Do druku nr 516

GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH
dr Edyta Bielak-Jomaa

Warszawa, dnia 10 maja 2016 r.

DOLiS-033-133/16/KK

Pan
Adam Podgórski
Zastępca Szefa Kancelarii Sejmu RP
ul. Wiejska 4/6/8
00-902 Warszawa

Szanowny Panie Ministrze,

w odpowiedzi na pismo z dnia 18 maja 2016 r. (sygn. GMS-WP-173-138/16, data wpływu do Biura GIODO: 23 maja br.) dotyczące **rządowego projektu ustawy o działaniach antyterrorystycznych oraz o zmianie niektórych innych ustaw (Druk sejmowy nr 516, dalej zwany projektem)**, uprzejmie informuję, iż Generalny Inspektor Ochrony Danych Osobowych – z punktu widzenia przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r. poz. 2135, z późn. zm., zwanej dalej ustawą) – **zgłasza następujące uwagi.**

W pierwszej kolejności podnieść należy, że **projekt nie został przedłożony przez Ministra Spraw Wewnętrznych i Administracji do zaopiniowania przez Generalnego Inspektora Ochrony Danych Osobowych** w toku prac rządowych. Organ do spraw ochrony danych osobowych przedstawił z własnej inicjatywy uwagi do tego projektu w dniu 12 maja br.[1]

Na pochwałę natomiast zasługuje inicjatywa P. Witolda Kołodziejskiego, Sekretarza Stanu w Ministerstwie Cyfryzacji dot. konsultacji z Generalnym Inspektorem poprawek Ministra Cyfryzacji do projektu w zakresie obowiązku rejestracji tzw. kart pre-paid. Stanowisko organu zostało przedstawione w dniu 9 maja[2].

Odnosząc się do całości projektu Generalny Inspektor ponownie zwraca uwagę na kwestię braku zapewnienia zewnętrznej kontroli przetwarzania danych przez Agencję Bezpieczeństwa Wewnętrznego sprawowanej przez niezależny, autonomiczny organ. Generalny

[1] DOLiS-033-133/16/TG/41198
[2] DOLiS-033-133/16/TG/39816

tel. 531 03 00
fax. 531 03 01

Inspektor Ochrony Danych Osobowych nie przesądza, jaki podmiot mógłby być właściwy do sprawowania takiej kontroli. Jednocześnie wskazuje, iż zapewnienie istnienia tego rodzaju kontroli jest obowiązkiem ustawodawcy, zwłaszcza w świetle stanowiska wyrażonego w wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 roku (Sygn. akt K 23/11). W opinii organu do spraw ochrony danych osobowych prowadzone w Sejmie Rzeczypospolitej Polskiej prace dotyczące projektu wydają się najbardziej prawidłowym momentem dla podjęcia działań legislacyjnych zmierzających do powołania podmiotu zapewniającego niezależną, zewnętrzną kontrolę przetwarzania danych przez wszystkie służby specjalne (ewentualnie nadania kompetencji do sprawowania takiej kontroli jakiemuś podmiotowi już istniejącemu) tym bardziej, że Generalnemu Inspektorowi Ochrony Danych Osobowych nie nie jest wiadomym na temat kontynuowania, podjętych przez Ministerstwo Spraw Wewnętrznych w 2013 roku, prac dotyczących projektu *ustawy o Komisji Kontroli Służb Specjalnych*[3] czy też projektu ustawy regulującej funkcjonowanie Agencji Bezpieczeństwa Wewnętrznego, które toczyły się w 2014 r.[4]

Przechodząc do uwag szczegółowych podkreślić trzeba, że były one konsekwentnie podnoszone przez Generalnego Inspektora Ochrony Danych Osobowych podczas poprzednich procesów legislacyjnych. Niestety, niżej zamieszczone uwagi organu do spraw ochrony danych osobowych nie zyskały akceptacji ze strony projektodawcy.

I tak organ do spraw ochrony danych osobowych ponownie wskazuje, iż **w projekcie brak jest unormowań określających zasady dokonywania przez Agencję Bezpieczeństwa Wewnętrznego weryfikacji przydatności przetwarzanych przez nią danych.** W projekcie nie powtórzono nawet rozwiązania przeniesionego do poprzednich projektów z ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym. (t.j. Dz. U. z 2014 r. poz. 1411 z późn. zm., dalej zwanej **ustawą o CBA**). Zgodnie z nim Agencja Bezpieczeństwa Wewnętrznego dokonywałaby weryfikacji potrzeby dalszego przetwarzania zebranych danych osobowych nie rzadziej niż co 5 lat. W opinii Generalnego Inspektora Ochrony Danych Osobowych brak nawet tak „szczątkowej" regulacji tego istotnego zagadnienia nie może być uznany za wystarczający dla zapewnienia skutecznej ochrony – gwarantowanych konstytucyjnie – praw obywateli.

Odnosząc się do art. 6 ust. 4 projektu za wysoce kontrowersyjne uznać trzeba zaproponowane rozwiązania. Podkreślenia wymaga, iż Generalny Inspektor Ochrony Danych Osobowych nie neguje potrzeby koordynacji i intensyfikacji działań służb specjalnych mających na

[3] https://legislacja.rcl.gov.pl/projekt/181401/katalog/181409#181409. DOLiS-033-442/13/71667
[4] Druk sejmowy nr 2295 (http://www.sejm.gov.pl/sejm7.nsf/PrzebiegProc.xsp?id=8E126F417E079EB7C1257CBA00279B51). DOLiS-033-337/13/TG/41198

celu przeciwdziałanie tak groźnemu rodzajowi przestępczości, jakim jest przestępczość o charakterze terrorystycznym, i zwalczanie tej przestępczości. Nie oznacza to jednak zgody organu do spraw ochrony danych osobowych na wprowadzanie konstrukcji prawnych, które budzą uzasadnione wątpliwości co do ich zgodności z – określoną w Konstytucji Rzeczypospolitej Polskiej – hierarchią źródeł prawa. Przypomnieć wypada, że – zgodnie z art. 93 ust. 2 Konstytucji Rzeczypospolitej Polskiej – „Zarządzenia są wydawane tylko na podstawie ustawy. Nie mogą one stanowić podstawy decyzji wobec obywateli, osób prawnych oraz innych podmiotów." W tym kontekście konstytucyjnym nie wydaje się dopuszczalną, przyjęta w art. 6 ust. 4 projektu, konstrukcja, w myśl której niemal wszystkie regulacje dotyczące prowadzenia wykazu osób mogących mieć związek z przestępstwami o charakterze terrorystycznym (zakres informacji gromadzonych w wykazie, sposób prowadzenia wykazu, tryb uzyskiwania informacji zawartych w wykazie) znajdą się w niejawnym zarządzeniu Szefa ABW. Warto zwrócić uwagę, że uprzednio krytykowana była przez Generalnego Inspektora propozycja regulowania omawianej kwestii przez zarządzenia Prezesa Rady Ministrów. W obydwu przypadkach regulacja ustawowa zostaje ograniczona do kwestii istnienia przedmiotowego wykazu (art. 6 ust. 1 projektu) i ogólnego wskazania organów, którym informacje z tego wykazu są przekazywane (art. 6 ust. 2 i 3 projektu). Trudno racjonalnie przyjąć, iż fakt umieszczenia danej osoby w wykazie osób mogących mieć związek z przestępstwami o charakterze terrorystycznym nie będzie skutkować podejmowaniem przez polskie organy władzy publicznej określonych decyzji wobec tej osoby. Nie można także pominąć konstytucyjnej zasady prymatu ustawy jako podstawowego źródła prawa krajowego (**Rozdział III Konstytucji RP**). Koniecznym jest także zwrócenie uwagi na **art. 51 Konstytucji RP**, w którym określono zasady i ograniczenia zbierania informacji o osobach. **Zgodnie z ust. 5 zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa. Dotyczy to zarówno obywateli Polski jak i cudzoziemców.**

W art. 8 ust. 4 projektu zaproponowano, by Szef ABW niezwłocznie zawiadamiał Ministra Koordynatora Służb Specjalnych oraz Prokuratora Generalnego o zarządzeniu wobec osoby niebędącej obywatelem polskim niejawnego prowadzenia czynności określonych w ust. 1 komentowanego przepisu. Jeżeli miałaby to być namiastka systemu kontroli nad czynnościami prowadzonymi wobec osób, to wydaje się zasadnym, aby Prokurator Generalny miał dostęp do informacji, które doprowadziły do wydania zarządzenia wobec danej osoby. W przeciwnym razie nie będzie miał on wiedzy niezbędnej celem nakazania zaprzestania czynności. Na taką ograniczoną obecnie rolę mogą wskazywać kolejne przepisy art. 8, w których określono, iż Prokurator Generalny jest informowany o wynikach czynności i zgromadzonych materiałach (art. 8 ust. 6 i 7) celem zarządzenia zniszczenia zbędnych materiałów uzyskanych w wyniku czynności. Prokurator

Generalny powinien mieć dostęp do informacji, które doprowadziły do wydania zarządzenia, o którym mowa w ust. 1. Z drugiej strony należy wskazać, iż osoba, wobec której prowadzone były czynności nie jest o tym fakcie informowana w żaden sposób, nawet po zakończeniu czynności. Stanowi to ograniczenie prawa ujętego w **art. 51 ust. 3 Konstytucji**, zgodnie z którym każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ma to szczególne znaczenie w przypadku, gdy czynności nie wykazały związków osoby z działalnością terrorystyczną. Jest to przewidywane w zakresie danych objętych tajemnicą bankową, o czym mowa poniżej (uwagi do art. 36 pkt 8 projektu).

W art. 35 pkt 2 projektu zaproponowano rozszerzenie kompetencji Żandarmerii Wojskowej na stosowanie wideomonitoringu i podsłuchu. Jest to kolejna (po proponowanej w projekcie ustawy o Straży Ochrony Kolei[5]) służba, która ma uzyskać uprawnienia do obserwowania i podsłuchiwania osób. W tym miejscu należy ponownie zwrócić uwagę na **szerszy kontekst stosowania monitoringu wizyjnego przez organy państwa**. Do Biura Generalnego Inspektora Ochrony Danych Osobowych nieprzerwanie płyną sygnały o potencjalnych naruszeniach prywatności osób obserwowanych, które z powodu braku regulacji ustawowej negatywnie wpływają na życie obywateli. W związku z tym Generalny Inspektor zwraca się do Ministra Spraw Wewnętrznych i Administracji z pytaniem, kiedy zostaną zakończone prace nad uregulowaniem monitoringu wizyjnego. Prowadzone od 2013 r. prace nad projektem założeń do ustawy o monitoringu wizyjnym[6] zostały przerwane wkrótce po zgłoszeniu w toku uzgodnień międzyresortowych i konsultacji publicznych uwag przez zainteresowane podmioty. Miało to miejsce w drugiej połowie 2014 r. Z odpowiedzi na interpelację poselską udzielonej przez Ministra[7] wynika, że celami uregulowania kwestii monitoringu wizyjnego są zapewnianie wysokiego poziomu bezpieczeństwa i porządku publicznego oraz zapewnienie gwarancji przestrzegania praw i wolności konstytucyjnych osób obserwowanych i że zadanie to będzie realizowane w obecnej kadencji Sejmu. Jednocześnie brak jest konkretnych informacji o postępach w tym obszarze. **Z drugiej strony Ministerstwo proponuje rozszerzenie katalogu podmiotów uprawnionych do stosowania obserwacji obywateli, co wpływa na prawo do prywatności osób obserwowanych.** Prace nad ustawą o monitoringu wizyjnym powinny zostać przyśpieszone, aby zagwarantować przestrzeganie praw osób obserwowanych oraz wprowadzić pewność prawną co do zasad działania systemów monitoringu wizyjnego dla ich operatorów. Także Rzecznik Praw Obywatelskich[8]

[5] http://legislacja.rcl.gov.pl/projekt/12284503/katalog/12348201#12348201, DOLiS-033-141/16/KK/40914, http://www.giodo.gov.pl/1520254/id_art/9333/j/pl/
[6] http://legislacja.rcl.gov.pl/projekt/200701/katalog/200707#200707
[7] Odpowiedź na interpelację poselską nr 245 z 01.02.2016 r. http://sejm.gov.pl/Sejm8.nsf/InterpelacjaTresc.xsp?key=060D0780
[8] https://www.rpo.gov.pl/pl/content/mswia-o-pracach-legislacyjnych-zmierzajacych-do-uregulowania-kwestii-monitoringu-wizyjnego

oraz Prezes Naczelnej Izby Kontroli[9] widzą potrzebę jak najszybszego unormowania tego obszaru.

W proponowanych przepisach brak jest regulacji zasad informowania osób o objęciu monitoringiem oraz dostępu do nagrań, co ograniczać może prawa ujęte w art. 51 Konstytucji oraz przepisach ustawy o ochronie danych osobowych. W braku postulowanej powyżej regulacji ogólnej kwestii monitoringu wizyjnego koniecznym jest wprowadzenie takich przepisów do ustaw pragmatycznych służb uprawnionych do obserwacji zdarzeń w miejscach publicznych i prowadzenia czynności operacyjno-rozpoznawczych oraz administracyjno-porządkowych.

W art. 35 pkt 6 projektodawca zaproponował dodanie art. 32c do ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. (t.j. Dz. U. z 2015 r. poz. 1929 z późn. zm., dalej zwaną **ustawą o ABW**). Miałby on umożliwiać blokowanie dostępu do danych informatycznych lub usług teleinformatycznych. Wątpliwość organu ds. ochrony danych osobowych budzą trzy kwestie. Po pierwsze, **w tiret 1 określono zbyt szeroko kryterium pozwalające na blokowanie treści**. Ma to dotyczyć danych lub usług mających związek ze zdarzeniem o charakterze terrorystycznym. Tak szerokie spektrum może obejmować także dane ujęte w artykułach prasowych, blogach, nagraniach wideo itp. treści dostępne w publicznych sieciach komunikacyjnych. Kryterium to powinno zostać doprecyzowane w taki sposób, by dane lub usługi blokowane miały bezpośredni związek z przeciwdziałaniem zdarzeniom o charakterze terrorystycznym. Nie powinno się utrudniać dozwolonej działalności, jak np. prasowa, wydawnicza czy ogólnie rzecz biorąc usługodawcza. Po drugie, należy wskazać, iż **dla podmiotu zobowiązanego do zablokowania treści nie określono możliwości złożenia odwołania** od postanowienia sądu czy zarządzenia albo żądania Szefa ABW, tak jak ma to miejsce w przypadku Szefa ABW i Prokuratora Generalnego (projektowany art. 32c ust. 10 ustawy o ABW). Ma to szczególne znaczenie w przypadku określonym w projektowanym art. 32c ust. 4 ustawy o ABW, kiedy to decyzję podejmuje Szef ABW. W projekcie powinna zostać przewidziana droga odwoławcza, aby zagwarantować możliwość weryfikacji decyzji o zablokowaniu treści. Po trzecie, **w projekcie nie przewidziano narzędzia na wypadek potrzeby uzyskania dostępu do danych albo usługi przez inne osoby niż podejrzewane o udział w zdarzeniu terrorystycznym.** Możliwym jest, iż zakres postanowienia sądu albo zarządzenia Szefa ABW utrudni osobom postronnym dostęp do treści, których są właścicielami albo użytkownikami. Ich prawa nie powinny być w sposób nieuzasadniony i nielimitowany ograniczane.

W projektowanym art. 32d ustawy o ABW upoważnia się Szefa ABW do prowadzenia rejestru zdarzeń naruszających bezpieczeństwo systemów teleinformatycznych. W ust. 2 pkt 1 nie wskazano, jakie dane operatora i administratora systemu teleinformatycznego mają być zbierane. Zgodnie z **zasadą adekwatności** ujętą w art. 26 ust. 1 pkt 3 ustawy administrator danych

[9] https://www.nik.gov.pl/aktualnosci/nik-o-miejskim-monitoringu-wizyjnym.html

powinien przetwarzać tylko takiego rodzaju dane i tylko o takiej treści, które są niezbędne ze względu na cel zbierania danych. W projekcie powinny zostać określone dane osobowe, które będą podlegać przetwarzaniu.

W art. 35 pkt 7 projektodawca zaproponował dodanie ust. 2a do art. 34 ustawy o ABW. Zgodnie z tym przepisem dostęp dla Szefa ABW ma być realizowany w drodze teletransmisji po spełnieniu warunków w tym przepisie określonych. **Generalny Inspektor zgłasza wątpliwość, czy system, z którego dane mają być udostępniane nie powinien być także wyposażony w urządzenia umożliwiające odnotowanie w systemie, kto, kiedy, w jakim celu oraz jakie dane uzyskał.** W przeciwnym wypadku administrator danych nie będzie w stanie sprawować skutecznej kontroli nad danymi, za które odpowiada niejednokrotnie pod groźbą kary – vide przepisy rozdziału 8 ustawy o ochronie danych osobowych. Należy także stwierdzić, iż żądania jednostek organizacyjnych ABW nie będą mogły być zweryfikowane przez podmiot, który ma udzielić informacji, pod względem spełnienia przez te komórki ABW wymogów określonych w projektowanym przepisie.

W art. 35 pkt 8 projektodawca zaproponował dodanie do ustawy o ABW art. 34a regulującego postępowanie m.in. z danymi objętymi tajemnicą bankową. **Wątpliwość Generalnego Inspektora budzi przepis ust. 5 pkt 4, w którym nie określono danych podmiotu objętego wnioskiem o udostępnienie informacji i danych.** Precyzyjne ich wskazanie umożliwiłoby identyfikację osób bez żadnych wątpliwości i ułatwiłoby pracę wszystkich zaangażowanych podmiotów – ABW, Sądu Okręgowego i podmiotu zobowiązanego do udostępnienia informacji. **Ponownie należy zgłosić uwagę do nieprzewidzenia trybu odwoławczego dla podmiotu, który dane ma przekazać** (vide projektowany art. 34a ust. 7 ustawy o ABW). Uwagi poczynione powyżej wobec proponowanego art. 32c ustawy o ABW mają odpowiednie zastosowanie. Należy jedynie dodać, iż w tym przypadku mamy do czynienia z informacjami szczególnej wartości, objętymi tajemnicą regulowaną m.in. przepisami ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe. (t.j. Dz. U. z 2015 r. poz. 128 z późn. zm.). **Także termin zaproponowany w projektowanym art. 34a ust. 9 ustawy o ABW należy uznać za nadmiarowy.** Podmiot, którego dane dotyczą powinien być informowany niezwłocznie po wykorzystaniu danych przez ABW o tym fakcie. Ma to zwłaszcza znaczenie w obliczu możliwości odroczenia poinformowania osoby przewidzianej w ust. 10 komentowanego artykułu.

W art. 37 pkt 2 lit. b) zaproponowano korzystanie przez Straż Graniczną z systemów monitoringu wizyjnego znajdujących się na terenie portu lotniczego oraz zapisów z tych systemów. Oznacza to korzystanie nie tylko z systemu ochrony lotniskowej, ale także systemów najemców powierzchni biurowej i handlowej na terenie lotniska. Może to być bardzo szeroki zakres

podmiotów zobowiązanych do współpracy ze Strażą Graniczną. Podobne rozwiązanie było proponowane przez Ministerstwo Spraw Wewnętrznych w toku prac nad projektem założeń do ustawy o monitoringu wizyjnym. **Uwagi poczynione wyżej do art. 35 pkt 2 projektu mają pełne zastosowanie.** Dodatkowo należy stwierdzić, iż administratorzy tych systemów powinni odnotowywać w dokumentacji przetwarzania przypadki korzystania i udostępniania nagrań na rzecz Straży Granicznej i ewentualnie innych uprawnionych podmiotów.

W art. 41 pkt 1 zaproponowano zmianę przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243 z późn. zm., dalej zwanej Prawem telekomunikacyjnym) w zakresie obowiązku rejestracji użytkowników usług telekomunikacyjnych. Obowiązujący art. 60 a ust. 1 a Prawa telekomunikacyjnego normujący zakres danych, które abonent niebędący stroną zawartej na piśmie umowy o świadczenie usług telekomunikacyjnych może udostępnić dostawcy publicznie dostępnych usług telekomunikacyjnych (dalej: dostawca), przewiduje zamknięty katalog takich danych (w przypadku abonenta będącego osobą fizyczną – imię, nazwisko, numer ewidencyjny PESEL, adres korespondencyjny, a przypadku osoby nieposiadającej numeru ewidencyjnego PESEL – nazwa i numer dokumentu stwierdzającego tożsamość). Tymczasem w projektowanym art. 60 b ust. 1 Prawa telekomunikacyjnego, katalog danych abonenta (z dwoma wyłączeniami) podlegających obligatoryjnemu przekazaniu dostawcy poprzedzony został sformułowaniem „co najmniej" i zyskał w ten sposób charakter otwarty. **Przyjęcie zaproponowanego brzmienia art. 60 b ust. 1 Prawa telekomunikacyjnego prowadziłoby do sytuacji, w której obowiązek abonenta przekazania danych dostawcy publicznie dostępnych usług telekomunikacyjnych mógłby obejmować wszelkie (dowolne) dane abonenta.** Taka konstrukcja (projektowanego) przepisu nakładającego obowiązki na abonentów pozostaje w sprzeczności ze – statuowaną w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych – **zasadą adekwatności przetwarzanych danych** w stosunku do celów, w jakich są przetwarzane.

W projektowanym art. 60b ust. 2 in fine Prawa telekomunikacyjnego, przewidziano swobodę dostawcy w zakresie określania sposobu, w jaki abonent ma mu przekazać swoje dane, o których mowa w w/w art. 60b ust. 1. Taka konstrukcja komentowanego przepisu rodzić może niebezpieczeństwo naruszenia praw abonenta. Będzie on bowiem zobligowany do przekazania („podania" według terminologii przyjętej w przepisie) swoich danych dostawcy, zaś dostawca może mu nakazać przekazanie tych danych w dowolny, wygodny dla siebie, sposób, w tym również taki, który nie zapewni ich bezpieczeństwa.

W myśl projektowanego art. 60b ust. 3 pkt 1 lit. a dostawca może rozpocząć świadczenie usługi telekomunikacyjnej abonentowi dopiero po potwierdzeniu zgodności podanych przez niego danych z danymi zawartymi w dokumencie potwierdzającym tożsamość abonenta będącego osobą

fizyczną albo we właściwym rejestrze. Pominięto wszakże całkowitym milczeniem kwestię zasadniczą z punktu widzenia oceny prawidłowości procesu przetwarzania danych, to jest zagadnienie sposobu, w jaki przedmiotowe potwierdzenie zgodności ma się odbywać. Projektodawca ograniczył się jedynie do stwierdzenia, iż potwierdzenia, o którym mowa w art. 60 b ust. 3 pkt 1 lit. a dostawca może dokonać również za pośrednictwem osoby trzeciej działającej w jego imieniu (projektowany art. 60 b ust. 4 Prawa telekomunikacyjnego). **Tym samym – w oparciu o projektowane przepisy Prawa telekomunikacyjnego nie tylko nie można ustalić, jak będzie się odbywać proces potwierdzania zgodności danych abonenta i jak w związku z tym procesem będą przetwarzane jego dane, lecz także – kto tego potwierdzenia może dokonywać.** Nie może zaś umknąć uwadze, że – zgodnie z art. 159 ust. 1 pkt 1 Prawa telekomunikacyjnego – dane użytkownika usługi telekomunikacyjnej są objęte tajemnicą telekomunikacyjną. Enigmatyczne sformułowanie „osoba trzecia działająca w imieniu dostawcy usług" nie pozwala na skonkretyzowanie kręgu osób, które w ramach procedury potwierdzania zgodności danych abonenta uzyskają dostęp do – objętych tajemnicą telekomunikacyjną – danych tych abonentów.

Stosownie do dyspozycji **projektowanego art. 60b ust. 3 pkt 2 lit. a** Prawa telekomunikacyjnego potwierdzenie podanych przez abonenta danych, o których mowa w (projektowanym) art. 60b ust. 1, może nastąpić drogą elektroniczną przy wykorzystaniu środków identyfikacji elektronicznej służących do uwierzytelniania w systemie teleinformatycznym banku krajowego, ważnego kwalifikowanego certyfikatu itd. Jak było to już podnoszone powyżej dane użytkownika usługi telekomunikacyjnej są objęte tajemnicą telekomunikacyjną. Na jakiej zatem podstawie prawnej bank będący „stroną trzecią" w stosunku prawnym abonent – dostawca ma – w związku z procesem potwierdzania zgodności danych abonenta drogą elektroniczną – uzyskać informację, iż dana osoba fizyczna jest użytkownikiem usługi telekomunikacyjnej oferowanej przez danego dostawcę publicznie dostępnych usług telekomunikacyjnych. Informacja taka jest przecież objęta tajemnicą telekomunikacyjną także wobec banku niebędącego uczestnikiem stosunku prawnego między abonentem a dostawcą publicznie dostępnych usług telekomunikacyjnych. Marginesowo zauważyć również należy, iż komentowany przepis – art. 60 b ust. 3 pkt 2 lit. a – nie reguluje kwestii zasad przetwarzania przez bank informacji pozyskanych w ramach procedury potwierdzania zgodności danych abonenta drogą elektroniczną. Takie same uwagi należy zgłosić do wykorzystania środków identyfikacji elektronicznej określonych w art. 60b ust. 3 pkt 2 lit. d.

Nie można jednocześnie nie zwrócić uwagi na kwestię osiągnięcia celu projektowanej zmiany Prawa telekomunikacyjnego. Jeżeli celem jest identyfikowanie wszystkich użytkowników usług telekomunikacyjnych, to należy pamiętać o dwóch kwestiach mających wpływ na osiągnięcie tego celu. Po pierwsze, jest to już dziś pośrednio możliwe poprzez weryfikację numerów IMEI. Po drugie, z uwagi na brak takiego obowiązku w innych krajach, należy się spodziewać wykorzystania przez osoby pragnące uniknąć identyfikacji kart SIM

sprowadzonych z tych państw. W takim wypadku cel identyfikacyjny nie zostanie osiągnięty, a na usługobiorców i usługodawców telekomunikacyjnych zostanie nałożony istotny obowiązek utrudniający zachowanie w uzasadnionych przypadkach anonimowości komunikacji (informatorzy Policji, źródła informacji dziennikarzy i zwykli użytkownicy).

Z uwagi na doniosły charakter proponowanej regulacji oraz nieprzeprowadzenie w tej sprawie pełnych uzgodnień międzyresortowych oraz konsultacji publicznych, Generalny Inspektor Ochrony Danych Osobowych deklaruje swój aktywny udział w pracach nad projektem oraz zastrzega możliwość zgłaszania dalszych uwag na każdym etapie procesu legislacyjnego.

Z wyrazami szacunku

GENERALNY INSPEKTOR
OCHRONY DANYCH OSOBOWYCH
dr Edyta Bielak-Jomaa

Do wiadomości:

Pan Poseł Arkadiusz Czartoryski, Przewodniczący podkomisji nadzwyczajnej do rozpatrzenia rządowego projektu ustawy o działaniach antyterrorystycznych oraz o zmianie niektórych innych ustaw (druk nr 516), e-mail: kasw@sejm.gov.pl