RZECZNIK PRAW OBYWATELSKICH

Adam Bodnar

Warszawa, [*1 lutego 2017 r.*]

VII.501.178.2015.AG

Pan
Mariusz Błaszczak
Minister Spraw Wewnętrznych
i Administracji

ul. Batorego 5
02-591 Warszawa

Uprzejmie dziękuję Panu Ministrowi za odpowiedź (pismo z 2 listopada 2016 r., nr BMP-0790-3/14/2016/EW) na moje wystąpienie[1] dotyczące analizy opinii Europejskiej Komisji na rzecz Demokracji przez Prawo (Komisji Weneckiej)[2] w sprawie ustawy z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz. U. poz. 147, dalej jako: ustawa nowelizująca). W wystąpieniu tym wskazałem także na wnioski płynące z raportu Agencji Praw Podstawowych Unii Europejskiej z 2015 r.[3] Podkreślałem w szczególności, że z obu dokumentów wynika konieczność dokonania zmian w systemie nadzoru nad pozyskiwaniem danych telekomunikacyjnych, pocztowych i internetowych.

Z dużym zadowoleniem przyjąłem, przekazaną mi do wiadomości w odpowiedzi Pana Ministra na moje wystąpienie, informację o rozpoczęciu prac nad przygotowaniem rozwiązań prawnych, mających na celu urealnienie demokratycznego standardu cywilnej kontroli nad umundurowanymi służbami porządku publicznego. Wyrażam zatem nadzieję, że powyższe prace doprowadzą do stworzenia mechanizmu nadzoru i kontroli, który spełni wymogi wskazane m.in. w wyżej przywołanych przeze mnie dokumentach.

[1] Pismo z 5 października 2016 r., VII.501.178.2016.AG
[2] Opinia Komisji Weneckiej nr 839/ 2016, CDL-AD(2016)012.
[3] „Inwigilacja prowadzona przez służby wywiadowcze: środki zabezpieczające prawa podstawowe oraz środki prawne dostępne w Unii Europejskiej", opublikowanego przez Agencję jeszcze w 2015 r. (http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services).

Konieczność stworzenia właściwego systemu wyrażania zgody na udostępnianie danych zgromadzonych przez operatorów telekomunikacyjnych czy danych internetowych stała się jeszcze bardziej aktualna w związku z wyrokiem Trybunału Sprawiedliwości Unii Europejskiej (TSUE) z dnia 21 grudnia 2016 r. w tzw. sprawie *Tele2*[4], w którym TSUE rozwinął tezy poczynione wcześniej w szeroko komentowanej sprawie *Digital Rights Ireland* (*DRI*)[5]. Należy przypomnieć, że w sprawie *DRI* TSUE stwierdził nieważność tzw. dyrektywy retencyjnej[6]. Wyrok ten wówczas wzbudził dyskusję m.in. co do jego skutków dla przepisów prawa krajowego, w których implementowano unieważnioną dyrektywę[7].

Wyrok z dnia 21 grudnia 2016 r. rozwija tezy zaprezentowane dwa lata temu przez TSUE i będzie miał znaczenie nie tylko dla wykładni przepisów dyrektywy 2002/58/WE (tzw. dyrektywy o e-prywatności)[8], czy też przepisów Karty Praw Podstawowych Unii Europejskiej (KPP UE)[9], ale przede wszystkim dla wykładni przepisów krajowych tych państw członkowskich, które po wyroku w sprawie *DRI* utrzymały obowiązki nałożone na operatorów telekomunikacyjnych.

Po wyroku w sprawie *DRI* pojawiły się wątpliwości co do tego, czy uznanie dyrektywy retencyjnej za nieważną oznacza powrót do możliwości samodzielnego regulowania tych zagadnień przez państwa członkowskie. Słusznie wskazywano jednak, że państwa członkowskie nie mają w tym zakresie dowolności, bowiem muszą stosować wymogi wynikające z KPP UE, a łącznikiem uzasadniającym jej stosowanie, jest właśnie art. 15 dyrektywy o e-prywatności. Przepis ten pozostaje bowiem podstawowym w zakresie

[4] 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.

[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, dalej jako wyrok w sprawie DRI.

[6] Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE, Dz. Urz. UE L 105 z 2006 r., s. 54, dalej jako dyrektywa retencyjna.

[7] Zob. A. Grzelak, *Granica między skuteczną walką z przestępczością a prawem do prywatności i do ochrony danych osobowych – glosa do wyroku TSUE z 8.04.2014 r. w sprawach połączonych: C-293/12 i C-594/12 Digital Rights Ireland*, „Europejski Przegląd Sądowy" 2016/7, s. 45 albo B. Grabowska-Moroz, *Glosa do wyroku TSUE z dnia 8 kwietnia 2014 r., C-293/12 i C-594/12 oraz do wyroku TK z dnia 30 lipca 2014 r., K 23/11*, „Europejski Przegląd Sądowy" 2016/1, s. 31.

[8] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), Dz. Urz. WE L 201 z 2002 r., s. 37 ze zm.; dalej jako dyrektywa o e-prywatności.

[9] Dz. Urz. UE C 202 z 2016 r., s. 389.

dopuszczalnych wyjątków od zasady poufności komunikacji w obszarze zharmonizowanym przez ten akt[10].

TSUE w wyroku w sprawie *Tele2* rozwiał te wątpliwości i uznał, że dyrektywa o e-prywatności jest tym łącznikiem, który uzasadnia ocenę prawa krajowego w świetle przepisów KPP UE (art. 51 ust. 1 KPP UE). TSUE wyjaśnił, że wyjątki, przewidziane w art. 15 ust. 1 dyrektywy o e-prywatności są zatem dopuszczalne, jednak muszą być interpretowane tak wąsko, by nie uchylić reguły podstawowej[11]. Przepisy krajowe, które takie wyjątki wprowadzają, muszą być zgodne z art. 7 i 8, ale także z art. 11 KPP, a wszelkie ograniczenia muszą spełniać wymóg niezbędności i proporcjonalności, co potwierdza także punkt 11 preambuły do dyrektywy o e-prywatności[12]. TSUE przypomniał też swoje wcześniejsze orzecznictwo, zgodnie z którym odstępstwa od prawa do prywatności muszą pozostawać w granicach tego, co jest „absolutnie konieczne".

Co istotne, TSUE wyraźnie wskazał, że art. 5 ust. 1 dyrektywy o e-prywatności ustanawia regułę poufności komunikacji, która obowiązuje wobec stron trzecich bez względu na to, czy są to podmioty prywatne czy państwowe. Skutkiem ustawodawstwa krajowego jest nałożenie na operatorów wymogu polegającego na umożliwieniu dostępu do danych, co samo w sobie stanowi akt przetwarzania danych, regulowany dyrektywą o e-prywatności[13]. Tym samym, TSUE zakwestionował prezentowany w trakcie postępowania pogląd Komisji i kilku państw, zgodnie z którym to retencja jest objęta zakresem dyrektywy o e-prywatności, natomiast sama regulacja dostępu do danych miałaby podlegać wyłącznie zasadom prawa krajowego. TSUE stwierdził, że skoro wyłącznym celem retencji jest umożliwienie dostępu właściwym organom do zgromadzonych i zatrzymanych danych, to tych dwóch kwestii nie można od siebie odróżniać i traktować ich odrębnie[14]. **TSUE potwierdził, że przedmiotem oceny z punktu widzenia zgodności z prawem UE powinny być nie tylko przepisy wdrażające dyrektywę retencyjną**

[10] Por. M. Taborowski, *Skutki wyroku Trybunału Sprawiedliwości Unii Europejskiej stwierdzającego nieważność dyrektywy retencyjnej*, opracowanie opublikowane na stronie Fundacji Helsińskiej http://www.hfhr.pl/wp-content/uploads/2014/04/skutki_wyroku_TSUE_MTaborowski-3.pdf (pobrano 13 maja 2014). Zob. także komentarz prof. S. Peersa, *Are national data retention laws withing the scope of the Charter?*, http://eulawanalysis.blogspot.com/2014/04/are-national-data-retention-laws-within.html.
[11] Pkt 89 wyroku w sprawie Tele2.
[12] Pkt 95 wyroku w sprawie Tele2.
[13] Pkt 78 wyroku w sprawie Tele2.
[14] Pkt 76 wyroku w sprawie Tele2.

bezpośrednio (w przypadku Polski – ustawy – Prawo telekomunikacyjne[15] i aktów wykonawczych), ale także przepisy regulujące dostęp właściwych organów do tych danych (w przypadku Polski – m.in. ustawy nowelizującej).

Odnośnie do samego procesu retencji danych w kontekście prawa do prywatności TSUE wskazał wyraźnie, że zatrzymywane dane umożliwiają wyciągnięcie bardzo szczegółowych wniosków dotyczących życia prywatnego osób, których dane zostały zatrzymane i dane te nie mają wcale mniejszego znaczenia niż treść komunikatu[16]. Ingerencję, będąca wynikiem stosowania przepisów krajowych przewidujących zatrzymywanie danych o ruchu i lokalizacji należy zatem uznać za szczególnie poważną. Prowadzić bowiem może do powstania wrażenia o podleganiu „ciągłej obserwacji". Tym samym, jedynym uzasadnieniem dla tego rodzaju ingerencji może być walka z poważną przestępczością. **Nawet konieczność walki z terroryzmem, zdaniem TSUE, nie uzasadnia sama w sobie, by uznać, że ustawodawstwo krajowe przewidujące uogólnione zatrzymywanie danych jest niezbędne[17].**

TSUE wyjaśnił jednak, że dopuszczalne jest ustanowienie obowiązku indywidualnego zatrzymywania danych w celu zwalczania poważnej przestępczości pod warunkiem, że takie zatrzymywanie nie będzie wykraczać poza to, co jest absolutnie konieczne jeśli chodzi o zakres danych, stosowane środki łączności, podmioty zaangażowane w tej proces, jak i przyjęty okres przechowywania tych danych[18]. Przepisy to regulujące muszą być jednoznaczne i szczegółowe, ale także muszą przewidywać gwarancje wystarczające do tego, by chronić przed ryzykiem nadużycia[19]. Przepisy te muszą wskazywać obiektywne okoliczności i warunki, w których środek w zakresie zatrzymywania danych może być zastosowany w celach prewencyjnych w sposób, których gwarantuje, że jego zakres będzie ograniczał się rzeczywiście do tego, co absolutnie konieczne[20].

TSUE potwierdził, że przepisy krajowe muszą ustanawiać materialne i proceduralne warunki regulujące dostęp odpowiednich organów krajowych do przechowywanych

[15] Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, Dz. U. z 2016 r. poz. 1489 ze zm.
[16] Pkt 99 wyroku w sprawie Tele2.
[17] Pkt 103 wyroku w sprawie Tele2.
[18] Pkt 108 wyroku w sprawie Tele2.
[19] Pkt 109 wyroku w sprawie Tele2.
[20] Punkt 110 wyroku w sprawie Tele2.

danych. Nie wystarczy ograniczenie się do ustanowienia wymogu, by dostęp ten uwzględniał jeden z celów realizowanych przez dyrektywę. Przepisy muszą opierać się na obiektywnych kryteriach umożliwiających określenie okoliczności i warunków przyznania dostępu do danych właściwym organom krajowym. TSUE odwołał się do wyroku Europejskiego Trybunału Praw Człowieka (ETPCz) w sprawie *Zakharov przeciwko Rosji*[21] i podkreślił, że dostęp ten może zostać zatem przyznany jedynie odnośnie do danych dotyczących osób podejrzewanych o planowanie, popełnienie czy też dopuszczenie się już poważnego przestępstwa, bądź też zaangażowanych w takie przestępstwo[22]. Dostęp do danych dotyczących innych osób może zostać przyznany również wówczas, gdy istnieją obiektywne elementy pozwalające uznać, że w konkretnym przypadku mogłoby do przyczynić się do ochrony interesów związanych z bezpieczeństwem narodowym, obroną czy bezpieczeństwem publicznym, zagrożonych wskutek działań terrorystycznych[23].

Wreszcie, TSUE uznał – odwołując się do wyroku ETPCz w sprawie *Szabó i Vissy przeciwko Węgrom*[24] – 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 postępowania tak, by wszyscy mogli skorzystać z prawa przyznanego im na mocy art. 15 ust. 2 dyrektywy o e-prywatności w zw. z art. 22 dyrektywy 95/46[25]. Dodał także, że przepisy krajowe muszą ustanawiać obowiązek przechowywania danych wyłącznie na obszarze UE[26], a także przewidywać wymóg ich nieodwracalnego niszczenia, po upływie okresu ich przechowywania. Państwa członkowskie są również zobowiązane do zapewnienia niezależnej kontroli zgodności przeprowadzanej przez niezależny organ – jest to wymóg wynikający z art. 8 ust. 3 KPP

[21] Wyrok ETPCz z 4.12.2015 r. w sprawie *Roman Zakharov przeciwko Rosji*, skarga nr 47143/06.
[22] Pkt 119 wyroku w sprawie Tele2.
[23] Pkt 119 wyroku w sprawie Tele2.
[24] Wyrok ETPCz z 12.01.2016 r. w sprawie *Szabó i Vissy przeciwko Węgrom*, skarga nr 37138/14.
[25] 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.
[26] Pkt 122 wyroku w sprawie Tele2.

i ma umożliwić korzystanie jednostkom z uprawnień związanych z ochroną danych osobowych, co podkreślane było również wcześniej w sprawach *DRI,* czy *Schrems*[27].

Pragnę wreszcie zaznaczyć, że chociaż wyrok w sprawie *Tele2* został wydany w odpowiedzi na pytania prejudycjalne sądów szwedzkiego i brytyjskiego, to jednak wykładnia dokonana przez TSUE w odpowiedzi na pytanie prejudycjalne sądu konkretnego państwa członkowskiego wiąże również pośrednio w innych państwach członkowskich[28]. Chociaż bowiem zasadniczo wyrok wiąże oczywiście sąd krajowy, który zwrócił się do TSUE z pytaniem prejudycjalnym, to jednak jego skutki mają o wiele szerszy zasięg, bowiem wyrok ma zastosowanie również poza konkretną sprawą. Innymi słowy, wyrok wydany w odpowiedzi na pytanie prejudycjalne sądu krajowego wywiera skutki nie tylko *inter partes,* ale *erga omnes*[29]. Za takim wnioskiem przemawia kilka argumentów, m.in. to, że wykładnia dokonana przez TSUE ma charakter deklaratoryjny, co oznacza, że TSUE nie ustanawia żadnych nowych zasad, a jedynie interpretuje przepisy - w tym przypadku KPP oraz prawa wtórnego (dyrektywy o e-prywatności). Dodatkowo, celem procedury pytań prejudycjalnych jest oczywiście zapewnienie spójności w wykładni prawa UE w państwach członkowskich i jego jednolitego stosowania. Służyć temu ma m.in. tzw. doktryna aktów wyjaśnionych, gdzie Trybunał – jeśli uzna, że na pytanie już odpowiedział – nie będzie odpowiadał po raz kolejny[30].

Podsumowując należy stwierdzić, że analiza wyroków wydanych w odpowiedzi na pytania prejudycjalne sądów innych państw członkowskich może prowadzić do wniosków o konieczności dokonania zmian w przepisach prawa krajowego. Taka sytuacja wydaje się mieć miejsce w przypadku przepisów polskich, w szczególności przepisów ustawy nowelizującej, regulującej dostęp właściwych organów do danych telekomunikacyjnych i danych internetowych.

W związku z powyższym, działając na podstawie art. 13 ust. 1 pkt 2 ustawy z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. z 2014 r. poz. 1648 ze zm.) zwracam się do Pana Ministra z uprzejmą prośbą o przedstawienie stanowiska

[27] Pkt 122 wyroku w sprawie Tele2.
[28] A. Grzelak, *Granica…, op. cit.,* s. 51-52. Zob. też rozważania TK w sprawie K 23/11, punkt III.3.2.2.
[29] Zob. m.in. K. Lenaerts, I. Maselis, K. Gutman, *EU Procedural Law*, Oksford 2014, s. 244.
[30] Por. także art. 99 Regulaminu postępowania przed TSUE.

w sprawie zgodności przepisów ustawy nowelizującej ze standardem wynikającym z KPP UE, w kontekście wyroku TSUE w sprawie Tele2.

Uprzejmie proszę również o przekazanie do wiadomości Rzecznika harmonogramu prac nad stworzeniem rozwiązań prawnych zmierzających do wzmocnienia demokratycznej kontroli nad służbami. Będę również ogromnie wdzięczny za udostepnienie treści „Wytycznych w sprawie realizacji przez Policję i Straż Graniczną obowiązków dotyczących przekazywania do sądu sprawozdania w zakresie uzyskiwania danych telekomunikacyjnych, pocztowych i internetowych oraz prowadzenie elektronicznego rejestru", zatwierdzonych przez MSWiA, o których poinformowano mnie w piśmie z dnia 2 listopada 2016 r.

(-) [*Adam Bodnar*]

Do wiadomości:

Pani Anna Streżyńska

Minister Cyfryzacji