązkach spoczywających na nich na mocy niniejszej ustawy oraz innych przepisów dotyczących ochrony danych;

2) prowadzenie działań podnoszących świadomość oraz organizowanie szkoleń dla osób uczestniczących w operacjach przetwarzania;

3) monitorowanie zgodności przetwarzania danych przez administratora oraz osoby zajmujące się przetwarzaniem danych osobowych z przepisami niniejszej ustawy oraz innymi przepisami dotyczącymi ochrony danych;

4) monitorowanie realizowania polityk administratora w dziedzinie ochrony danych osobowych, w tym przydział na ich podstawie obowiązków dla osób zajmujących się przetwarzaniem;

5) współpraca z Prezesem Urzędu Ochrony Danych;

6) monitorowanie realizacji zaleceń, o których mowa w art. 38 ust. 4, oraz przedstawianie Prezesowi Urzędu stanu ich realizacji;

7) pełnienie funkcji punktu kontaktowego wobec Prezesa Urzędu Ochrony Danych w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 38, oraz prowadzenie z Prezesem Urzędu konsultacji we wszelkich innych sprawach;

8) pełnienie funkcji punktu kontaktowego wobec osób, których dane dotyczą w zakresie przysługujących im praw, o których mowa w rozdziale 4;

9) przygotowywanie zaleceń co do oceny skutków dla ochrony danych osobowych w przypadku, o którym mowa w art. 37, oraz monitorowanie wykonania tych zaleceń;

10) sporządzanie i przekazywanie administratorowi raz na rok, do końca I kwartału za rok ubiegły, sprawozdania z wykonywania zadań z zakresu ochrony i sposobu przetwarzania danych osobowych.

Pamiętać należy również, że na mocy art. 5-12 ustawy to właśnie Prezes Urzędu Ochrony Danych umocowany jest do monitorowania, nadzorowania i kontrolowania sposobu przestrzegania i wykonywania przez służby policyjne norm prawnych w omawianym obszarze.

Reasumując, należy uznać, że przyjęte rozwiązania normatywne z pewnością poszerzają dostęp obywateli do danych gromadzonych na ich temat. Nie powinny przesłaniać tego faktu niektóre regulacje, które w przyszłości mogą być przedmiotem krytycznej oceny, z uwagi na ich stosowanie w praktyce.

Bibliografia

Gawroński M., *Ochrona danych osobowych. Przewodnik po ustawie i RODO ze wzorami*, Warszawa 2018.

Kamińska I., Rozbicka-Ostrowska M., *Ustawa o dostępie do informacji publicznej. Komentarz*, Warszawa 2015.

Opalniński B., Rogalski M., Szustakiewicz P., *Ustawa o Policji. Komentarz*, Warszawa 2015.

Rusinek M., *Z problematyki zakazów dowodowych w postępowaniu karnym*, Warszawa 2019.

Streszczenie: W artykule omówiono podstawowe kwestie związane z wejściem w życie ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, która wymusza na szefach służb policyjnych (administratorach) podniesienie poziomu ochrony danych przez te służby gromadzonych, ale również zwiększa zakres i możliwości dostępu do nich przez osoby, których dane dotyczą. Co więcej, mają one możliwość inicjowania procedury poprawienia lub usunięcia danych błędnych. Samo to uprawnienie wynika nie tylko z treści dyrektywy UE 2016/680, ale przede wszystkim z art. 51 Konstytucji RP.

Słowa kluczowe: ochrona danych osobowych, policja, służby policyjne, gromadzenie informacji

New rules for the collection and protection of personal data by police services

Summary: The article refers to the basic issues related to the entry into force the act of 14th of December 2018 on the protection of personal data processed regarding to the prevention and combating of crime. Due this act chiefs of the police services (administrators) are forced into increase the level of data protection collected by their forces. Also the act is obligated them to increase the scope and possibilities of access to data by persons which are subjects of it. What's more, they have the option of initiating the procedure to correct or delete erroneous data. This possibility is a result not only the EU's Directive 2016/680 but primarily it is fulfillment of the obligation arising from art. 51 of the Polish Constitution.

Keywords: data protection, police, police services, gathering information