

MARIA HAPUNIK

Komenda Wojewódzka Policji w Białymstoku

Zakres uprawnień służb państwowych do przetwarzania informacji w celu zapobiegania przestępstwom i ich zwalczania na przykładzie Policji

Zwalczanie zagrożeń bezpieczeństwa i zapobieganie im wymaga zastosowania przez współczesne państwo mechanizmów ochrony informacji. Działania takie przebiegają dwutorowo. Z jednej strony chroniona jest wiedza służb państwowych, która jest nieustannie zdobywana i służyć ma szeroko rozumianemu zagwarantowaniu bezpieczeństwa czy zwalczaniu przestępczości. Z drugiej strony państwo tworzy nowe gwarancje ochrony prywatności obywateli. Ciążące na ustawodawcy zobowiązanie zagwarantowania praw oraz wolności sprowadza się do zakazu nadmiernej ingerencji, dotyczy to przede wszystkim niejawnego pozyskiwania informacji, jak również na umożliwieniu swobodnego korzystania z tych wolności. Nie ulega wątpliwości, że to właśnie równowaga pomiędzy tymi gwarancjami buduje poczucie bezpieczeństwa w państwie. Wiadomo jednak, że jawność i prywatność często pozostają w konflikcie. Zarówno rozwój technologiczny, przykładowo związany z rewolucją elektroniczną, jak i przemiany społeczne są tak dynamiczne, że próg „niezbędnych” ograniczeń prywatności rzeczywiście jest trudny do określenia w dłuższej perspektywie czasowej.

Ochronę prywatności gwarantują przepisy ustawy zasadniczej, nie znaczą się w nich jednak wprost ograniczeń, które wynikają z tytułu jawności. Artykuł 49 Konstytucji RP określa wolność i ochronę komunikowania się, w artykule 50 – „zapewnia się nienaruszalność mieszkania”. Konstytucja ogranicza

rodzaj pozyskiwanych, gromadzonych i udostępnianych przez organy państwowe informacji – nie można tego czynić w stosunku do „innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym”, ponadto do ich ujawnienia może zobowiązywać wyłącznie ustawa. Stwierdzenie, co oznacza „niezbędne”, jest trudne przy podejmowaniu prób interpretacyjnych.

W 2018 r. w Polsce doszło do istotnych zmian w ramach regulacji prawnych dotyczących ochrony informacji oraz danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Warto na początku zwrócić uwagę na regulacje, które miały bezpośredni wpływ na obecny kształt systemu prawnego Unii Europejskiej w tym zakresie. Organizacją, która jako pierwsza wypracowała porozumienie w zakresie ochrony danych osobowych, jest Rada Europejska. Była to Konwencja Nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu dnia 28 stycznia 1981 r.¹ Powyższa Konwencja reguluje omawiany obszar wraz z Protokołem dodatkowym o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych dotyczącym organów nadzoru i transgranicznych przepływów danych, sporządzonym w Strasburgu dnia 8 listopada 2001 r.² oraz Protokołem zmieniającym Konwencję Nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzonym w Strasburgu dnia 10 października 2018 r. Ustawa z dnia 16 października 2019 r. o ratyfikacji Protokołu zmieniającego Konwencję Nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzonego w Strasburgu dnia 10 października 2018 r.³ obowiązuje od grudnia 2019 r. Prezydent RP podpisał ustawę 8 listopada 2019 r. Konwencja nr 108 została opracowana pod auspicjami Rady Europy jako pierwsza umowa międzynarodowa dotycząca ochrony danych osobowych w kontekście przestrzegania prawa do prywatności. Wprowadziła ona mechanizmy ochrony osób przed naruszeniami, jakie mogą mieć miejsce w związku z gromadzeniem i automatycznym przetwarzaniem danych osobowych oraz uregulowała kwestię przepływu danych osobowych przez granice państw. Polska stała się jej stroną 1 września 2002 r.⁴ Fenomenalny rozwój technologii oraz zmiany w systemach

¹ Dz.U. z 2003 r., poz. 25.

² Dz.U. z 2006 r., poz. 15.

³ Dz.U. z 2019 r., poz. 2284.

⁴ <https://uodo.gov.pl/pl/454> [dostęp 22.02.2020].

prawnych w odniesieniu do ochrony danych osobowych zdeterminowały istotne modernizacje w tekście konwencji nr 108. Wzmocnione zostały w niej m.in. standardy ochrony związane z przetwarzaniem danych ze względów bezpieczeństwa narodowego ze wskazaniem niezależnej oraz skutecznej kontroli i nadzoru w tym obszarze. Powyższe regulacje mają szeroki zakres podmiotowy i przedmiotowy, normujący system ochrony danych osobowych, również tych przetwarzanych przez organy ścigania i wymiar sprawiedliwości. Należy zwrócić jednak uwagę na przepis art. 9 ust. 1 oraz art. 11 konwencji nr 108, które dopuszczają wprowadzenie odstępstw od zasad ogólnych na rzecz utrzymania bezpieczeństwa publicznego oraz zwalczania przestępczości, jak również wyłączeń dla prowadzonych postępowań karnych. Podwaliny prawnej ochrony autonomii informacyjnej jednostki w systemie europejskim ukształtowała Konwencja o ochronie praw człowieka i podstawowych wolności z 4 listopada 1950 r.⁵ Przepisem, który reguluje prawo do prywatności, do poszanowania życia prywatnego i rodzinnego, jak również prawo do ochrony danych osobowych, jest art. 8 Konwencji.

Poza umowami międzynarodowymi wiążącymi państwa – strony tych umów – duże znaczenie miały również rezolucje (zalecenia) Komitetu Ministrów, z których niektóre dotyczą również ochrony danych osobowych⁶. Należy postrzegać ich jako zespół wytycznych stanowiących punkt odniesienia dla ustawodawcy tworzącego prawo krajowe i w szczególności dla krajowych organów stosujących prawo, które posługują się nimi przy dokonywaniu wykładni prawa krajowego⁷. W omawianej tematyce najbardziej istotna wydaje się Rekomendacja R (87)15 o ochronie danych osobowych wykorzystywanych w sektorze policji z dnia 17 września 1987 r., która dotyczy przetwarzania danych w systemie informatycznym (kraje członkowskie mają prawo rozszerzyć te ochronę na dane przetwarzane ręcznie). W 2018 r. komitet konsultacyjny, pracujący nad zmianami w konwencji nr 108, opracował praktyczny przewodnik w sprawie wykorzystywania danych osobowych w sektorze policji⁸. Rekomendację kilkakrotnie oceniano pod

⁵ Dz.U. z 1993 r., poz. 284 ze zm.

⁶ *Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Komentarz*, red. A. Grzelak, Wyd. C.H.Beck, Warszawa 2019, s. 8.

⁷ Tamże.

⁸ Zob. dokument z dnia 15 lutego 2018 r. T-PD(2018)01, Consultative Committee of the Convention for the Protection of Individuals with regard to automatic processing of personal data,

kątem jej modernizacji, jednak uznano, że nie ma potrzeby wprowadzania do niej znaczących zmian. Według omawianego zalecenia dane zbierane na potrzeby policji powinny być ograniczone w niezbędnym zakresie w celu zapobiegania konkretnemu niebezpieczeństwu bądź zwalczania konkretnego przestępstwa. Ponadto zwrócono uwagę na konieczności oddzielenia zbiorów danych opartych na faktach od danych, które opierają się na subiektywnych opiniach i indywidualnych ocenach. W rekomendacji istnieje również zalecenie, aby przetwarzanie danych osobowych w Policji nadzorował niezależny organ.

Rozwój systemu ochrony danych osobowych w Unii Europejskiej (wcześniej Wspólnoty Europejskiej) był ograniczony ze względu na jej strukturę oraz odmienności systemu prawnego. Regulacje tego obszaru w zakresie współpracy sądowej i policyjnej obejmował filar III, natomiast przetwarzanie danych osobowych zostało uregulowane w obszarze podlegającym zasadom I filaru Unii Europejskiej, które wynikały z dyrektywy ogólnej w sprawie ochrony danych (dyrektywa 95/46/WE). Od momentu jej przyjęcia ukształtowało się całe *acquis*: prawodawstwo [można w tym miejscu wymienić dyrektywy szczegółowe, regulujące problematykę ochrony danych w szczególnych obszarach, jak np. dyrektywę 2000/31/WE Parlamentu Europejskiego i Rady z 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym)⁹, czy chociażby dyrektywę 2002/58/WE Parlamentu Europejskiego i Rady z 12 lipca 2002 r. dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)]¹⁰, przez instytucje [Grupa Robocza 29 (obecnie to Europejska Rada Ochrony Danych – EROD)] czy też Europejski Inspektor Ochrony Danych (EIOD)], zostało też wypracowane orzecznictwo Trybunału Sprawiedliwości¹¹. Nie należy pomijać regulacji odnoszących się do Systemu Informacyjnego Schengen drugiej generacji (SIS II)¹², europejskiego nakazu

Practical guide on the use of personal data in the police sector, <https://rm.coe.int/practical-guide-use-of-personal-data-in-the-police-sector/1680789a74> [dostęp 24.02.2020].

⁹ Dz.Urz. UE L 178 z 17.07.2000 r., s. 1.

¹⁰ Dz.Urz. UE L 201 z 31.07.2002 r. ze zm., s. 37.

¹¹ *Ustawa o ochronie...*, red. A. Grzelak, dz. cyt., s. 10.

¹² Rozporządzenie (WE) nr 1987/2006 – utworzenie, funkcjonowanie i użytkowanie Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz.Urz. UE L 381 z 28.12.2006 r.), s. 4, Decyzja

aresztowania (ENA)¹³, Europolu¹⁴, Eurojustu¹⁵ czy dyrektywy PNR¹⁶. W 2008 r. przyjęta została Decyzja ramowa Rady 2008/977/WSiSW z 27.11.2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych¹⁷. Akt prawny regulował zasady przetwarzania danych osobowych w relacjach transgranicznych pomiędzy państwami Unii Europejskiej. Dyrektywa nie regulowała form przetwarzania danych, miała ogólny charakter, pomimo innych pierwotnych założeń powstałych w obliczu potrzeb wprowadzenia znowelizowanych regulacji jako odpowiedzi na nowe metody przetwarzania i nowe formy współpracy pomiędzy organami UE. Omawiana dyrektywa w Polsce została implementowana Ustawą z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi¹⁸, znacząco zmienioną po wejściu w życie Ustawy z dnia 10 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości¹⁹.

Wejście w życie w dniu 1 grudnia 2009 r. Traktatu z Lizbony²⁰ pozwoliło państwom członkowskim na bardziej równomierny rozwój współpracy w dziedzinie zarówno systemu ochrony, jak i dostępu uprawnionych służb do informacji i danych osobowych. Należy zwrócić uwagę, że to dzięki zniesieniu struktury

2007/533/WSiSW – utworzenie, funkcjonowanie i użytkowanie Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz.Urz. UE L 205 z 07.08.2007 r.), s. 63.

¹³ Decyzja ramowa Rady z dn. 13 czerwca 2002 r. w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między Państwami Członkowskimi (Dz.Urz. WE L 190 z 18.7.2002 r.), s. 1.

¹⁴ Konwencja sporządzona na podstawie artykułu K.3 Traktatu o Unii Europejskiej w sprawie ustanowienia Europejskiego Urzędu Policji (Konwencja o Europolu), sporządzona w Brukseli dnia 26 lipca 1995 r. (Dz.U. z 2005 r. Nr 29, poz. 243).

¹⁵ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1727 z dnia 14 listopada 2018 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych (Eurojust) oraz zastąpienia i uchylenia decyzji Rady 2002/187/WSiSW (Dz.Urz. UE L 295 z 21.11.2018 r.), s. 138.

¹⁶ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (Dz.Urz. UE L 119 z 4 maja 2016 r.), s. 3.

¹⁷ Dz.Urz. UE L 350 z 30.12.2008 r., s. 60.

¹⁸ Dz.U. z 2018 r., poz. 484 ze zm.

¹⁹ Dz.U. z 2019 r., poz. 125.

²⁰ Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską (Dz.Urz. C 306 z 17.12.2007 r.).

trójfilarowej ustanowiona została jedna wspólna podstawa dla ochrony danych osobowych. System filarowy został zastąpiony jednolitym reżimem prawnym, Unia uzyskała osobowość prawną. Do Traktatu o funkcjonowaniu Unii Europejskiej²¹ wprowadzony został art. 16, który zagwarantował zmiany systemowe w omawianym obszarze, przede wszystkim ustanawiając indywidualne prawo podmiotu danych do ochrony jego danych osobowych. Wejście w życie Traktatu z Lizbony spowodowało nadanie statusu prawa pierwotnego Karcie Praw Podstawowych Unii Europejskiej (dalej: KPP), przyznano jej charakter prawnie wiążący. KPP została proklamowana w Nicei w dniu 7 grudnia 2000 r. Po wejściu w życie Traktatu z Lizbony jej pierwotną wersję poddano redakcji, a następnie została ona ponownie uchwalona przez Komisję Europejską, Radę i Parlament Europejski. Postanowienia dotyczące ochrony autonomii informacyjnej jednostki zawarte są w art. 7 i 8 KPP. Prawo do ochrony danych osobowych jest niezmiennie związane z prawem do poszanowania życia prywatnego ustanowionym w art. 7 KPP. Treść art. 8 KPP oparta jest – jak wynika z objaśnień Sekretariatu Konwencji redagującej KPP – na tekście art. 16 TFUE, Dyrektywie 95/46/WE, art. 8 EKPCz oraz konwencji nr 108²². Jednocześnie stwierdza się tam dość lakonicznie, że Dyrektywa 95/46/WE i Rozporządzenie (WE) 45/2001 „zawierają warunki i ograniczenia stosowane w wykonywaniu prawa do ochrony danych osobowych”²³. Wspomniane powyżej artykuły 8 KPP oraz 16 TFUE stanowiły podstawę prawną do przyjęcia nowych norm w zakresie ochrony danych osobowych, dotyczących współpracy policyjnej i sądowej w sprawach karnych. Komisja, przygotowując projekt dyrektywy, w związku z treścią deklaracji nr 21²⁴, miała do wyboru dwie opcje: albo mogła przedstawić jeden, spójny, ustanawiający standardy tekst, który będzie określał zasady ogólne przetwarzania danych w UE, albo – odmiennie – kontynuować rozróżnienie między podejściem ogólnym a podejściem szczególnym dla spraw związanych z bezpieczeństwem wewnętrznym i zwalczaniem

²¹ Dz.Urz. UE 2016 C 202, s. 1.

²² A. Gajda, *Ochrona danych osobowych i kierunki zmian w tej dziedzinie w prawie Unii Europejskiej*, „Kwartalnik Kolegium Ekonomiczno-Społecznego Studia i Prace” / OW SGH 2014, nr 4, s. 77.

²³ Tamże.

²⁴ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej”, COM(2010)609 final.

przestępczości²⁵. Komisja zdecydowała się na drugi wybór ze względu na szczególny charakter regulowanego obszaru. Przemawiały za tym różne potrzeby, w tym przechowywanie danych przez długi czas, konieczność porównywania i analizowania posiadanych danych z napływającymi, czy zagwarantowanie braku dostępu do informacji określonej grupie osób do danych na swój temat, np. osobom podejrzanym. Ponadto uregulowanie zasad ochrony danych osobowych w dwóch aktach prawnych – rozporządzeniu i dyrektywie – uwzględniło zwiększony margines swobody państw członkowskich UE w kształtowaniu regulacji dotyczących funkcjonowania organów państwowych zwalczających przestępczość. 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 uchyłająca decyzję ramową Rady 2008/977/WSiSW²⁶ uchwalona została w tym samym dniu, razem z RODO – 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)²⁷. Termin implementacji dyrektywy został wyznaczony na 5 maja 2016 r., lecz polski ustawodawca nie dotrzymał tego terminu, uchwalając ustawę o ochronie danych osobowych przetwarzanych w związku ze zwalczaniem i zapobieganiem przestępczości w dniu 14.12.2018 r.²⁸.

Transpozycja dyrektywy 2016/680 nie mogła polegać wyłącznie na uchwaleniu powyższej ustawy, koniecznym było wprowadzenie licznych zmian w przepisach sektorowych. W rozdziale 9 ustawy o ochronie danych osobowych przetwarzanych w związku ze zwalczaniem i zapobieganiem przestępczości zawarto przepisy zmieniające 42 ustawy. W większości zmienianych ustaw dostosowuje się legislacyjnie przepisy do zmian w zakresie funkcjonowania Prezesa

²⁵ *Ustawa o ochronie...*, red. A. Grzelak, dz. cyt., s. 17-18.

²⁶ Dz.Urz. UE L 194 z 19.07.2016 r., s. 1.

²⁷ Dz.Urz. UE L 119 z 04.05.2016 r., s. 1 ze zm.

²⁸ Dz.U. z 2019 r., poz. 125.

UODO oraz prawidłowych odesłań do aktualnie obowiązujących ustaw²⁹. Poza tym jednak uchwalone zmiany dotyczą przede wszystkim wskazania administratora, okresu retencji danych, nadzoru nad przetwarzaniem danych czy wyłączenia stosowania niektórych przepisów RODO³⁰. Największy zakres obejmują zmiany w Ustawie z dnia 6 kwietnia 1990 r. o Policji³¹, zawarte w art. 58 omawianej ustawy. Znowelizowany został art. 1 ust. 2 pkt 8, który ustanawia podstawowe zadanie Policji do przetwarzania informacji kryminalnych, w tym danych osobowych. Kompetencję tę wprost wymienia art. 20 ust. 1 ustawy o Policji: „W celu realizacji zadań ustawowych Policja jest uprawniona do przetwarzania informacji, w tym danych osobowych, z zachowaniem ograniczeń wynikających z art. 19 (zarządzenie kontroli operacyjnej)”.

Przetwarzanie informacji, w tym danych osobowych, może odbywać się za pomocą środków technicznych, zakres danych określa art. 14 ust. 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Policja ma prawo przetwarzać dane osobowe, o których mowa w art. 9 i 10 RODO, wyłączając dane dotyczące kodu genetycznego. Omawiana ustawa dodaje przepisy, które pozwalają Policji w ramach wykonywanych czynności operacyjno-rozpoznawczych, dochodzeniowo-śledczych i administracyjno-porządkowych (art. 15 ust. 1 pkt 5a) obserwować i rejestrować przy użyciu środków technicznych obrazy zdarzeń w miejscach publicznych, a w przypadku czynności operacyjno-rozpoznawczych i administracyjno-porządkowych podejmowanych na podstawie ustawy – także i dźwięk towarzyszący tym zdarzeniom (art. 15 ust. 1 pkt 5b³²). Policjanci mogą obserwować i rejestrować przy użyciu środków technicznych obraz lub dźwięk w trakcie interwencji w miejscach innych niż publiczne, podczas prowadzenia działań kontrterrorystycznych oraz wspierania działań jednostek organizacyjnych Policji przez służbę kontrterrorystyczną w warunkach szczególnego zagrożenia lub wymagających użycia specjalistycznych sił i środków oraz specjalistycznej taktyki działań, a także w policyjnych środkach transportu. Okres przechowywania danych, uzyskanych podczas

²⁹ *Ustawa o ochronie...*, red. A. Grzelak, dz. cyt., s. 511.

³⁰ Tamże.

³¹ Dz.U. z 2020 r., poz. 360.

³² Art. 58 Ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r., poz. 125).

wykonywania czynności, o których mowa w art. 15 ust. 1 pkt 5a i 5 b ustawy o Policji, to co najmniej 30 dni, nie dłużej jednak niż 60 dni od dnia ich zarejestrowania. Informacje uzyskane podczas czynności operacyjno-rozpoznawczych podlegają zniszczeniu po okresie przechowywania do 60 dni, z tym, że termin przechowywania liczy się od dnia zakończenia tych czynności. Kolejna istotna zmiana to nadanie uprawnienia do pobierania i udostępniania danych telekomunikacyjnych, pocztowych i internetowych także organom ścigania państw członkowskich UE i innych państw, agencjom UE, które zajmują się zapobieganiem i zwalczaniem przestępczości oraz Międzynarodowej Organizacji Policji Kryminalnej – Interpolu, na ich wniosek, jeżeli następuje to w celu wykrywania przestępstw oraz ścigania ich sprawców, ratowania zdrowia lub życia ludzkiego albo poszukiwania osób zaginionych (art. 20 c ust. 8 ustawy o Policji).

Efektywne wypełnianie zadań ustawowych w zakresie zapobiegania i zwalczania przestępczości przez Policję jest zależne od możliwości dysponowania przez tę służbę odpowiednim zasobem informacji. Trzon uprawnień Policji stanowią przepisy art. 15 oraz 19-21nb. Szczególnym uprawnieniem Policji jest prowadzenie czynności operacyjno-rozpoznawczych, które poprzedzają co do zasady postępowanie przygotowawcze, gdy stanowią podstawę do jego wszczęcia, jak również często prowadzone są równoległe do tego postępowania. Czynności te można prowadzić także po umorzeniu postępowania przygotowawczego na podstawie przepisu art. 325f §2 k.p.ksgj.pl (niewykrycie sprawców).

Czynności operacyjno-rozpoznawcze umocowane są ustawą o Policji oraz w niejawnym zarządzeniu nr pf – 1 Komendanta Głównego Policji z dnia 3 stycznia 2019 r. w sprawie metod i form wykonywanych przez Policję czynności operacyjno-rozpoznawczych (niepublikowane). Prawo podejmowania czynności operacyjno-rozpoznawczych przysługuje Policji na podstawie art. 14 ust. 1 ustawy o Policji: „W granicach swych zadań Policja wykonuje czynności: operacyjno-rozpoznawcze, dochodzeniowo-śledcze i administracyjno-porządkowe w celu: rozpoznawania, zapobiegania i wykrywania przestępstw, przestępstw skarbowych i wykroczeń; poszukiwania osób ukrywających się przed organami ścigania lub wymiaru sprawiedliwości, zwanych dalej »osobami poszukiwanymi«; poszukiwania osób, które na skutek wystąpienia zdarzenia uniemożliwiającego ustalenie miejsca ich pobytu należy odnaleźć w celu zapewnienia ochrony ich życia, zdrowia lub wolności, zwanych dalej »osobami zaginionymi«”.

Do ustawowo uregulowanych czynności operacyjno-rozpoznawczych zaliczyć należy przepisy art. 19 ust. 1 – kontrola operacyjna, art. 19a – zakup kontrolowany, kontrolowane wręczenie lub przyjęcie korzyści i sprzedaż kontrolowana, art. 19b – przesyłka niejawnie nadzorowana oraz art. 20c – żądanie od przedsiębiorców telekomunikacyjnych danych retencyjnych. Do uregulowanych w ustawie o Policji czynności operacyjno-rozpoznawczych zaliczyć trzeba także wykorzystanie dokumentów legalizacyjnych – art. 20a oraz art. 22 – współpraca z osobami niebędącymi policjantami, udzielającymi pomocy Policji.

Pozyskiwanie przez nieuprawnione osoby (czy to ze służb wywiadowczych innego państwa, czy grup przestępczych) informacji, które mają wpływ na bezpieczeństwo danego państwa (czyli jego niepodległość, suwerenność oraz pozycję na arenie międzynarodowej), może mieć daleko idące konsekwencje³³. Dlatego, by zachować stabilność państwa i dawać poczucie bezpieczeństwa obywatelom, najważniejszym obowiązkiem rządu jest ochrona informacji³⁴. Współcześnie informacja przekazywana jest niezwykle szybko i w dodatku do nieograniczonej liczby odbiorców. Nowe normy prawne chroniące informację powstają z opóźnieniem w stosunku do rozwoju technologii informacyjno-komunikacyjnych. Obecnie zasoby informacji chronione są szczególnie w kontekście podejmowania decyzji algorytmicznych, które są istotne w związku z rozwojem w krajach rozwiniętych sztucznej inteligencji. W stosunku do obywateli źródłami zagrożenia są cyberprzestępcy zajmujący się „kradzieżą” cudzej tożsamości czy firmy profilujące konsumentów. Nie ustaje również dyskusja kontestująca legalne działania służb państwowych wykorzystujących potencjał ICT³⁵ do swoich potrzeb. Niedopuszczalne jest, by służby państwowe działały na szkodę obywateli, dlatego tak ważna jest kwestia kontroli ich działalności i nadzoru nad nimi.

Informacja jest zatem produktem cennym, chronionym zarówno systemami fizycznymi jak i teleinformatycznymi. Państwo rozszerza normy prawne zabezpieczające prywatność obywateli, jednak skuteczna walka z szeroko pojętymi zagrożeniami wymaga dostępu służb państwowych do tajemnic. Wkraczanie w strefę wolności i praw człowieka jest możliwe wyłącznie na podstawie ustaw kompetencyjnych poszczególnych służb państwowych oraz ich niejawnych instrukcji.

³³ S. Topolewski, *Ochrona informacji niejawnych w Siłach Zbrojnych Rzeczypospolitej Polskiej*, Wyd. Nauk. UPH, Siedlce 2017, s. 353.

³⁴ Tamże.

³⁵ ICT – technologie informacyjno-komunikacyjne.

W Dokumencie roboczym nr 1 w sprawie amerykańskich i unijnych programów nadzoru oraz ich wpływu na podstawowe prawa obywateli UE stwierdza się, że „postęp techniczny jest jednym z czynników mających wpływ na zasadniczą zmianę modelu działania i praktyk służb specjalnych, które odeszły od tradycyjnej koncepcji ukierunkowanego nadzoru, stanowiącego konieczny i proporcjonalny środek zwalczania terroryzmu, i skierowały się ku systemom nadzoru prowadzonego na skalę masową”³⁶. Zdaniem autorki nie jest możliwe zapobieganie i zwalczanie zagrożeń bez szerokich uprawnień służb państwowych, szczególnie biorąc pod uwagę rozwój cyberprzestrzeni. Skuteczność służb nie jest możliwa bez odpowiednich norm prawnych, narzędzi oraz specjalistycznie wykształconej kadry. W Polsce istnieje przestrzeń w działaniu państwa, którą powinna wypełnić służba specjalna do prowadzenia wywiadu zarówno CYBER HUMINT, jak i SIGINT. Według doniesień prasowych³⁷ jest szansa, aby taka służba specjalna, zajmująca się wywiadem elektronicznym i cyberbezpieczeństwem kraju, powstała. Współcześnie służby państwowe gromadzą i wykorzystują informacje nie tylko przedstawiające wartość dowodową w prowadzonych postępowaniach. W ramach proaktywnych strategii, prowadzonych w związku z działaniami kontr- i antyterrorystycznymi czy ze zwalczaniem przestępczości zorganizowanej dane zbierane są prewencyjnie. Oczywiście dyskusja na temat równoważenia działań inwigilacyjnych i chroniących prywatność obywateli jest potrzebna. To dzięki protestom, m.in. organizacji pozarządowych, służby państwowe są poddane koniecznej w państwie demokratycznym kontroli społecznej.

Bibliografia

Akty prawne

Decyzja 2007/533/WSiSW – utworzenie, funkcjonowanie i użytkowanie Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz.Urz. UE L 205 z 07.08.2007 r.).

Decyzja ramowa Rady 2008/977/WSiSW z 27.11.2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (Dz.Urz. UE L 350 z 30.12.2008 r.).

³⁶ Parlament Europejski, Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych, Sprawozdawca Claude Moraes, 11.12.2013 r. (DT\1012434PL.doc), s. 2.

³⁷ <https://forsal.pl/artykuly/906998,nowa-sluzba-specjalna-w-polsce-wywiad-elektroniczny-na-sluch-radioelektroniczny-program-pis.html> [dostęp 28.03.2020].

Decyzja ramowa Rady z dnia 13 czerwca 2002 r. w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między Państwami Członkowskimi (Dz.Urz. WE L 190 z 18.7.2002 r.).

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 uchyłająca decyzję ramową Rady 2008/977/WSiSW (Dz.Urz. UE L 194 z 19.07.2016 r.).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (Dz.Urz. UE L 119 z 4 maja 2016 r.).

Konwencja Nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu dnia 28 stycznia 1981 r.

Konwencja sporządzona na podstawie artykułu K.3 Traktatu o Unii Europejskiej w sprawie ustanowienia Europejskiego Urzędu Policji (Konwencja o Europolu), sporządzona w Brukseli dnia 26 lipca 1995 r. (Dz.U. z 2005 r. Nr 29, poz. 243).

Protokół dodatkowy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych dotyczący organów nadzoru i transgranicznych przepływów danych, sporządzony w Strasburgu 8 listopada 2001 r. (Dz.U. z 2006 r., poz. 15).

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 119 z 04.05.2016 r. ze zm.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1727 z dnia 14 listopada 2018 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych (Eurojust) oraz zastąpienia i uchylenia decyzji Rady 2002/187/WSiSW (Dz.Urz. UE L 295 z 21.11.2018 r.).

Rozporządzenie (WE) nr 1987/2006 – utworzenie, funkcjonowanie i użytkowanie Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz.Urz. UE L 381 z 28.12.2006 r.).

Traktat o funkcjonowaniu Unii Europejskiej (Dz.Urz. UE z 2016 r. C 202).

Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską podpisany w Lizbonie 13 grudnia 2007 (Dz.Urz. UE z 2007 r. C 306/1).

Ustawa z dnia 16 października 2019 r. o ratyfikacji Protokołu zmieniającego Konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzonego w Strasburgu dnia 10 października 2018 r. (Dz.U. z 2019 r., poz. 2284).

Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz.U. z 2020 r., poz. 360).

Ustawa z dnia 10 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r., poz. 125).

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

Ustawa z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi (Dz.U. z 2018 r., poz. 484 ze zm.).

Dokumenty

Consultative Committee of the Convention for the Protection of Individuals with regard to automatic processing of personal data – Practical guide on the use of personal data in the police sector, dokument z dnia 15 lutego 2018 r. T-PD(2018)01, <https://rm.coe.int/practical-guide-use-of-personal-data-in-the-police-sector/1680789a74>.

Dokument roboczy nr 1 w sprawie amerykańskich i unijnych programów nadzoru oraz ich wpływu na podstawowe prawa obywateli UE Parlament Europejski, Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych, Sprawozdawca Claude Moraes, 11.12.2013 r. (DT\1012434PL.doc).

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej”, COM(2010)609 final.

Opracowania

Gajda A., *Ochrona danych osobowych i kierunki zmian w tej dziedzinie w prawie Unii Europejskiej*, „Kwartalnik Kolegium Ekonomiczno-Społecznego Studia i Prace” / OW SGH 2014, nr 4.

Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Komentarz, red. A. Grzelak, Wyd. C.H. Beck, Warszawa 2019.

Topolewski S., *Ochrona informacji niejawnych w Siłach Zbrojnych Rzeczypospolitej Polskiej*, Wyd. Nauk. UPH, Siedlce 2017.

Źródła internetowe

<https://forsal.pl/artykuly/906998,nowa-sluzba-specjalna-w-polsce-wywiad-elektroniczny-nasluch-radioelektroniczny-program-pis.html> [dostęp 28.03.2020].

<https://uodo.gov.pl/pl/454> [dostęp 22.02.2020].

<https://rm.coe.int/practical-guide-use-of-personal-data-in-the-police-sector/1680789a74> [dostęp 24.02.2020].

The scope of powers of law enforcement to process information in order to determine and fight crime

Summary: The purpose of this article is to present normative elements concerning national law enforcement information processing, including personal data, to prevent and combat crime. Legal acts regulating information processing in activities of state services are discussed, using the Police as a case study. The author tries to underline the necessity of surveillance activities undertaken by state services in situations of largely understood threats prevention.

Keywords: *security, personal data protection, data processing by police, crime prevention, police intelligence operations*