RZECZNIK PRAW OBYWATELSKICH

Adam Bodnar

Warszawa, [*27 stycznia 2017 r.]*

VII.520.10.2017.AG

Pan
Mateusz Morawiecki
Wiceprezes Rady Ministrów
Minister Rozwoju i Finansów

Rzecznik Praw Obywatelskich, monitorując proces legislacyjny, zapoznał się z przygotowanym przez Ministra Rozwoju i Finansów projektem ustawy o Centralnej Bazie Rachunków (UD28, wersja z 14 grudnia 2016 r., dalej jako: projekt ustawy o CBR albo projekt).

Projekt ustawy o CBR przewiduje utworzenie Centralnej Bazy Rachunków, czyli systemu teleinformatycznego służącego przetwarzaniu informacji o rachunkach przekazywanych przez instytucje zobowiązane. Celem ustawy, zgodnie z przedstawionym projektem uzasadnienia, ma być „ułatwienie lokalizowania składników majątkowych pochodzących z przestępstwa". Ponadto, zadaniem CBR ma być też „umożliwienie szybkiego uzyskania przez komorników sądów i organy egzekucyjne pełnej informacji o potencjalnych miejscach przechowywania przez dłużników wartości majątkowych".

Należy podkreślić, że zgodnie z art. 51 ust. 2 Konstytucji RP władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. Dopuszczalne ograniczenia prawa do prywatności uregulowanego w art. 47 Konstytucji RP wynikają z art. 31 ust. 3 ustawy zasadniczej, a zatem projektodawca, a następnie ustawodawca, musi dokładnie rozważyć i ocenić, czy proponowane ograniczenie jest konieczne i przydatne dla osiągnięcia założonego celu, niezbędne dla ochrony interesu publicznego i proporcjonalne w relacji między zamierzonym

efektem a obciążeniami nakładanymi na jednostkę. Przedstawione uzasadnienie projektu ustawy o CBR nie wyjaśnia wszystkich wątpliwości w tym zakresie. Można nawet stwierdzić, że lektura uzasadnienia w zestawieniu z projektem nasuwa kolejne pytania i wątpliwości z punktu widzenia ochrony praw obywatelskich.

Zgodnie z art. 7 projektu ustawy o CBR, instytucje zobowiązane (wymienione szeroko w art. 2 pkt 2 projektu) przekazują do CBR informacje o rachunkach w przypadku otwarcia rachunku, zmiany przekazanych informacji o rachunku i zamknięcia rachunku. Wśród danych, które mają być przekazywane przez instytucje zobowiązane, znajdują się m.in. dane identyfikacyjne wszystkich posiadaczy rachunku, czy też dane identyfikacyjne pełnomocników do rachunku (art. 8 ust. 1 pkt 2 i 4 projektu), w tym dane osobowe wymienione w art. 8 ust. 2 projektu. Informacje te, zgodnie z art. 10 projektu, mają być przekazywane za pomocą środków komunikacji elektronicznej, po spełnieniu warunków techniczno-organizacyjnych zamieszczonych w Biuletynie Informacji Publicznej na stronie podmiotowej urzędu obsługującego organ właściwy i zgodnie z wzorem dokumentu elektronicznego zamieszczonym w tym Biuletynie. Z kolei art. 11 ust. 1 projektu stanowi, że informacje o rachunkach są przetwarzane w CBR przez okres 10 lat, licząc od pierwszego dnia roku następującego po roku, w którym została wprowadzona informacja o zamknięciu rachunku. Wreszcie, w art. 12 projektu wskazano podmioty, którym będą udostępniane informacje o rachunkach.

Przepisy zaproponowane w projekcie ustawy o CBR budzą poważne wątpliwości konstytucyjne z punktu widzenia celowości i niezbędności utworzenia takiej bazy danych. Pragnę podkreślić, że przetwarzanie powyższych danych musi być uznane za ingerencję w prawo do prywatności i w prawo do ochrony danych osobowych, zwłaszcza dlatego, że dane, które mają być gromadzone i przetwarzane, są objęte tajemnicą bankową, o której mowa w art. 104 ust. 1 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2016 r., poz. 1988 ze zm.). W uzasadnieniu do projektu ustawy o CBR wskazano, że „celem projektowanej regulacji nie jest istotna zmiana dotychczasowych przepisów określających zakres uprawnień przysługujących organom publicznym w tym obszarze ani zmiana zakresu tajemnic służbowych, w tym tajemnicy bankowej". Tymczasem w obecnym stanie prawnym nie istnieją przepisy, które przewidywałyby

istnienie systemu pozyskiwania tak pełnych danych, co zresztą w poprzedzającym akapicie uzasadnienia zaznacza sam projektodawca. Przyjęcie ustawy w proponowanym kształcie będzie zatem nową regulacją – ze względu na materię – w polskim systemie prawnym.

Po drugie, w uzasadnieniu do projektu ustawy kilkakrotnie wskazuje się na dodatkowy (wydaje się – podstawowy) cel ustawy, jakim ma być **analiza proaktywna, polegająca na analizowaniu danych hurtowych dotyczących rachunków w celu typowania tych, które mogą być wykorzystywane do działalności przestępczej** (s. 3 oraz s. 5-6 uzasadnienia do projektu). Pragnę podkreślić, że takie uzasadnienie dla tworzenia kolejnej bazy zawierającej informacje o obywatelach musi budzić wątpliwości w kontekście wymogów określonych w art. 51 ust. 2 Konstytucji. Pragnę podkreślić, że z orzecznictwa Trybunału Konstytucyjnego jasno wynika, że „artykuł 51 ust. 2 Konstytucji chroni obywateli polskich, wprowadzając dla władz publicznych (ustawodawczej, wykonawczej, sądowniczej) zakaz wkraczania w autonomię informacyjną jednostki w sposób zbędny z punktu widzenia standardów demokratycznego państwa prawa. Ani więc względy celowości, ani wygody władzy nie uzasadniają naruszenia autonomii informacyjnej. (…) Normatywne wyodrębnienie, ustanowienie w art. 51 ust. 2 Konstytucji odrębnego zakazu - ułatwia dostrzeżenie takiego wkroczenia [w prywatności - dod. wł.] i upraszcza przedmiot dowodu, iż takie wkroczenie nastąpiło. Przedmiotem dowodu staje się wtedy bowiem tylko to, czy pozyskiwanie informacji było konieczne, czy tylko „wygodne" lub „użyteczne" dla władzy. Dowodu wymaga, że złamanie autonomii informacyjnej było konieczne (niezbędne) w demokratycznym państwie prawnym" (tak w wyroku TK w sprawie o sygn. akt K 41/02). **W tym kontekście uzasadnienie projektu wydaje się wyraźnie wskazywać, że chodzi wyłącznie o ułatwienie działania władzy publicznej.** Szczególne wątpliwości w tym zakresie rodzi gromadzenie w CBR danych o numerze telefonu, czy adresie poczty elektronicznej, które będą mogły być wykorzystywane w innych postępowaniach prowadzonych przez właściwe organy. Należy mieć przy tym na względzie, że w CBR znajdą się dane niemal wszystkich osób fizycznych mających rachunki w instytucjach zobowiązanych, a zatem niemal wszystkich mieszkańców Polski.

Również stwierdzenie, znajdujące się w uzasadnieniu do projektu, wskazujące na małą ilość zapytań kierowanych przez organy ścigania do centralnej informacji

o rachunkach prowadzonej obecnie w ramach KIR S.A. (s. 2 i 3 uzasadnienia do projektu) może wskazywać na brak uzasadnienia dla tworzenia takiej bazy i nieprzydatność mających znaleźć się w niej informacji.

Pozwalam sobie również podkreślić, że niewystarczającym argumentem dla przyjęcia proponowanych rozwiązań w obecnym kształcie jest powołanie się w uzasadnieniu na postanowienia projektu dyrektywy zmieniającej d*yrektywę Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniającą rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylającą dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE*. W uzasadnieniu do projektu wskazano, że według wersji z dnia 5 lipca 2016 r. na państwa członkowskie UE będzie nałożony obowiązek budowy scentralizowanego systemu, takiego jak centralny rejestr lub centralny system pozyskiwania danych, umożliwiający identyfikację posiadaczy rachunków płatniczych oraz bankowych. To po pierwsze nie oznacza, że dyrektywa zostanie w tym kształcie przyjęta ostatecznie, a po drugie – **przy jej wdrożeniu będą musiały zostać uwzględnione przepisy Karty Praw Podstawowych Unii Europejskiej** (KPP UE) oraz relewantne orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej (TSUE), który dokonywał już kilkakrotnie wykładni art. 7 i 8 KPP UE, również w kontekście dostępu organów państwowych do danych osób fizycznych i masowego ich gromadzenia[1].

Projekt ustawy **nie przewiduje żadnej formy kontroli dostępu do danych**. Tymczasem w sprawie *Tele2*, dotyczącej retencji danych telekomunikacyjnych i dostępu do nich TSUE uznał – odwołując się również do wyroku Europejskiego Trybunału Praw Człowieka w sprawie *Szabó i Vissy p. Węgrom*[2] – że dostęp do przechowywanych danych musi podlegać uprzedniej kontroli, sprawowanej przez sąd lub inny niezależny organ, a jedynym dopuszczalnym wyjątkiem od konieczności wyrażenia uprzedniej zgody są sytuacje pilne. Właściwe organy muszą również poinformować o dostępie do danych zainteresowane osoby w momencie, gdy nie ma już zagrożenia dla prowadzonego

[1] Zob. np. niedawny wyrok TSUE z 21.12.2016 r. w sprawach połączonych C-203/15 i C-698/15 *Tele2 Sverige AB przeciwko Post- och telestyrelsen* oraz *Secretary of State for the Home Department przeciwko Tom Watson, Peter Brice, Geoffrey Lewis*, EU:C:2016:970; dalej jako: wyrok w sprawie Tele2.
[2] Wyrok ETPCz z 12.01.2016 r. w sprawie *Szabó i Vissy przeciwko Węgrom*, skarga nr 37138/14.

postępowania tak, by możliwe było skorzystanie z uprawnień przewidzianych chociażby w dyrektywie 95/46[3]. Również wyrok Trybunału Konstytucyjnego, w którym TK zajmował się dostępem służb do danych telekomunikacyjnych (w tym do tzw. metadanych) wyraźnie wyznacza standard polegający na ustanowieniu kontroli nad tym procesem (wyrok TK w sprawie o sygn. akt K 23/11).

Wreszcie, projekt ustawy w art. 21 przewiduje wyłączenie stosowania art. 47 i 48 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922), co uzasadniono bardzo lakonicznie, wskazując na konieczność wymiany informacji pomiędzy podmiotami uprawnionymi. To wyłączenie oznacza, że **przekazanie danych osobowych obywatela polskiego do państwa trzeciego nie będzie wymagało zgody GIODO, oraz że w ogóle nie będzie wymagało, by w państwie, do którego dane będą przekazane zapewniony został adekwatny poziom ich ochrony.** W kontekście retencji danych telekomunikacyjnych TSUE wyraźnie podkreślił, że przepisy krajowe muszą ustanawiać obowiązek przechowywania danych wyłącznie na obszarze UE[4], a także przewidywać wymóg ich nieodwracalnego niszczenia, po upływie okresu ich przechowywania. Państwa członkowskie UE są również zobowiązane do zapewnienia niezależnej kontroli zgodności przeprowadzanej przez niezależny organ – jest to wymóg wynikający z art. 8 ust. 3 KPP UE i ma umożliwić korzystanie jednostkom z uprawnień związanych z ochroną danych osobowych, co podkreślane było również wcześniej w wyrokach TSUE w sprawach *DRI*[5], czy w sprawie *Schrems*[6].

W związku z powyższym, działając na podstawie art. 16 ust. 2 pkt 1 ustawy z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. z 2014 r., poz. 1648 ze zm.) **pozwalam sobie przedłożyć Panu Premierowi powyższe, wstępne, uwagi z uprzejmą prośbą o ich rozważenie w toku procesu legislacyjnego i poinformowanie mnie o zajętym stanowisku. Jednocześnie uprzejmie proszę o informację, czy w sprawie**

[3] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz. Urz. WE L 281 z 1995 r., s. 31.
[4] Pkt 122 wyroku w sprawie Tele2.
[5] Wyrok TSUE z 8.04.2014 r. w sprawach połączonych C-293/12 i C-594/12, *Digital Rights Ireland Ltd przeciwko Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General* i *Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others*, EU:C:2014:238.
[6] Wyrok TSUE z 6.10.2015 r. w sprawie C-362/14 *Maximillian Schrems przeciwko Data Protection Commissioner*,ECLI:EU:C:2015:650.

niniejszego projektu zasięgnięto opinii Generalnego Inspektora Ochrony Danych Osobowych.

(-) [*Adam Bodnar***]**

Do wiadomości:

Pani Edyta Bielak – Jomaa

Generalny Inspektor Ochrony Danych Osobowych