ZESZYT PRAWNICZY UAM
2021 • nr 11

DARIA BONIEC-BŁASZCZYK

Doktorantka w Zakładzie Postępowania Karnego
Wydział Prawa i Administracji, Uniwersytet im. Adama Mickiewicza w Poznaniu
https://orcid.org/0000-0002-3273-1188

Ochrona danych osobowych w sprawach karnych a zakres uprawnień przysługujących jednostce w świetle dyrektywy 2016/680 oraz ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości

Wprowadzenie

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań

Zeszyt Prawniczy UAM 11, 2021: 27–43.

przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW[1] w założeniu miała zrewolucjonizować podejście do ochrony danych osobowych w sprawach karnych, tworząc ramy spójnego systemu, którego jednym z głównych filarów miały być wzmocnione uprawnienia przysługujące osobie, której dane dotyczą. Do polskiego systemu prawnego dyrektywa 2016/680 wdrożona została ustawą o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości z dnia 14 grudnia 2018 r.[2]

Celem niniejszego artykułu jest przybliżenie zakresu uprawnień przysługujących jednostce w świetle dyrektywy 2016/680 oraz ustawy implementującej, a także poddanie ich analizie i ocenie w kontekście realizacji założeń dyrektywy co do wzrostu efektywności uprawnień jednostki w ramach systemu ochrony danych osobowych w sprawach karnych.

1. Znaczenie uprawnień przysługujących jednostce dla ochrony jej danych osobowych w sprawach karnych

Dyrektywa 2016/680 jest obok rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 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

[1] Dyrektywa 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 uchylająca decyzję ramową Rady 2008/977/WSISW (Dz.Urz. UE L Nr 119, s. 89), dalej: dyrektywa 2016/680.

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

oraz uchylenia dyrektywy 95/46/WE[3] szczególnym instrumentem dotyczącym ochrony danych osobowych w sprawach karnych wskazującym, że charakter współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej uzasadnia przyjęcie owych szczególnych przepisów regulujących ochronę danych osobowych i swobodny ich przepływ w tych dziedzinach[4].

Podstawowymi celami dyrektywy 2016/680 są ochrona podstawowych praw i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych, oraz zapewnienie swobodnego przepływu danych osobowych między właściwymi organami w ramach całej Unii Europejskiej[5]. Cele te mogą być osiągnięte tylko dzięki wysokiemu stopniowi ochrony danych osobowych osób fizycznych zapewnionemu dzięki harmonizacji przepisów we wszystkich państwach członkowskich, które to przepisy stworzą efektywną ochronę danych osobowych i wyeliminują różnice utrudniające wymianę danych między właściwymi organami[6].

Prawa osób, których dane dotyczą, mają w płaszczyźnie współpracy karnej szczególne znaczenie, ze względu na konieczność utrzymania równowagi pomiędzy prawem do ochrony danych osobowych a koniecznością zachowania poufności w przetwarzaniu danych dla dobra postępowania, zwłaszcza na jego początkowym etapie. Zakres uprawnień przysługujących jednostce zgodnie z dyrektywą 2016/680 obejmuje: dostęp do informacji o organie przetwarzającym i warunkach przetwarzania, dostęp do danych oraz uprawnienia weryfikacyjne, wśród których wyróżnić można prawo do sprostowania lub usunięcia danych osobowych oraz ograniczenia ich przetwarzania.

Podkreślenia wymaga, że cała regulacja dyrektywy 2016/680 dotycząca praw osoby, której dane dotyczą, opiera się na przekonaniu,

---

[3] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L Nr 119, s. 1).

[4] Zob. motyw 10 preambuły dyrektywy 2016/680.

[5] Zob. motyw 93 preambuły dyrektywy 2016/680.

[6] Zob. motywy 7 i 15 preambuły dyrektywy 2016/680.

że każda osoba powinna mieć prawo do informacji i dostępu do danych, aby miała świadomość ich przetwarzania i mogła zweryfikować zgodność tego przetwarzania z prawem.

Powyższe okoliczności rodzą wiele pytań, w tym o to, czy możliwe jest pogodzenie konieczności przetwarzania danych osobowych dla celów wykrywania i ścigania czynów zabronionych z zapewnieniem realnych środków ochrony osobom, których dane dotyczą, a przede wszystkim czy implementowana do polskiego systemu prawnego regulacja daje taką możliwość.

2. Prawo dostępu do informacji o organie przetwarzającym i warunkach przetwarzania danych

Podstawowym uprawnieniem jednostki z zakresu ochrony danych osobowych jest prawo dostępu do informacji o organie przetwarzającym dane i o warunkach ich przetwarzania.

Zgodnie z art. 13 ust. 1 dyrektywy 2016/680 administrator obowiązany jest udostępniać osobie, której dane dotyczą, przynajmniej następujące informacje: tożsamość i dane kontaktowe administratora, w razie potrzeby dane kontaktowe inspektora danych osobowych, cele przetwarzania, do których mają posłużyć dane, informacje o prawie wniesienia skargi do organu nadzorczego i dane kontaktowe organu nadzorczego oraz informacje o prawie żądania od administratora dostępu do danych, ich sprostowania, usunięcia lub ograniczenia ich przetwarzania. Powyższe informacje powinny być łatwo dostępne (np. na stronie internetowej administratora danych) i sformułowane w jasny, zrozumiały sposób, w prostym języku[7].

Z perspektywy administratora danych przepis ten reguluje obowiązek informacyjny, tj. obowiązek przekazania osobie, której dane dotyczą, podstawowych informacji o organie przetwarzającym i warunkach przetwarzania danych. Z perspektywy osoby, której dane dotyczą, jest to zaś jedna z głównych gwarancji autonomii informacyjnej

[7] Zob. motywy 39 i 42 preambuły dyrektywy 2016/680.

jednostki, w tym gwarancji dla wykonywania przyznawanych jej uprawnień kontrolnych[8]. Z tego powodu do uzyskania rzeczonego zakresu informacji jednostka zawsze jest uprawniona, a obowiązek ten nie może zostać ograniczony czy pominięty.

Ponadto, w konkretnych przypadkach, jeżeli udzielenie takich informacji jest konieczne dla zagwarantowania rzetelnego przetwarzania danych, administrator ma również obowiązek przekazania jednostce dalszych informacji dotyczących podstawy prawnej przetwarzania, okresu przechowywania danych osobowych lub gdy nie jest to możliwe, kryteriów służących określeniu tego okresu, kategorii odbiorców danych osobowych, w tym odbiorców w państwach trzecich lub organizacjach międzynarodowych, a w razie potrzeby także dalszych informacji, zwłaszcza gdy dane osobowe są zbierane bez wiedzy osoby, której dotyczą (art. 13 ust. 2 dyrektywy 2016/680).

Jednakże odnośnie do wspomnianych dodatkowych informacji dyrektywa 2016/680 w art. 13 ust. 3 statuuje możliwość przyjęcia przez państwa członkowskie przepisów pozwalających opóźnić, ograniczyć lub pominąć informowanie osoby w takim zakresie i przez taki czas, w jaki jest to konieczne i proporcjonalne, np. aby: uniemożliwić utrudnianie czynności postępowań urzędowych i sądowych, postępowań przygotowawczych lub procedur, uniemożliwić zakłócanie zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu i ściganiu czynów zabronionych i wykonywaniu kar, chronić bezpieczeństwo publiczne, chronić bezpieczeństwo narodowe bądź prawa i wolności innych osób. Dodatkowo zgodnie z art. 13 ust. 4 państwa mogą przyjąć także przepisy dla określenia kategorii przetwarzania, które w całości lub w części wchodzą w zakres stosowania środków wskazanych powyżej.

Regulacja zawarta w art. 13 dyrektywy 2016/680 jest zatem najlepszym przykładem deklarowanego w tym akcie wyważenia interesów jednostki w zakresie ochrony danych osobowych i interesów organów ścigania.

---

[8] P. Litwiński, P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2018, s. 364.

Unormowanie to należy zestawić z art. 22 ust. 1–3 i art. 26 ustawy, które implementują omawiane przepisy dyrektywy 2016/680 do polskiego porządku prawnego. Przepis art. 22 ust. 1 określa zestandaryzowane obowiązki informacyjne realizowane niezależnie od wniosku osoby, której dane dotyczą, i niezależnie od konkretnej sytuacji, tworząc katalog podstawowy informacji przekazywanych przez administratora, odpowiadający art. 13 ust. 1 dyrektywy 2016/680[9]. Z kolei art. 22 ust. 3 ustawy – tak jak art. 13 ust. 2 dyrektywy 2016/680 – tworzy katalog rozszerzony informacji, jakie przekazywane są osobie, której dane dotyczą, w konkretnych przypadkach, a więc wówczas, gdy jest to konieczne dla zapewnienia rzetelnego przetwarzania danych tej osoby, w celu umożliwienia wykonywania przysługujących jej praw[10]. Ustawa utrzymuje więc zastosowany w dyrektywie 2016/680 podział obowiązków informacyjnych na dwie kategorie, lecz nie realizuje głównego celu ich podziału przyjętego w instrumencie unijnym. Jest tak, gdyż owym głównym celem było stworzenie podstawowego, zawsze dostępnego dla podmiotu, katalogu informacji o organie przetwarzającym dane i warunkach ich przetwarzania, a obok niego katalogu rozszerzonego, co do którego obowiązek informacyjny może zostać wyłączony. Tymczasem art. 26 ustawy daje możliwość wyłączenia wszystkich obowiązków informacyjnych, w tym tych podstawowych, o których mowa w art. 22 ust. 1 ustawy, podczas gdy dyrektywa 2016/680 nie przewiduje w ogóle takiej możliwości.

W kontekście powyższego prawo dostępu do informacji o organie przetwarzającym i warunkach przetwarzania statuowane w art. 13 dyrektywy 2016/680 oraz art. 22 ust. 1–3 ustawy należy uznać za podstawowe uprawnienie, które realnie powinno przyczyniać się do wzrostu świadomości jednostek w zakresie warunków przetwarzania danych oraz dalszych uprawnień przysługujących im w związku

[9] M. Gumularz, P. Kozik, *Komentarz do art. 22*, [w:] A. Grzelak (red.), *Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Komentarz*, Legalis/el. 2019, nb. 1–2.

[10] Ibidem.

z przetwarzaniem danych w celach wykrywania i ścigania czynów zabronionych. Z tego też powodu negatywnie należy ocenić regulację zawartą w art. 22 ust. 1 w zw. z art. 26 ustawy, pozwalającą na wyłączenie obowiązku informacyjnego w odniesieniu do wszelkich informacji przekazywanych osobie, której dane dotyczą. Takie unormowanie przeczy istocie wyodrębnienia podstawowego katalogu obowiązków informacyjnych, naruszając gwarancję autonomii informacyjnej jednostki.

3. Prawo dostępu do danych osobowych

Kolejnym, znacznie dalej idącym uprawnieniem jednostki w zakresie ochrony danych osobowych jest prawo do uzyskania od administratora danych informacji, czy przetwarzane są dane jej dotyczące, a jeżeli takie dane są przetwarzane – prawo dostępu do tych danych oraz informacji o ich przetwarzaniu.

Uprawnienie to wyrażone zostało w art. 14 dyrektywy 2016/680 i osadza się na wskazaniu osobie, której dane dotyczą, jakie jej dane osobowe są przetwarzane, oraz podaniu wszelkich dostępnych informacji o ich pochodzeniu, a nadto na przekazaniu danej osobie informacji o celach i podstawie prawnej przetwarzania, kategoriach danych, odbiorcach lub kategoriach odbiorców, którym dane zostały ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych, w miarę możliwości o planowanym okresie przechowywania danych lub gdy nie jest to możliwe, o kryteriach służących określeniu tego okresu, informacji o prawie żądania od administratora sprostowania lub usunięcia danych lub ograniczenia przetwarzania danych dotyczących tej osoby, informacji o prawie wniesienia skargi do organu nadzorczego oraz danych kontaktowych tego organu.

Realizacja tego uprawnienia powinna nastąpić poprzez przekazanie jednostce pełnego podsumowania danych w zrozumiałej formie (np. w formie kopii przetwarzanych danych). Jeśli jednak przekazywane informacje obejmują wiadomości o pochodzeniu danych

osobowych, nie powinny one ujawniać tożsamości osób fizycznych, w szczególności poufnych źródeł informacji[11], co koresponduje z możliwością uzyskiwania przez organy informacji także w sposób niejawny[12].

Dostęp do danych jest warunkiem świadomości osoby, której dane są przetwarzane, że w jej przypadku przetwarzanie danych rzeczywiście następuje, co z kolei jest zasadnicze dla możności zweryfikowania zgodności tego przetwarzania z prawem. Prawo dostępu do danych ma zatem dla osoby, której dane są przetwarzane, potrójne znaczenie: pozwala poznać dane osobowe jej dotyczące, które są przetwarzane, umożliwia sprawdzenie ich prawidłowości i zapewnia weryfikowalność zgodności tego przetwarzania z prawem. Stwierdzić zatem trzeba, że omawiane prawo jest jednym z najistotniejszych uprawnień kształtujących prawo do ochrony danych osobowych i powinno być rozpatrywane w kontekście zagwarantowania jednostce możliwości obrony jej praw wobec administratora danych, znajdującego się zwykle w pozycji uprzywilejowanej[13].

Prawo dostępu do danych może jednak zostać ograniczone w całości lub w części w przypadkach wskazanych w art. 15 dyrektywy 2016/680. Ograniczenie może nastąpić w takim stopniu i przez taki okres, w jakim jest działaniem niezbędnym i proporcjonalnym w społeczeństwie demokratycznym, przy należytym uwzględnieniu praw podstawowych i uzasadnionych interesów danej osoby fizycznej, w jednym z wymienionych przez dyrektywę 2016/680 celów, w tym uniemożliwienia utrudniania czynności postępowań urzędowych i sądowych. Dodatkowo w myśl art. 15 ust. 2 dyrektywy 2016/680 państwa mogą przyjąć przepisy określające kategorie przetwarzania, które w całości lub w części wchodzą w zakres tych celów.

Ograniczenie prawa dostępu nie powinno być przy tym dokonywane *a priori*, gdyż w motywie 44 preambuły dyrektywy 2016/680

---

[11] Zob. zalecenie zawarte w motywie 43 preambuły dyrektywy 2016/680.

[12] Zob. np. art. 20 Ustawy o Policji z dnia 6 kwietnia 1990 r. (t.j. Dz.U. z 2017 r., poz. 2067).

[13] M. Jagielski, *Prawo do ochrony danych osobowych. Standardy europejskie*, Warszawa 2010, s. 119.

zasugerowano, że administrator powinien dokonywać oceny, badając konkretnie i indywidualnie każdy przypadek i dopiero potem decydować o ewentualnym wyłączeniu prawa dostępu do danych[14].

Jednakże, co do zasady, w przypadku ograniczenia prawa dostępu administrator danych winien bez zbędnej zwłoki pisemnie poinformować osobę, której dane dotyczą, o każdej odmowie lub ograniczeniu dostępu i o przyczynach tej odmowy lub ograniczenia. Biorąc jednak pod uwagę cele ograniczenia dostępu, także powyższe informacje można pominąć, jeżeli ich udzielenie godziłoby w którykolwiek z tych celów (art. 15 ust. 3 dyrektywy 2016/680). W każdym wypadku administrator danych obowiązany jest jednak do dokumentowania faktycznych lub prawnych powodów, na jakich opiera się decyzja, a informacje te udostępnia się organom nadzorczym (art. 15 ust. 4 dyrektywy 2016/680). Administrator powinien również każdorazowo w takiej sytuacji poinformować osobę, której dane dotyczą, o możliwości wniesienia skargi do organu nadzorczego lub środka prawnego do sądu (art. 15 ust. 3 dyrektywy 2016/680).

Właściwe implementowanie regulacji art. 14 i 15 dyrektywy 2016/680 do polskiego porządku prawnego wymagało przyjęcia przepisów, które z jednej strony zapewnią realne prawo dostępu do danych gromadzonych w odniesieniu do konkretnej osoby, a z drugiej prawidłowo uregulują procedurę w przypadku odmowy udzielenia dostępu do danych, ograniczenie prawa dostępu w sprawach karnych musi bowiem mieć miejsce, przynajmniej w pewnym zakresie, ze względu na charakter przetwarzanych danych i cel tego przetwarzania. Całokształt przepisów rozdziału czwartego ustawy (dotyczący praw osoby, której dane dotyczą) świadczy o tym, że polski ustawodawca temu trudnemu zadaniu w pełni nie podołał.

W pierwszej kolejności należy zauważyć, że przepis art. 14 dyrektywy 2016/680 zapewniający prawo dostępu do danych w ustawie został włączony do dwóch przepisów – art. 22 ust. 4 i art. 23 ustawy. Doprowadziło to do symbolicznego rozdzielenia prawa do informacji o przetwarzaniu danych (w tym do uzyskania informacji o parametrach przetwarzania) wyrażonego w art. 22 ust. 4 ustawy

[14] Zob. motyw 44 preambuły dyrektywy 2016/680.

(tzw. zindywidualizowanego obowiązku informacyjnego[15]) oraz prawa dostępu do samych danych, co umożliwia art. 23 ustawy. Uprawnienie to w sposób oczywisty wiąże się z obowiązkiem administratora danych udostępnienia lub przekazania osobie, której dane dotyczą, kopii tych danych lub sporządzonego w przystępnej formie wyciągu z tych danych (art. 23 ust. 2 ustawy).

Jak wskazano powyżej, najistotniejsze w tym zakresie było jednak właściwe uregulowanie procedury odmowy udzielenia zindywidualizowanych informacji o przetwarzaniu danych oraz odmowy dostępu do tych danych. Ograniczenie prawa dostępu z art. 15 dyrektywy 2016/680 implementowano w art. 26 ustawy[16], zgodnie z którym obowiązki informacyjne oraz inne prawa podmiotu, w tym prawo dostępu do danych, nie będą realizowane, jeżeli mogłoby to spowodować m.in. ujawnienie informacji uzyskanych w wyniku czynności operacyjno-rozpoznawczych czy utrudnienie lub uniemożliwienie rozpoznawania, zapobiegania, wykrywania lub zwalczania czynów zabronionych. Prawidłowość implementacji powyższego uregulowania budzi wiele zastrzeżeń zgłaszanych już w piśmiennictwie[17]. Za najpoważniejszą wadę ustawowej regulacji należy uznać zupełne pominięcie w art. 26 tzw. przesłanek wstępnych wprowadzenia ograniczeń w prawach osoby, której dane dotyczą, na które wskazuje art. 15 ust. 1 i art. 13 ust. 3 dyrektywy 2016/680. Zgodnie z dyrektywą 2016/680 wprowadzanie ograniczeń musi być konieczne i proporcjonalne w społeczeństwie demokratycznym, w sposób należyty powinno uwzględniać prawa podstawowe i uzasadnione interesy danej osoby fizycznej, a także ma chronić wartości wskazane w art. 15 ust. 1 i art. 13 ust. 3. Tymczasem w świetle art. 26 ustawy odwołanie się do przywołanego testu proporcjonalności przy ograniczaniu praw osoby, której dane dotyczą, nie jest w ogóle konieczne. Omawiany przepis

[15] M. Gumularz, P. Kozik, *Komentarz do art. 22*, nb. 40 i n.

[16] Doprecyzowania wymaga, że art. 26 ustawy implementuje dwa przepisy dyrektywy 2016/680 – zarówno art. 13 ust. 3–4, jak i art. 15, i co za tym idzie, łączy przesłanki występujące w obu przepisach dyrektywy 2016/680, co budzi wątpliwości dotyczące prawidłowości ich implementacji, zob. M. Gumularz, P. Kozik, *Komentarz do art. 26*, [w:] A. Grzelak (red.), *Ustawa o ochronie danych osobowych*…, nb. 3 i n.

[17] Zob. M. Gumularz, P. Kozik, *Komentarz do art. 26*, nb. 13.

daje administratorowi danych niezwykle dużą swobodę w ocenie dopuszczalności i zasadności wyłączenia praw osoby, której dane dotyczą, również ze względu na połączenie w przepisie art. 26 ustawy przesłanek z przepisów art. 13 ust. 3 i art. 15 ust. 1 dyrektywy 2016/680 oraz zawężenie pojęcia prawa lub wolności innych osób do życia i zdrowia ludzkiego oraz istotnego naruszenia dóbr osobistych innych osób.

Dyrektywa 2016/680 wprowadza *novum* w zakresie ciążącego na administratorze danych obowiązku uzasadnienia odmowy lub ograniczenia dostępu do danych, dokumentowania podstaw tych decyzji i informowania osoby, której dane dotyczą, w postaci możliwości wniesienia skargi do organu nadzorczego lub środka prawnego do sądu, a także możliwości dostępu do danych za pomocą organu nadzorczego na mocy art. 17 dyrektywy 2016/680. Zgodnie z art. 23 ust. 3 ustawy administrator ma obowiązek poinformować osobę, której dane dotyczą, o przyczynach odmowy lub ograniczenia dostępu oraz o możliwości wniesienia do organu nadzorczego skargi w przypadku naruszenia praw osoby w wyniku przetwarzania jej danych. Choć ustawa nie stanowi o tym wprost, należy przyjąć, że powyższe informacje można pominąć, jeżeli ich udzielenie godziłoby w którykolwiek z tych celów (art. 15 ust. 3 dyrektywy 2016/680 oraz art. 26 ustawy), jednakże w takiej sytuacji administrator zawsze powinien poinformować osobę, której dane dotyczą, o możliwości wniesienia skargi do organu nadzorczego lub środka prawnego do sądu (art. 15 ust. 3 dyrektywy 2016/680 i art. 23 ust. 3 ustawy). W każdym przypadku administrator danych obowiązany jest jednak do dokumentowania faktycznych lub prawnych przyczyn odmowy lub ograniczenia dostępu do danych, a informacje te udostępnia się Prezesowi UODO na jego wniosek (art. 23 ust. 4 ustawy).

Jednoznacznie negatywnie należy ocenić zrezygnowanie przez ustawodawcę z implementacji art. 17 dyrektywy 2016/680, który podmiotowi danych daje możliwość wykonywania części swoich praw w przypadkach określonych w art. 13 ust. 2, art. 15 ust. 3 i art. 16 ust. 4 za pośrednictwem organu nadzorczego. Zgodnie z dyrektywą 2016/680 administrator ma obowiązek poinformowania osoby, której dane dotyczą, o możliwości wykonywania przysługujących jej

praw za pośrednictwem organu nadzorczego (art. 17 ust. 2 dyrektywy 2016/680). Jednocześnie organ nadzorczy, przejmując wykonywanie uprawnień, ma obowiązek informować osobę o fakcie weryfikacji danych lub przeglądach oraz prawie do wnoszenia właściwych środków prawnych (art. 17 ust. 3 dyrektywy 2016/680). Ustawa przewiduje zaś jedynie możliwość wniesienia skargi do Prezesa UODO, jeżeli dane są przetwarzane niezgodnie z prawem (art. 29 w zw. z art. 50 ust. 1 dyrektywy 2016/680).

Z powyższych przyczyn, a w szczególności z powodu błędnej implementacji konstrukcji wyłączenia praw osoby, której dane dotyczą, z przepisów art. 13 ust. 3 i art. 15 ust. 1 dyrektywy 2016/680 do art. 26 ustawy, faktyczne realizowanie prawa dostępu osób, których dane dotyczą, w istocie będzie zależało od praktyki stosowania omawianych przepisów.

4. Prawo do sprostowania lub usunięcia danych osobowych oraz ograniczenia ich przetwarzania

Kolejnymi uprawnieniami jednostki z zakresu ochrony danych osobowych są określone w art. 16 dyrektywy 2016/680: prawo do sprostowania danych osobowych, prawo do ich usunięcia oraz prawo do ograniczenia przetwarzania danych. Uprawnienia te mają charakter kontrolny, są uzupełnieniem prawa dostępu do danych. Umożliwiają podjęcie przez osobę, której dane dotyczą, właściwej reakcji na przekazane jej informacje o przetwarzanych danych w zakresie ich prawdziwości i zgodności przetwarzania z prawem. Podmiotem obowiązanym do sprostowania, usunięcia lub ograniczenia przetwarzania danych jest ich administrator.

W przypadku nieprawidłowości obowiązek administratora sprowadza się do sprostowania danych bez zbędnej zwłoki, a w przypadku, gdy dane są niekompletne, do ich uzupełnienia, co może nastąpić na podstawie przedstawionego przez osobę, której dane dotyczą, dodatkowego oświadczenia (art. 16 ust. 1 dyrektywy 2016/680). Zgodnie z art. 24 ust. 1 pkt 1 ustawy osoba, której dane dotyczą, może wystąpić z wnioskiem do administratora o niezwłoczne uzupełnienie,

uaktualnienie lub sprostowanie danych – jeśli dane te są niekompletne, nieaktualne lub nieprawdziwe. Sprostowaniu nie podlegają jednak dane zawarte np. w treści zeznań świadka[18]. Wówczas administrator pozostawia dokument zawierający zeznanie, wypowiedź czy oświadczenie osoby fizycznej w postaci niezmienionej, umieszczając na nim stosowną adnotację (art. 24 ust. 3 ustawy). Oczywiście w przypadku sprostowania danych na administratorze będzie ciążył obowiązek poinformowania organu, od którego zaczerpnął dane, o ich nieprawidłowości (art. 16 ust. 5 i art. 25 ust. 2 ustawy).

Prawo do usunięcia danych powiązane jest z przepisami dyrektywy 2016/680 dotyczącymi zasad przetwarzania danych (art. 4 dyrektywy 2016/680), o konieczności zapewnienia przez państwo zgodności przetwarzania danych z prawem, m.in. poprzez przyjęcie przepisów określających powody przetwarzania oraz dane podlegające przetwarzaniu i cele przetwarzania (art. 8 dyrektywy 2016/680) oraz o przetwarzaniu szczególnych kategorii danych osobowych (art. 10 dyrektywy 2016/680). Powyższe przepisy dyrektywy 2016/680 wyznaczają przesłanki usunięcia przetwarzanych danych. W sytuacji, w której przetwarzanie danych naruszać będzie przepisy krajowe przyjęte na podstawie regulacji dyrektywy 2016/680 lub jeżeli dane osobowe będą musiały zostać usunięte w celu wypełnienia obowiązku prawnego ciążącego na administratorze, osoba, której dane dotyczą, ma prawo uzyskać od administratora usunięcie jej danych bez zbędnej zwłoki (art. 16 ust. 2 i art. 24 ust. 1 pkt 2 dyrektywy 2016/680).

Zamiast usunięcia danych administrator zgodnie z dyrektywą 2016/680 powinien ograniczyć przetwarzanie danych w dwóch przypadkach: gdy osoba, której dane dotyczą, kwestionuje prawidłowość danych, a ich prawidłowości lub nieprawidłowości nie można stwierdzić, a także gdy dane osobowe muszą zostać zachowane do celów dowodowych (art. 16 ust. 3 i art. 25 ust. 1 ustawy). Ograniczenie przetwarzania danych polega na przetwarzaniu ich tylko w celu, który zapobiegł usunięciu danych. Jako metody ograniczonego przetwarzania danych wskazuje się przeniesienie danych do innego systemu przetwarzania, np. do celów archiwizacyjnych, albo uniemożliwienie

[18] Zob. motyw 47 preambuły dyrektywy 2016/680.

użytkownikom dostępu do tych danych, a w zautomatyzowanych zbiorach danych ograniczenie przetwarzania powinno być zapewnione środkami technicznymi. Fakt ograniczenia przetwarzania danych należy w jasny sposób zaznaczyć w systemie[19].

W przypadku dokonania sprostowania, usunięcia lub ograniczenia przetwarzania danych na administratorze ciąży obowiązek powiadomienia o tym odbiorców danych, którzy zobowiązani są wówczas do podjęcia takich samych czynności wobec uzyskanych przez nich danych (art. 16 ust. 5 i art. 25 ust. 3 ustawy).

Natomiast w przypadku odmowy sprostowania, usunięcia lub ograniczenia przetwarzania danych dyrektywa 2016/680 nakłada na administratora danych obowiązek pisemnego poinformowania o tym osoby, której dane dotyczą, wraz z podaniem przyczyn tej odmowy. Także jednak w tym przypadku możliwe jest przyjęcie przez państwo przepisów wyłączających w całości lub w części obowiązek udzielania takich informacji dla ochrony wymienionych w instrumencie wartości. W takim przypadku administrator danych obowiązany jest do poinformowania jednostki o możliwości wniesienia skargi do organu nadzorczego lub środka prawnego do sądu (art. 16 ust. 4 dyrektywy 2016/680). Powyższa regulacja wdrożona została do ustawy w art. 24 ust. 6, art. 26 ust. 1 i art. 29 ustawy.

Uprawnienia jednostki wyartykułowane w przepisie art. 16 dyrektywy 2016/680 i wdrożone do polskiego porządku prawnego w postaci art. 24 i 25 ustawy niewątpliwie wzmacniają sytuację prawną osoby fizycznej w zakresie jej uprawnień kontrolnych. Oczywiście również w tym zakresie ustawodawca nie wdrożył całościowo regulacji dyrektywy 2016/680, gdyż art. 24 ustawy nie odwołuje się w ramach prawa do usunięcia danych do sytuacji, o której mowa w art. 16 ust. 2 dyrektywy 2016/680 (usunięcia danych w celu wypełnienia obowiązku prawnego ciążącego na administratorze). Jednakże mimo powyższego implementowane przepisy zapewniają czynny udział osoby, której dane dotyczą, w kontroli nad informacjami o niej, co stanowi przejaw realnej ochrony danych, na jaką osoba zainteresowana sama ma wpływ. Wprowadzone na płaszczyźnie prawa krajowego przepisy

[19] Zob. motyw 47 preambuły dyrektywy 2016/680.

ustawowe zachowują niezbędny balans, z jednej bowiem strony przyznają jednostce możliwość wpływania na dane jej dotyczące, które są przetwarzane, z drugiej zaś nie niweczą przy tym zadań w zakresie zapobiegania i ścigania przestępczości.

Podsumowanie

Jak wskazano na wstępie, dyrektywa 2016/680 miała zrewolucjonizować podejście do ochrony danych osobowych w sprawach karnych. Daleko idące uprawnienia osób, których dane dotyczą, wraz ze środkami prawnymi je wspomagającymi w założeniu mają dawać podmiotowi danych większą kontrolę nad dotyczącymi go informacjami zbieranymi przez organy w sprawach karnych. Znaczenie uprawnień przyznanych przez dyrektywę 2016/680 jeszcze bardziej wzrasta, jeżeli uświadomimy sobie, jak wiele danych osobowych jest gromadzonych i przetwarzanych do celów zapobiegania i ścigania przestępczości i od jak wielu podmiotów mogą one pochodzić.

Wydaje się jednak, że w polskim systemie prawnym rewolucja w zakresie danych osobowych w sprawach karnych nie nastąpiła. Przyczyn tego należy upatrywać w niepełnej implementacji dyrektywy 2016/680. Oprócz zarysowanych w artykule problemów z pełnym wdrożeniem wszystkich uprawnień jednostki największą przeszkodę we wzroście znaczenia ochrony danych osobowych w sprawach karnych stanowi ograniczony zakres ustawy, wyłączający jej zastosowanie do ochrony danych osobowych znajdujących się w aktach spraw lub czynności lub urządzeniach ewidencyjnych, prowadzonych na podstawie enumeratywnie wymienionych w tym artykule ustaw (m.in. Ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego[20], art. 3 pkt 1). Z tego też powodu w odniesieniu do danych zgromadzonych w postępowaniach prowadzonych na podstawie ustaw, o których mowa w art. 3 pkt 1 ustawy, prawa osób, których dane dotyczą, są wykonywane wyłącznie na podstawie i w zakresie

[20] Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (t.j. Dz.U. z 2021 r., poz. 534).

przewidzianym przez przepisy regulujące te postępowania (art. 27 dyrektywy 2016/680). Próżno jednak obecnie szukać w przedmiotowych ustawach jakichkolwiek regulacji dotyczących uprawnień osób, których dane są przetwarzane, i zasad, na jakich mogą być one wykonywane. Należy przy tym zwrócić uwagę, że dyrektywa 2016/680 w art. 18 daje jedynie możliwość dostosowania, a nie całkowitego wyłączenia praw jednostki w ramach postępowań przygotowawczych i sądowych.

W konsekwencji w ramach postępowań karnych *sensu largo*, do których zastosowanie znajduje dyrektywa 2016/680, muszą istnieć przepisy statuujące uprawnienia jednostki z zakresu danych osobowych i umożliwiające realizację praw osób, których dane są przetwarzane. Kwestia ta wymaga zatem pilnego uregulowania przez ustawodawcę. Do tego czasu otwarta pozostaje możliwość stosowania przepisów Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[21], częściowo utrzymanych w mocy na podstawie art. 175 Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych i art. 107 ustawy[22], chyba że zgodnie z regułą pierwszeństwa prawa unijnego możliwe będzie bezpośrednie zastosowanie dyrektywy 2016/680 wobec jej nieimplementowania do krajowego porządku prawnego w zakreślonym terminie oraz przyznania jednostkom przez przepisy dyrektywy 2016/680 prawa w relacji wobec państwa, które były przede wszystkim jasne i bezwarunkowe[23].

---

[21] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r., poz. 922).

[22] Tak: A. Grzelak, *Komentarz do art. 107*, [w:] A. Grzelak (red.), *Ustawa o ochronie danych osobowych…*, nb. 2. Odmienne stanowisko zajmuje P. Liwszic, *Komentarz do art. 3*, [w:] P. Liwszic, T. Ochocki, Ł. Pociecha (red.), *Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Komentarz*, Legalis/el. 2019, nb. 12.

[23] Szerzej na temat bezpośredniego skutku dyrektywy zob. m.in.: K. Wójtowicz, *Bezpośredni skutek przepisów prawa wspólnotowego w porządku prawnym RP*, „Kwartalnik Prawa Publicznego" 2004, nr 4/2, s. 43–70; M. Domańska, *Implementacja dyrektyw przez sądy krajowe*, Warszawa 2014, s. 23–74.

Personal data protection in criminal cases and the range of rights of the data subject in the light of Directive 2016/680 and the act on the protection of personal data processed in connection with the prevention and combating of crime

Summary

The subject of the article is an issue of the protection of personal data in criminal cases in the context of the range of rights of the data subject in the light of Directive 2016/680 and the act on the protection of personal data processed in connection with the prevention and combating of crime.

The article presents the relevance of data subjects' rights for the protection of personal data in criminal cases in the light of the fundamental objectives of Directive 2016/680. The main part of the article is an analysis, to which the individual rights established by Directive 2016/680 are subjected: the right of access to information about the processing authority and the conditions of data processing, the right of access to data, the right to rectification, erasure or restriction of data processing, as well as legal remedies, by comparing the model provided by Directive 2016/680 with the Polish regulation.