



SENAT RP

ZAPIS STENOGRAFICZNY

Posiedzenie
Komisji Praw Człowieka,
Praworządności i Petycji (176.)
w dniu 13 maja 2014 r.

VIII kadencja

Porządek obrad:

1. Omówienie wpływu orzeczenia Trybunału Sprawiedliwości UE z dnia 8 kwietnia 2014 r. w sprawie Digital Rights Ireland na zasady korzystania przez policję i inne organy publiczne z danych telekomunikacyjnych dla celów zapobiegania i zwalczania przestępczości.

(Początek posiedzenia o godzinie 14 minut 06)

(Posiedzeniu przewodniczy przewodniczący Michał Seweryński)

Przewodniczący Michał Seweryński:

Dzień dobry państwu.

Otwieram posiedzenie senackiej Komisji Praw Człowieka, Praworządności i Petycji.

Będzie to posiedzenie... No, nie powiem, że nadzwyczajne, ale na pewno nietypowe, ponieważ nie będziemy rozpatrywać zwykłych spraw, jakie wpływają do nas z Sejmu, tylko pewną ekstraordynaryjną sprawę niezwyklej wagi. Zajmiemy się nią z inspiracji pana ministra Wiewiórowskiego, którego serdecznie witam. Pan minister będzie dźwigał na sobie częściową odpowiedzialność za tę konferencję.

Witam wszystkie osoby, które reprezentują instytucje rządowe i pozarządowe. Przejrzałem całą listę gości i muszę powiedzieć, że jest ona imponująca, więc pozwolę państwu, że z imienia i nazwiska wymienię tylko te najważniejsze osoby, to znaczy prelegentów. Mamy nadzieję, że powiedzą nam oni coś mądrego, co skłoni nas do dalszego działania, tym bardziej że sprawy, na które nasza dyskusja może mieć potem wpływ, zostały podniesione przez trzy ważne urzędy. A więc pozwolę sobie wymienić, w kolejności wystąpień, panią profesor Sylwię Majkowską-Szulc z Uniwersytetu Gdańskiego, pana profesora Andrzeja Adamskiego z Uniwersytetu Mikołaja Kopernika w Toruniu, panią Katarzynę Szymielewicz z Fundacji „Panoptikon” – ta fundacja jest często obecna na naszych posiedzeniach – panią doktor Agnieszkę Grzelak ze Szkoły Głównej Handlowej w Warszawie, panią Barbarę Grabowską z Helsińskiej Fundacji Praw Człowieka i pana mecenas Mikołaja Pietrzaka z Naczelnej Rady Adwokackiej. Pan mecenas będzie występował jako ostatni. Proszę państwa, jeszcze raz witam wszystkich gości, ale oczywiście najważniejsze jest to, że są z nami panowie senatorowie. Najpierw witamy gości, ale bez panów senatorów komisja nie mogłaby funkcjonować, tak więc cieszę się, że jesteście tu razem.

Program jest bardzo napięty, bo jak zwykle mamy zaplanowane jeszcze inne posiedzenia komisji, więc nie będziemy mogli za bardzo przedłużać naszej dyskusji. Właściwie w ogóle nie mamy zamiaru jej przedłużać. Chcemy zacząć i skończyć punktualnie. Wobec tego do wszystkich państwa referentów kieruję nieśmiały apel, żeby zechcieli państwa respektować ten rygor czasowy. Najlepiej po prostu za-

czynać od konkluzji, od powiedzenia o najważniejszych sprawach, a nie od wstępu, bo wtedy zabraknie czasu na konkluzje. A potem na tyle, na ile będzie to możliwe, postaramy się udzielić głosu wszystkim chętnym. Liczymy na krótkie, treściwe wypowiedzi, tak żeby odbyła się jeszcze jakaś dyskusja. Zależy nam na jak najliczniejszych wypowiedziach, ponieważ sprawa jest doniosła.

Może niech o tym wszystkim opowie jeszcze pan minister Wiewiórowski. Bardzo proszę, żeby zechciał pan w kilku słowach wyjaśnić tę sprawę. To będzie chyba najlepsze wprowadzenie. Bardzo proszę, Panie Ministrze.

Generalny Inspektor Ochrony Danych Osobowych Wojciech Wiewiórowski:

Panie Przewodniczący! Panowie Senatorowie! Szanowni Państwo!

Przede wszystkim chciałbym bardzo podziękować komisji za przychylenie się do idei zorganizowania takiego spotkania. Tak naprawdę nie jest to spotkanie o charakterze konferencji naukowej, tylko pewnego rodzaju próba zastanowienia się nad tym, co zdarzyło się 8 kwietnia 2014 r., kiedy to Trybunał Sprawiedliwości Unii Europejskiej orzekł to, co orzekł. Co tak naprawdę znajduje się w słynnym orzeczeniu nazywanym powszechnie kazusem Digital Rights Ireland, okaże się w trakcie naszej dzisiejszej dyskusji. Jeszcze raz bardzo dziękuję za możliwość zorganizowania tej sesji. No, przyznaję, że przyszedłem tutaj, żeby słuchać, a nie po to, żeby mówić. Chciałbym się dowiedzieć, jakie trzeba przyjąć rozwiązania prawne w kontekście tego, co w Polsce dzieje się w sprawie tak zwanej retencji danych telekomunikacyjnych.

Jak państwo wiecie, generalny inspektor ochrony danych osobowych w poprzednich latach wielokrotnie zgłaszał zastrzeżenia w sprawie implementacji do prawa polskiego przepisów dotyczących retencji danych telekomunikacyjnych. Przede wszystkim zwracaliśmy uwagę na to, że problem zaczyna się już na poziomie dyrektywy. Coś jest nie tak z samą dyrektywą, bo nie prowadzi ona do tego, do czego takie dyrektywy generalnie prowadzić powinny.

Chciałbym też przypomnieć stwierdzenie, które wielu oburzyło, ale z którym trudno się nie zgodzić. Mam na myśli słowa pani komisarz Malmström, która ponad dwa lata temu stwierdziła, że retencja danych i tak będzie miała miejsce. Oburzyło to wiele osób, ale w tamtym momencie właściwie nie mówiła ona o dyrektywie czy o przepisach

dotyczących retencji, tylko o samym zjawisku przechowywania danych telekomunikacyjnych. Otóż tak czy inaczej będą one przechowywane.

Nie chcę uprzedzać dyskusji, ale domyślam się, że nasi prelegenci mają różne poglądy na temat tego, jak korzystanie z danych telekomunikacyjnych przez pewne podmioty, przede wszystkim podmioty publiczne, wygląda w praktyce. Zapewne różni ich też podejście do tego, czy ta regulacja powinna być regulacją europejską, czy krajową. Obecnie czekamy na orzeczenie Trybunału Konstytucyjnego w sprawie po części dotyczącej zagadnień retencyjnych. Przede wszystkim jednak doceniamy to, że komisja senacka rozpoczęła dyskusję na temat tego, jak w przyszłości powinno wyglądać polskie prawo w kontekście między innymi tych zagadnień. Zresztą nie jest to początek tej dyskusji. Jesteśmy w jej środku. W kwietniu zdarzyło się coś ważnego. Oczywiście myślę o orzeczeniu Trybunału Sprawiedliwości Unii Europejskiej. Mam nadzieję, że wyjdziemy stąd ze świadomością, co tak naprawdę się stało i czy ma to w ogóle jakikolwiek wpływ na instytucje, które działają w Polsce.

Nie chcę przedłużać, więc myślę, że moglibyśmy od razu przejść do rzeczy. Czy pozwoli pan, że zapowiem pierwszą prelegentkę?

(Przewodniczący Michał Seweryński: Tak, bardzo proszę. Zakładam, że wszyscy wiedzą, że mają po dziesięć minut.)

Zanim przejdziemy do właściwej dyskusji dotyczącej dyrektywy retencyjnej i jej oddziaływania na prawo polskie, pozwolę sobie poprosić o wystąpienie panią doktor habilitowaną Sylwią Majkowską-Szulc z Uniwersytetu Gdańskiego, która wypowie się na temat kompetencji państw członkowskich do regulowania kwestii retencji danych po wspomnianym wyroku Trybunału Sprawiedliwości Unii Europejskiej. Chodzi o to, co tak naprawdę, z punktu widzenia europeisty, zdarzyło się w momencie, kiedy na skutek pytań prejudycjalnych uznano dyrektywę za nieważną.

Pani Profesor, zapraszam serdecznie. Będzie pani wyświetlać prezentację, czy nie? Proszę wybrać, czy woli pani mówić stąd, czy z mównicy. Mikrofon na mównicy też jest czynny, tak że to już zależy od pani.

**Adiunkt w Katedrze Prawa Handlowego i Międzynarodowego Prawa Prywatnego na Wydziale Prawa i Administracji na Uniwersytecie Gdańskim
Sylwia Majkowska-Szulc:**

Może będę mówić ze swojego miejsca. Czy jestem słyszalna?

(Głosy z sali: Tak, tak.)

Panie Przewodniczący! Generalny Inspektorze Ochrony Danych Osobowych! Szanowni Państwo!

Bardzo dziękuję za możliwość wypowiedzenia się w sprawie skutków wspomnianego orzeczenia Trybunału Sprawiedliwości Unii Europejskiej. Przypadła mi w udziale sprawa kompetencji państw członkowskich do regulowania kwestii objętych unieważnioną dyrektywą, choć jest to tylko jeden z wielu bardzo ciekawych aspektów wyroku z 8 kwietnia 2014 r.

Idąc za słuszną radą pana przewodniczącego, zacznę od konkluzji. Otóż moim zdaniem państwa członkowskie w tej chwili, po wyroku w sprawie Digital Rights Ireland, niejako z powrotem mają kompetencje do regulowania kwestii retencji danych. Dlaczego z powrotem? Otóż wyróżniamy kategorię kompetencji nieprzyznanych Unii Europejskiej – w tych właśnie dziedzinach teoretycznie możemy działać swobodnie – jak również kategorię kompetencji przyznanych Unii Europejskiej. Ponieważ dyrektywa nie została unieważniona ze względu na błędną podstawę prawną, uznajemy, że została ona wydana prawidłowo.

Celem tej dyrektywy było zbliżenie ustawodawstwa państw członkowskich w kwestii retencji danych, ponieważ rzekomo istniejące tutaj różnice mogły wpływać na rynek wewnętrzny. Po wyroku pojawiają się jednak komentarze, również znanych oficjeli unijnych, że zbliżenie ustawodawstwa się nie udało. Różnice nadal istnieją.

Jeśli chodzi o samo wdrożenie dyrektywy, to mieliśmy do czynienia z wyjątkowo dużym tak zwanym deficytem transpozycji. Dodatkowo były trzy postępowania w sprawie uchybienia zobowiązaniom państwa w związku z brakiem transpozycji dyrektywy w wyznaczonym terminie. Jedno z tych postępowań, jak państwo zapewne wiecie, zakończyło się nałożeniem na Szwecję zryczałtowanej kary pieniężnej w wysokości 3 milionów zł.

(Generalny Inspektor Ochrony Danych Osobowych Wojciech Wiewiórowski: 3 milionów euro)

A, przepraszam. Oczywiście, 3 milionów euro.

Proszę państwa, tutaj jest wiele ciekawych aspektów. Oczywiście jeśli jakieś kompetencje są przekazywane Unii Europejskiej, to nie oznacza to, że państwa członkowskie nie mogą podejmować działań legislacyjnych. Jak najbardziej mogą, ponieważ w sytuacji, w której Unia Europejska nie zadziałała, nie może pozostać luka. W związku z tym powstają tak zwane kompetencje mieszane. Niemniej jednak wraz z wydaniem aktu wewnątrzunijnego, jakim w tym przypadku była dyrektywa 2006/24/WE, pewne kompetencje automatycznie stały się kompetencjami wyłącznymi Unii Europejskiej. Oczywiście dotyczyło to zakresu normowania dyrektywy. W momencie, kiedy dyrektywa została unieważniona, akt wewnątrzunijny niejako zniknął, a skoro zniknął, to wróciliśmy do podziału kompetencji między państwa członkowskie a Unię Europejską, tak że działania legislacyjne w tej sprawie znów może podjąć zarówno państwo członkowskie, jak i Unia Europejska. Wieść brukselska niesie, że Komisja Europejska posiadająca prawo inicjatywy ustawodawczej nie spieszy się z przygotowaniem projektu kolejnego aktu prawnego, a to oznacza, że wracamy do regulowania kwestii retencji danych na poziomie państw członkowskich.

Także w samym wyroku, a właściwie w opinii rzecznika generalnego – to on zaproponował treść wyroku Trybunału Sprawiedliwości Unii Europejskiej, w związku z czym możemy uznać tę opinię za wiarygodną – nadzieję pokładamy właśnie w prawie krajowym. Rzecznik twierdzi, że dyrektywa narusza prawa podstawowe w zakresie objętym pytaniami prejudycjalnymi, niemniej jednak jest możliwe, by ta nieprawidłowość została naprawiona na poziomie państw członkowskich w ramach ustaw implementujących dyrektywę. Wprost mówi o tym punkt dotyczący skutków

temporalnych ewentualnej nieważności dyrektywy. Tak więc myślę, że jak najbardziej jest to kolejne zielone światło do regulowania kwestii retencji danych na poziomie państw członkowskich.

Jeżeli chodzi o okoliczności wydania tego wyroku, to Trybunał Sprawiedliwości Unii Europejskiej już wcześniej miał możliwość wypowiedzania się na temat wspomnianej dyrektywy pochodzącej z 2006 r. Nie zapominajmy, że została ona unieważniona z powodu niezgodności z Kartą Praw Podstawowych, która uzyskała moc prawa pierwotnego dopiero 1 grudnia 2009 r. Co działo się od roku 2006 do 2009? No, w tym czasie Trybunał Sprawiedliwości orzekał tak, jakby Karty Praw Podstawowych nie było. W związku z tym zapadły dwa wyroki w sprawach dotyczących uchybień, a trzecie postępowanie, wszczęte przeciwko Niemcom, nie zostało jeszcze zakończone. Postępowanie przeciwko Szwecji zakończyło się karą, a przeciwko Austrii nie, ponieważ nie było tutaj możliwości, żeby skorzystać z systemu nicejskiego, czyli wnieść jednocześnie o stwierdzenie uchybienia i o nałożenie ryczałtu. Pikanterii sprawie dodaje fakt, że wcześniej niejedyn trybunał konstytucyjny w Europie stwierdzał niekonstytucyjność krajowych ustaw wdrażających tę dyrektywę, ale Trybunał Sprawiedliwości Unii Europejskiej uchylił ją dopiero po wyroku niemieckiego Federalnego Trybunału Konstytucyjnego, który stwierdził, że nie ma nawet prawnych możliwości prawidłowej implementacji tej dyrektywy. I to jest, proszę państwa, odpowiedź na pytanie o kwestie politycznych okoliczności. Myślę, że ta sytuacja świetnie wpisuje się w to, co sędziowie Trybunału Sprawiedliwości określają jako kooperację czy dialog sędziowski z trybunałami konstytucyjnymi państw członkowskich.

Jeżeli zaś chodzi o kwestie merytoryczne i zakres normowania dyrektywy, to w jednym z wyroków Trybunał Sprawiedliwości stwierdził, że decyzja organów krajowych nakładająca obowiązek udostępnienia adresu IP danego użytkownika internetu nie wchodzi w zakres regulowania dyrektywy. I to jest jedyny wyrok prejudycjalny, w którym Trybunał Sprawiedliwości Unii Europejskiej dał nam wskazówkę, jaki jest zakres tej dyrektywy.

W tym samym wyroku – mówię o sprawie C-461/10 – zwraca się również uwagę na konieczność zachowania zasady proporcjonalności. Ja dodałabym do tego jeszcze zasadę celowości, od której poniekąd zaczął pan inspektor. Generalnie chodzi o cel, ze względu na który zostają wprowadzone ograniczenia praw człowieka. Zasada celowości, jako zasada szczególna, w ścisłym znaczeniu wywodzi się właśnie z ochrony danych osobowych. Najważniejszy jest cel, w jakim gromadzimy dane. Jeżeli ten cel został określony prawidłowo, to należy się go trzymać, a następnie przyjmować proporcjonalne środki.

Oczywiście różnice między państwami były bardzo duże, bo wprowadzone rozwiązania zależały od kultury prawnej każdego państwa członkowskiego. I myślę, że teraz będzie tak samo. To się po prostu nie zmienia. Wszystkie państwa będą to regulowały tak, jakby dyrektywa nie istniała.

Formalnie mieliśmy do czynienia z pytaniami prejudycjalnymi, o czym będzie, mam nadzieję, mówiła inna prelegentka, jednak co do zasady dyrektywa ta nie ma już

skutków prawnych. Jest to rzecz osądzona, *res iudicata*, w związku z czym każdy sąd polski, który wystosuje podobne pytanie prejudycjalne, zamiast wyroku otrzyma postanowienie o odmowie wydania wyroku ze względu na to, że Trybunał Sprawiedliwości Unii Europejskiej już w tej kwestii orzekał.

(*Generalny Inspektor Ochrony Danych Osobowych Wojciech Wiewiórowski: Prosilibyśmy już o podsumowanie.*)

Tak jest. W takim razie, tak jak mówiłam, przede wszystkim zwracam państwa uwagę na zasadę celowości. Mówię to w kontekście ewentualnej przyszłej polskiej ustawy i w kontekście poczynań naszego Trybunału Konstytucyjnego, który zapewne czekał ze swoim orzeczeniem do 8 kwietnia. A przynajmniej tak głosi wieść. Dziękuję bardzo.

Generalny Inspektor Ochrony Danych Osobowych Wojciech Wiewiórowski:

Dziękuję bardzo.

Zapraszam serdecznie pana profesora Andrzeja Adamskiego z Uniwersytetu Mikołaja Kopernika w Toruniu. Proszę o zaprezentowanie swojego wystąpienia.

Zapewne jesteście państwo świadomi tego, że pan profesor Adamski dwa lata temu opublikował książkę poświęconą zasadom przetwarzania danych pochodzących od operatorów telekomunikacyjnych w krajach Unii Europejskiej.

Kierownik Katedry Prawa Karnego i Polityki Kryminalnej na Wydziale Prawa i Administracji na Uniwersytecie Mikołaja Kopernika w Toruniu Andrzej Adamski:

Bardzo dziękuję za zaproszenie i za rekomendację, choć „książka” to zbyt duże słowo. Ta publikacja dotyczy kwestii zasadniczej, a mianowicie kontroli dostępu do danych telekomunikacyjnych, które podlegają obowiązkowi retencji. Jest to zagadnienie, które ma pierwszorzędne znaczenie, ponieważ zaistniała potrzeba nowego uporządkowania tej problematyki. Wynika to bezpośrednio ze wspomnianego wyroku, w którym Trybunał Sprawiedliwości Unii Europejskiej uznał, że jednym z poważnych uchybień tej unieważnionej dyrektywy było to, że milczy ona w kwestiach niezwykle istotnych z punktu widzenia ochrony prawa do prywatności i prawa do ochrony danych osobowych. To właśnie w relacji do tych praw dyrektywa ta została oceniona w orzeczeniu.

Można antycypować możliwy bieg wydarzeń w naszym kraju, ponieważ na tle innych państw wyróżniamy się tym, że mamy rekordowe statystyki, jeżeli chodzi o liczbę zapytań o różnego rodzaju dane telekomunikacyjne kierowanych przez podmioty uprawnione do operatorów telekomunikacyjnych. Milion osiemset zapytań rocznie, nawet biorąc poprawkę na pewien mętnik wynikający z krzyżowania się kwestii metodologicznych i definicyjnych, to rezultat statystyczny, który pod tym względem zdecydowanie daje Polsce pierwsze miejsce w Unii Europejskiej.

Musimy też wziąć pod uwagę, że pewne kwestie, jak się wydaje, nie są oczywiste nawet dla składu orzekającego, o czym świadczą niektóre sformułowania zawarte w tym wyroku. Nie ulega wątpliwości, że dostęp do tego rodzaju danych ma absolutnie bezdyskusyjne znaczenie z punktu widzenia możliwości efektywnego ścigania wielu rodzajów przestępstw. Co do tego panuje konsensus. Kwestią otwartą jest zaś sprawa uregulowania zasad kontrolowanego dostępu do tych danych.

W Polsce ma to szczególne znaczenie, ponieważ jesteśmy jednym z niewielu krajów – no, z mojej analizy porównawczej wynika, że w Unii Europejskiej są jeszcze dwa inne kraje, które wykazują się podobną postawą – w których nie istnieją żadne mechanizmy niezależnej, zewnętrznej kontroli dostępu do danych tego rodzaju. Nie istnieją tutaj żadne ograniczenia, nawet w przypadku najdrobniejszego przestępstwa. Wystarczy, że prowadzący postępowanie uzna, że dostęp do danych telekomunikacyjnych ma ważne znaczenie dla losów toczącego się postępowania. W konsekwencji doszło do takiej sytuacji, że ogromna liczba tych zapytań właściwie działa odstrasżająco.

Mówię to wszystko z perspektywy osoby, która chciałaby zmiany tego stanu rzeczy – absolutnie odbiegającego od europejskiej normy – poprzez włączenie jakichś mechanizmów kontrolnych. Postulat bazujący na orzecznictwie Europejskiego Trybunału Praw Człowieka, aby zajmował się tym organ sądowy albo jakiś inny niezależny organ administracyjny, zwłaszcza jeżeli chodzi o służby specjalne, jest czymś, z czym nikt nie polemizuje, niemniej jednak trudno sobie wyobrazić, jak moglibyśmy poradzić sobie z tym problemem w polskich warunkach, skoro tych zapytań jest tak wiele. Jakie sądy mogłyby się tym zajmować?

W związku z tym dochodzimy do wniosku, że próbując zmienić aktualny stan rzeczy, musimy serio potraktować to, co zawiera unieważniona dyrektywa, a co w dalszym ciągu pozostaje aktualne. Chodzi o to, że faktycznie potrzebny jest nam instrument, który zapewni efektywne ściganie przestępstw oraz zachowanie ładu i bezpieczeństwa publicznego. Istnieje jednak potrzeba wprowadzenia tutaj określonych ograniczeń aksjologicznych, to znaczy oddzielenia pewnej kategorii przestępstw związanych z możliwością skorzystania z danych telekomunikacyjnych po to, aby zwiększyć szanse powodzenia organów ścigania, od pozostałej części przestępstw, w przypadku których coś takiego nie wchodziłoby w rachubę.

Z polskiej perspektywy wydaje się jednak, że będzie to trudne zadanie, ponieważ musimy brać pod uwagę przyzwyczajenia naszych organów, które mają dzisiaj zapewnione luksusowe warunki pracy i automatyczny dostęp online do baz danych operatorów telekomunikacyjnych. Uczestnicząc w konferencji zorganizowanej przez jednego z operatorów, dowiedziałem się, że w tej chwili czas dostępu do tych danych, o ile zapytanie przedstawiciela uprawnionego podmiotu dotyczy nie więcej niż dziewięciu rekordów, nie przekracza pięciu godzin. Jeśli chodzi o bardziej skomplikowane konfiguracje czy jakieś niestandardowe zapytania, to tutaj czas oczekiwania jest dłuższy, bo sięga trzydziestu sześciu godzin. Tak więc taka sytuacja, w której przedstawiciele organów ścigania mają niczym nieskrępowany dostęp do tego rodzaju informacji i nikt tego nie kontroluje,

jest rozwiązaniem unikalnym z punktu widzenia regulacji istniejących w innych krajach europejskich. Ograniczenie tego jest absolutnie warunkiem sine qua non. Bez tego nie ma mowy, żeby w ogóle zabrać się do zmieniania istniejącego stanu rzeczy. Mam na myśli zmianę idącą w tym kierunku, który wyznacza wspomniany wyrok.

Oczywiście pojawiają się również głosy, które sugerują zróżnicowanie reżimu kontroli. Wydaje się, że nie najlepsze doświadczenia związane z falstartem Trybunału Konstytucyjnego w tej kwestii wskazują, że jest to warte rozważenia. Zresztą mówię o tym w kontekście wielu dokumentów międzynarodowych, między innymi dokumentów Komisji Weneckiej, która zajmuje się problemem pogodzenia interesów służb specjalnych z interesami innych grup społecznych czy w ogóle z prawami obywatelskimi. Można bowiem postawić pytanie, czy sędzia, który nie jest odpowiednio wyszkolony, jest właściwym podmiotem do tego, aby sprawować tak odpowiedzialną funkcję i decydować o tym, czy dać zezwolenie na dostęp do tego rodzaju informacji, czy nie.

Ja jestem pesymistą. Antycypuję, że wszelkie próby zmiany tej sytuacji napotykać będą na bardzo duży opór ze strony lobby, które zainteresowane jest utrzymaniem status quo. No, z perspektywy służb trudno wyobrazić sobie bardziej komfortową sytuację, ale taki stan rzeczy w ewidentny sposób pozostaje w sprzeczności ze standardami europejskimi. Nie wiem, jak długo jeszcze można by grać na zwłokę i niczego nie zmieniać. Te zmiany są konieczne. Dziesięć minut to zbyt mało czasu, żeby pogłębić ten temat i powiedzieć, w jakim kierunku powinny pójść zmiany, ale to, że powinny one nastąpić, wiadomo od dawna. Napisałem to już cztery lata temu, a potwierdzenie tego znalazłem w niektórych fragmentach wspomnianego wyroku. Osoby, które zajmują się tym problemem z punktu widzenia instancji judykacyjnej mającej bardzo istotny wpływ na rozwój legislacji europejskiej, właściwie myślą bardzo podobnie jak ja.

Nie wiem, czy mam jeszcze trochę czasu, ale...

(Generalny Inspektor Ochrony Danych Osobowych Wojciech Wiewiórowski: Jeszcze dwie minuty.)

Tak więc chciałbym zakończyć postulatem w sprawie, która kompromituje nas na tle prawoporównawczym. Otóż Polska jest wyjątkowo nietransparentnym krajem, jeżeli chodzi o publikowanie informacji na temat tego, w jakim stopniu wykorzystuje się pewne informacje i na jaką skalę stosuje się określone środki operacyjne. Nie mogę wyjść ze zdumienia, gdy słyszę reakcję niektórych sędziów, którzy mówią, że ich zdaniem nie powinno się tego ujawniać, bo to godzi w interes państwa.

Proszę państwa, ostatnio zapoznałem się z najnowszym holenderskim raportem dotyczącym funkcjonowania instytucji retencji danych w tym kraju. Otóż prawo telekomunikacyjne przewiduje tam coroczne publikowanie tego rodzaju informacji. Jest to standard i nikt nie wyobraża sobie, że mogłoby być inaczej. Jeżeli chodzi o efektywność wykorzystania tych danych do zapewniania bezpieczeństwa publicznego, czyli do walki z najgroźniejszą przestępczością, to przytoczę państwu to, co w tym raporcie jest najbardziej uderzające. Otóż w okresie od stycznia 2009 r. do lutego 2013 r. tylko w dwudziestu sześciu wy-

rokach pojawiła się kategoria adresu IP jako element istotny z punktu widzenia rozstrzygnięcia o winie bądź braku winy oskarżonego. W siedemdziesięciu czterech wyrokach, które zapadły pomiędzy czerwcem 2012 r. a lutym 2013 r., pojawiło się zaś pojęcie tak zwanych historycznych danych o ruchu w sieciach telekomunikacyjnych. Czemu to służyło? No, we wszystkich tych sprawach chodziło o wykazanie związku pomiędzy pokrzywdzonym a miejscem popełnienia przestępstwa. Oczywiście trzeba tu uwzględnić różnice populacyjne, ale w Holandii łączna liczba zapytań o tego rodzaju dane w 2012 r. nie przekroczyła pięćdziesięciu trzech tysięcy. A mówię to, biorąc pod uwagę wszystkie możliwe kategorie danych, jakie wchodzi tutaj w grę. U nas tych zapytań było milion siedemset czy coś koło tego. Dziękuję bardzo za uwagę.

Generalny Inspektor Ochrony Danych Osobowych Wojciech Wiewiórowski:

Bardzo serdecznie dziękuję, Panie Profesorze.

W tej chwili poprosiłbym o zabranie głosu przez Fundacji „Panoptikon”, panią Katarzynę Szymielewicz, która wyjaśni, jakie dyrektywy legislacyjne dla polskiego ustawodawcy płyną z orzeczenia Trybunału Sprawiedliwości Unii Europejskiej.

Pani prezes przedstawiać nie trzeba, zwłaszcza że uczestniczyła ona również w pracach komisji senackiej jako jeden z gości, kiedy rozpoczęto dyskusję na temat ewentualnych zmian prawnych w tym zakresie.

Prezes Zarządu Fundacji „Panoptikon” Katarzyna Szymielewicz:

Dzień dobry państwu.

Przede wszystkim dziękuję za możliwość zabrania głosu w tak ważnym momencie i w tak znakomitym gronie. Postaram się nie przekroczyć limitu czasu i powiedzieć tylko o najważniejszych sprawach.

Oczywiście zacznę od konkluzji. Z perspektywy organizacji takiej jak Fundacja „Panoptikon”, która zajmuje się tym tematem od pięciu lat – również na szczeblu Unii Europejskiej, gdzie czasem prowadziliśmy, muszę przyznać, dość frustrujące dysputy z osobami odpowiedzialnymi za wdrożenie tych przepisów na poziomie Komisji Europejskiej – wyrok Trybunału Sprawiedliwości rzeczywiście jest przełomem, kończy pewien etap. Mam nadzieję, że to już koniec tych bezpłodnych dyskusji, które moglibyśmy toczyć jeszcze długo. Osobiście uważam ten wyrok za na tyle autorytatywny, niezależny i merytoryczny, że trudno będzie – taką mam przynajmniej nadzieję – podważyć zawarte w nim tezy czy też stwierdzenia.

Przejdę więc od podkreślenia tychże tez, bo uważam, że powinny one wpłynąć na debatę polityczną w Brukseli, ale również na prace legislacyjne w Polsce. Są to kwestie fundamentalne. Przede wszystkim Trybunał Sprawiedliwości Unii Europejskiej potwierdził, że gromadzenie na wszelki wypadek danych telekomunikacyjnych o wszystkich obywatelach jest poważną ingerencją w prywatność, mimo że

są to tak zwane metadane. W debacie publicznej, szczególnie w Polsce, często słyszymy kontrargument, iż zbieranie danych o komunikacji bez ingerencji w treść tejże komunikacji nie jest jeszcze poważną ingerencją w prywatność. Trybunał rozważył ten argument i wydaje mi się, że ponad wszelką wątpliwość przesądził na korzyść obywateli, że zbieranie informacji o tym, kto z kim, kiedy i gdzie się komunikował, również jest bardzo poważną ingerencją. W istocie z tego typu danych można wywnioskować dużo więcej o życiu danej osoby – jej nawykach komunikacyjnych, relacjach, powiązaniach, tajemnicach zawodowych i różnych innych aspektach życia – niż z podsłuchu założonego w konkretnym miejscu i czasie. Przedstawiciele służb doskonale to wiedzą i dlatego uważają te dane za tak cenne, ale dzięki różnym badaczom i dzięki temu, co orzekł Trybunał Sprawiedliwości, wiemy to też i my.

Druga istotna sprawa jest taka, że nie chodzi tylko o prywatność, ale także o funkcjonowanie demokracji i o coś, co nazywa się *chilling effect*, mrozącym wpływem na życie obywatelskie. Zdaniem Trybunału Sprawiedliwości to, że człowiek cały czas podlega nadzorowi i ma poczucie, że w każdej chwili dane o nim mogą zostać w dość swobodny sposób wykorzystane przez państwo, może ograniczać także inne jego prawa, choćby do wolności słowa lub wolności zgromadzeń, czy też stanowić ingerencję w tajemnice zawodowe. To także jest bardzo ważna konkluzja.

Trzecia sprawa dotyczy tego, że już samo gromadzenie tego typu danych w jednym miejscu czy też nawet w wielu bazach danych – techniczne niuansy są tak naprawdę bez znaczenia – sprzyja nadużyciom. To, że tego typu informacje mogą być pozyskiwane w sposób automatyczny, a więc bez pośrednika, jakim byłby sąd, prokurator czy ktokolwiek inny, kto mógłby stać na straży takiego zbioru danych, sprzyja nadużyciom i wyciekom. To jest być może banalna prawda, ale cieszę się, że Trybunał Sprawiedliwości też ją podkreślił. Każdy zbiór danych stwarza ryzyko nadużycia i wycieków. Musimy o tym pamiętać, szczególnie w Polsce, gdzie niepokojąca tendencja do tworzenia nowych baz danych wydaje mi się dość wyraźna.

Czwarta fundamentalna kwestia, która została zawarta w orzeczeniu, to stwierdzenie, że retencja danych może pełnić ważną funkcję w walce z przestępczością, ale tylko jeśli towarzyszą jej pewne gwarancje. Tego typu instrument, właśnie ze względów, o których powiedziałam przed chwilą, nie może funkcjonować bez zapewnienia odpowiednich gwarancji prawnych. To również wydaje się dość oczywiste, ale dotąd oczywistym nie było.

Jak zapewne państwo pamiętacie, dyrektywa, o której rozmawiamy, została wprowadzona w Unii Europejskiej jako instrument harmonizujący rynek wewnętrzny, a nie jako instrument walki z przestępczością, ponieważ wówczas Unia nie miała nawet kompetencji do tego, żeby regulować kwestie związane z wymiarem sprawiedliwości czy pracą Policji, a już na pewno nie w formie dyrektywy. Tak że pojawienie się dyrektywy było związane z harmonizacją rynku, co miało działać na korzyść podmiotów prywatnych. A więc byliśmy świadkami czegoś, co w mojej opinii było po prostu... No, bardzo trudno byłoby przeprowadzić to na poziomie krajów członkowskich, ale mając wytrych w postaci polityki wspólnego rynku, Unia umożliwiła sobie,

mówiąc kolokwialnie, przepchnięcie bardzo kontrowersyjnej dyrektywy, która tak naprawdę służyła czemuś zupełnie innemu, niż wówczas deklarowano.

Moim zdaniem tego typu mechanizm jest niedopuszczalny. Trybunał też powiedział, że nie można wprowadzać obowiązku, który dotyczy ograniczenia praw obywateli, bez zapewnienia żadnych gwarancji. A taka była logika Unii: obowiązek – tak, gwarancje – nie, bo to jest już problem państw członkowskich. Trybunał zwraca nas z tej drogi i mówi: jeśli Unia Europejska reguluje tak newralgiczne kwestie, to musi również zadbać o zapewnienie odpowiednich gwarancji. Jeśli nie może tego zrobić, bo nie ma kompetencji, to w ogóle nie powinna tego dotyczyć. Tak właśnie rozumiem ten element wyroku, z którego jako obywatelka cieszę się najbardziej.

Jeśli chodzi o konkretne dyrektywy, jakie wypływają z tego wyroku, czy też wskazówki dla polskiego ustawodawcy lub kogokolwiek innego, kto chciałby zmierzyć się z trudnym zadaniem regulacji tego obszaru, to ja widzę tutaj pięć ważnych gwarancji. Teraz postaram się je szybko wymienić.

Pierwsza jest taka, że musimy ograniczyć cele, w jakich tego typu dane są wykorzystywane, tylko do ścigania poważnych przestępstw. Powraca tutaj problem definicji. Jak na poziomie Unii Europejskiej możemy zdefiniować poważne przestępstwo? Czy to w ogóle jest możliwe? Czy nie byłaby to nadmierna ingerencja w suwerenność państw członkowskich? Nie wiem, nie mnie to oceniać, ale jeśli chodzi o Polskę, to ten temat ciągle wraca. Dzisiaj tego typu dane są w Polsce wykorzystywane w celach błahych, nawet do ścigania wykroczeń czy do działań prewencyjnych. Trybunał Sprawiedliwości Unii Europejskiej jest zdania, że takie wykorzystywanie tych danych jest nieuzasadnione.

Druga ważna dyrektywa dotyczy gwarancji proceduralnych. Chodzi o to, kto ma stać na straży dostępu do tych danych. Jeżeli już mamy tego rodzaju zbiór danych i się z tym faktem godzimy – tego akurat Trybunał Sprawiedliwości nie podważa – to musimy go bronić przed nieuprawnionym dostępem. Musi tutaj zaistnieć kontrola sądowa, bo nie wyobrażam sobie, żeby jakikolwiek inny organ mógł przejąć tę funkcję.

Jakkolwiek oczywiście nie każdy typ danych musi podlegać kontroli o tak wysokich standardach. I to jest trzecia dyrektywa, o której mówi Trybunał Sprawiedliwości. Chodzi o różnice między kategoriami danych. Nie każda ingerencja w prywatność jest równie niepokojąca. Pobieranie danych o lokalizacji czy bilingów to bardzo duże ingerencje w prywatność, ale na przykład sprawdzenie danych abonenckich na pewno stanowi mniejszą ingerencję. Ustawodawca powinien dostrzegać te różnice i dostosowywać do nich gwarancje proceduralne i inne zmienne, które uwzględnią się w procesie legislacji.

Czwarta gwarancja odnosi się do kwestii bezpieczeństwa danych. Skoro już tworzymy taki zbiór danych – szczególnie jeśli jest on w rękach prywatnych podmiotów – to musimy zadbać o jego bezpieczeństwo. Unieważniona dyrektywa nie sprecyzowała, w jaki sposób operatorzy powinni zabezpieczać dane, i to był kolejny poważny problem.

I wreszcie piąta dyrektywa, dosyć ciekawa w kontekście tego, czego na temat programów amerykańskiej inwigilacji dowiedzieliśmy się dzięki Edwardowi Snowdenowi. Otóż

dotyczy ona lokalizacji danych, czyli tego, gdzie takie bazy danych mają być ulokowane. Czy mogą się one znajdować poza granicami kraju, który wymaga retencji, czy też powinny niejako podlegać jego terytorialnej jurysdykcji, a tym samym ochronie, jaką stanowią lokalne standardy prawne? Zdaniem Trybunału Sprawiedliwości to też jest ważna kwestia. Wydaje mi się, że przywołane przeze mnie rewelacje Edwarda Snowdena pokazały, jak ważna w dzisiejszym świecie jest lokalizacja danych i że o tym również powinniśmy pamiętać.

To chyba wszystko, co chciałam państwu powiedzieć. Jeżeli będzie taka potrzeba, to w czasie dyskusji z chęcią podam więcej szczegółów. Dziękuję bardzo.

Generalny Inspektor Ochrony Danych Osobowych Wojciech Wiewiórowski:

Dziękuję bardzo za respektowanie reżimu czasowego, a przede wszystkim za te praktyczne wskazówki dotyczące tego, jakie kwestie należy wziąć pod uwagę.

Teraz zapraszam panią doktor Agnieszkę Grzelak ze Szkoły Głównej Handlowej w Warszawie, która poniekąd powróci do tematu rozważanego przez nas już na początku, czyli do europejskich aspektów tego orzeczenia. Tym razem przede wszystkim zastanowimy się jednak nad tym, jaki skutek będzie miało stwierdzenie nieważności dyrektywy w trybie prejudycjalnym. Chodzi o to, czy będzie to skutek *ex tunc*, *ex nunc*, *erga omnes* czy *inter partes*.

Adiunkt w Katedrze Prawa Europejskiego w Kolegium Ekonomiczno-Społecznym w Szkole Głównej Handlowej Agnieszka Grzelak:

Dziękuję bardzo.
Szanowni Państwo!

W sentencji wyroku w sprawie DRI czytamy, że stwierdza się nieważność dyrektywy Parlamentu Europejskiego i Rady dotyczącej retencji danych telekomunikacyjnych. Z punktu widzenia prawa Unii Europejskiej, w którym się specjalizuję, powstaje w związku z tym szereg pytań odnoszących się do skutków takiego orzeczenia.

Dlaczego? Otóż dlatego, że wyrok wydany w procedurze prejudycjalnej zasadniczo służyć ma wyjaśnieniu wątpliwości, które mają sądy krajowe. Oczywiście umożliwia on również ocenę ważności aktu prawnego Unii, z czym mieliśmy do czynienia w tej właśnie sprawie, jednak co do zasady postępowanie prejudycjalne ma na gruncie prawa krajowego charakter wpałkowy. Dotychczas było niewiele przypadków, w których unieważniano całą dyrektywę, a w procedurze prejudycjalnej – sprawdziłam to – nie było ani jednego takiego przypadku. Zdarzały się wyłącznie sprawy, w których unieważniano poszczególne przepisy dyrektyw. Jedną z ważniejszych spraw tego typu była sprawa *Test-Achats*. Możemy się więc zastanawiać, jakie skutki będzie miał taki wyrok dla innych państw członkowskich, zwłaszcza że można to porównać do innej procedury istniejącej w Unii Europejskiej, a mia-

nowicie do skargi na nieważność aktu prawnego Unii uregulowanej w art. 263 Traktatu o funkcjonowaniu Unii Europejskiej.

W temacie swojego wystąpienia postawiłam pytanki, dlatego że... No, jeśli chodzi o skutek *erga omnes*, to jest tu mniej wątpliwości. Formalnie rzecz biorąc, orzeczenie to zostało wydane w związku z postępowaniem krajowym, więc można by powiedzieć, że w tej sprawie mamy do czynienia ze skutkiem *inter partes*, ale w praktyce wyrok ten ma również skutek *erga omnes*. Myślę, że nie ma co do tego żadnej wątpliwości.

Skąd taki wniosek? No, można się tutaj powołać na wcześniejsze orzeczenia Trybunału Sprawiedliwości, chociażby w słynnej sprawie C-66/80 dotyczącej International Chemical Corporation czy w sprawie C-475/01, w której Komisja Europejska występowała przeciwko Grecji. Akurat w tej sprawie, w pktcie 18 orzeczenia, Trybunał Sprawiedliwości wyraźnie wymienił procedury, które powodują, że domniemanie ważności aktu przestaje obowiązywać. Przede wszystkim jest to skarga na nieważność, ale stwierdzenie nieważności w trybie prejudycjalnym również powoduje, że domniemanie ważności przestaje obowiązywać. W takim razie stwierdzenie nieważności w wyniku postępowania prejudycjalnego sprawia, że akt przestaje wywoływać skutki prawne.

Potwierdzeniem tego jest jeszcze zasada rzeczy osądzonej, *res iudicata*. Mogę tu przywołać kilka orzeczeń, chociażby postanowienie w sprawie T-305/08, Włochy przeciwko Komisji, w którym Trybunał Sprawiedliwości wyraźnie stwierdził, że unieważnienie aktu w trybie prejudycjalnym skutkuje brakiem zasadności skargi opartej na tej drugiej procedurze, bo obie procedury są identyczne w skutkach.

Poza tym, zgodnie z orzecznictwem Trybunału Sprawiedliwości, niedopuszczalne jest ponowne zadanie pytania prejudycjalnego przez inny sąd w sprawie nieważności tej samej dyrektywy.

I wreszcie, proszę państwa, argument dotyczący zasady jednolitego stosowania prawa unijnego. Jeżeli wyrok Trybunału Sprawiedliwości stwierdzający, że dyrektywa jest nieważna, byłby wiążący wyłącznie w danej sprawie, to prowadziłoby to do dosyć absurdalnych rezultatów. Moglibyśmy wówczas dojść do wniosku, że wyrok ten wiąże tylko DRI czy też podmioty austriackie, ale na przykład Irlandii już nie, bo Irlandia nie była stroną postępowania. Oczywiście byłaby to dosyć absurdalna sytuacja. Zresztą analogiczna sytuacja pojawia się w odniesieniu do tych orzeczeń wydawanych w trybie prejudycjalnym, które dotyczą wykładni prawa unijnego. Jeżeli Trybunał Sprawiedliwości Unii Europejskiej dokonuje wykładni jakiegoś przepisu na wniosek danego sądu, to trudno sobie wyobrazić, by wykładnia ta miała nie obowiązywać w odniesieniu do innych sądów. Zresztą wiemy, że w prawie unijnym obowiązuje zasada, że w takiej sytuacji pozostałe sądy nie zadają już pytań w tej sprawie.

Niemniej jednak pojawiają się wątpliwości co do kwestii formalnych. Mianowicie chodzi o to, czy instytucje unijne muszą podjąć działania zmierzające do uchylenia dyrektywy w sposób formalny. Jeśli przeczytamy przepisy Traktatu o funkcjonowaniu Unii Europejskiej, to znajdzie-

my tam art. 266, który zobowiązuje te instytucje do podjęcia środków zapewniających wykonanie wyroku Trybunału Sprawiedliwości. Dotychczasowe orzecznictwo potwierdza, że przepis ten per analogiam stosuje się również do procedury prejudycjalnej. Byłoby to więc pożądane, ale oczywiście w praktyce tak się nie dzieje. Przepisy dyrektyw są uchylane, ale nie z powodu stwierdzenia ich nieważności przez Trybunał Sprawiedliwości. Jeżeli chcemy się dowiedzieć, czy dany przepis nie obowiązuje, po prostu sprawdzamy adnotacje w EUR-Leksie, która odwołuje nas do odpowiedniego orzeczenia.

Tak więc jeżeli chodzi o skutki prawne, to ta dyrektywa de facto już nie istnieje, co nie oznacza oczywiście, że prawo krajowe, które ją implementuje, automatycznie stało się nieważne. Kwestia oceny zgodności orzeczenia z przepisami krajowymi to osobne zagadnienie. Nie oznacza to również, że w przyszłości nie mógłby zostać przyjęty nowy akt, który regulowałby te kwestie, bo Trybunał nic takiego nie powiedział. Wręcz przeciwnie, w sprawie C-301/06 potwierdził kompetencje Unii do regulowania tych spraw.

Można by jeszcze powiedzieć kilka słów na temat skutków tej dyrektywy dla spraw, które się toczą, albo dla tych, które już się zakończyły, zwłaszcza w tych przypadkach, kiedy stwierdzono naruszenie przez państwa członkowskie zobowiązań w związku z niewdrożeniem dyrektywy. Powstaje pytanie, czy takie postępowania można wznowić. Ja nie znalazłam jakichś szczególnych podstaw proceduralnych ku temu, niemniej te państwa, których to dotyczy, na pewno przeanalizują to dokładniej. Zwłaszcza Szwecja, która zapłaciła 3 miliony euro kary.

Kolejny wątek też jest ciekawy, bo temporalne skutki wyroku, czyli skutki czasowe – chodzi o to, od którego momentu dyrektywa przestaje obowiązywać – to moim zdaniem najsłabszy punkt orzeczenia w sprawie DRI. Rzecznik generalny wskazywał, że niektóre państwa, implementując dyrektywę, niejako poprawiły jej postanowienia w prawie krajowym, w związku z czym warto by rozważyć pozostawienie dyrektywy w mocy do czasu przyjęcia nowych przepisów. To też nie byłoby najbardziej fortunne rozwiązanie, ale taka sugestia została przedstawiona przez rzecznika. Trybunał jednak nie przyjął tej argumentacji i nie skorzystał z możliwości zawartych w art. 264 Traktatu o funkcjonowaniu Unii Europejskiej.

I tutaj pojawia się problem, bo w tej sytuacji dyrektywa powinna przestać obowiązywać niejako od samego początku swojego istnienia, jednakże jest jeden argument, który wskazuje na to, że należy wyznaczyć inny moment. Otóż Karta Praw Podstawowych stała się w Unii Europejskiej aktem prawnie wiążącym z dniem 1 grudnia 2009 r. Skoro Trybunał Sprawiedliwości stwierdził nieważność dyrektywy z art. 7, 8 oraz 52 Karty Praw Podstawowych, to w takim razie być powinniśmy stwierdzić, że dyrektywa przestaje obowiązywać od 1 grudnia 2009 r.

Nie znam argumentów, które nakazywałyby mi jakieś kategoryczne rozstrzygnięcie tej sprawy. Mogę przedstawić pewne argumenty i za jednym, i za drugim rozwiązaniem. Za pierwszym rozwiązaniem, które zakłada, że dyrektywa przestaje obowiązywać od momentu jej przyjęcia, przemawia po prostu to, że Trybunał Sprawiedliwości nie ograniczył skutków wyroku w czasie, a zatem możemy

domniemywać, że miał na myśli to, by dyrektywa przestała obowiązywać od momentu, kiedy została przyjęta, czyli *ex tunc*. Inny argument jest taki, że w preambule do dyrektywy jest odwołanie do art. 7 i 8 Karty Praw Podstawowych, która oczywiście istniała jeszcze przed 1 grudnia 2009 r., choć nie była wtedy aktem prawnie wiążącym. Skoro więc prawodawca unijny miał świadomość istnienia tych przepisów, to w związku z tym można twierdzić, że dyrektywa powinna przestać obowiązywać od momentu jej przyjęcia.

Niemniej jednak trzeba również pamiętać, że Karta Praw Podstawowych ma w wielu aspektach dosyć innowacyjny charakter. Przykładem takiej innowacyjności jest chociażby prawo do ochrony danych osobowych, które nie pojawia się w Europejskiej Konwencji Praw Człowieka ani nie zostało wprost zaliczone do zasad ogólnych prawa unijnego. W związku z tym można rozważać, czy nie powinno mieć tutaj miejsca czasowe ograniczenie zakresu stosowania tego aktu.

Proszę państwa, takie argumenty pojawiają się też wśród przedstawicieli doktryny. Mogę przywołać artykuł z chyba najważniejszego czasopisma dotyczącego prawa unijnego, czyli z „Common Market Law Review”. W 2012 r. pani profesor Sánchez przedstawiła na jego łamach pogląd, że w sprawach, w których wyłącznym punktem odniesienia jest Karta Praw Podstawowych, stwierdzenie nieważności aktu sprzed jej wejścia w życie byłoby sprzeczne z zasadą pewności prawa.

Sprzeciwiają się temu z kolei opinie rzeczników generalnych w sprawie Toshiba i w sprawie Dominguez, którzy twierdzą, że odebranie możliwości stosowania Karty Praw Podstawowych w odniesieniu do zdarzeń, które miały miejsce przed jej wejściem w życie, zanegowałoby fakt, że sądy unijne już wcześniej przyznały temu instrumentowi ogromne znaczenie. No, tak było, ale trzeba pamiętać, że nie mieliśmy wcześniej przypadku, w którym Trybunał Sprawiedliwości stwierdziłby nieważność jakiegoś przepisu ze względu na jego sprzeczność z Kartą Praw Podstawowych.

Tak jak mówiłam, nie udzielam tutaj żadnej odpowiedzi. Sprawa jest otwarta. Można by też przywołać jeszcze inne orzeczenie, w którym Trybunał Sprawiedliwości stwierdził, że zakres Karty Praw Podstawowych jest taki sam jak zakres zasad ogólnych, ale w wyroku w sprawie DRI nie ma odwołania do zasad ogólnych prawa Unii Europejskiej.

Nie wykluczam, że wkrótce o skutki tego orzeczenia zapyta któryś z sądów krajowych. I to byłoby chyba najkorzystniejsze rozwiązanie, bo wyjaśniłoby ono szereg wątpliwości. Ale czy w praktyce przyniosłoby to jakieś efekty? No, można się nad tym zastanawiać. Pozostawiam tę kwestię do dyskusji. Dziękuję bardzo.

Generalny Inspektor Ochrony Danych Osobowych Wojciech Wiewiórowski:

Bardzo serdecznie dziękuję.

Komentarz do tego orzeczenia jako jedna z pierwszych przedstawiła na swoich stronach internetowych Helsińska Fundacja Praw Człowieka. Fundacja ta zasugerowała też, zresztą również jako pierwsza, co miałyby z tego wynikać dla działań organów publicznych w Polsce.

W związku z tym bardzo proszę panią Barbarę Grabowską, przedstawicielkę Helsińskiej Fundacji Praw Człowieka, o odniesienie się do tego problemu. Jakie pani zdaniem będą skutki tego wyroku dla polskiego ustawodawstwa oraz Trybunału Konstytucyjnego?

Przedstawiciel Helsińskiej Fundacji Praw Człowieka Barbara Grabowska:

Bardzo państwu dziękuję za zaproszenie i za możliwość bardzo wnikliwego przedyskutowania tego wyroku, który faktycznie jest dość niecodzienny. Jednym z nietypowych elementów jest chociażby to, że jest to prawdopodobnie pierwszy wyrok Trybunału Sprawiedliwości tak wnikliwie analizowany przez polskiego ustawodawcę.

Sprawa jest tym bardziej ciekawa, że analogiczną debatę prowadzimy również na sali sądowej przy Alei Szucha, to znaczy przed Trybunałem Konstytucyjnym. Wniosek rzecznika praw obywatelskich dotyczy tego, na ile ta polska regulacja, która implementuje dyrektywę retencyjną, jest zgodna z... No, tym razem nie z Kartą Praw Podstawowych, tylko z polską konstytucją oraz z art. 8 Europejskiej Konwencji Praw Człowieka.

Polecam państwu opinię prawną, którą przygotował pan doktor Taborowski. Jest ona dostępna na naszej stronie internetowej, więc proszę ją potraktować jako załącznik do mojego wystąpienia. Pan doktor dość szczegółowo analizuje wszystko to, o czym ja prawdopodobnie, ze względu na ograniczenia czasowe, powiem dość ogólnikowo. Tak więc w opinii tej znajdują państwo rozwinięcie wielu kwestii, które poruszę w moim dzisiejszym wystąpieniu. Odnosi się ona także do tych kwestii, które były tu poruszane już wcześniej.

Działaniem, które fundacja podjęła zaraz po wydaniu tego wyroku, było skierowanie do Trybunału Konstytucyjnego pisma procesowego z prośbą o to, aby rozważono wydanie odpowiedniego postanowienia sygnalizacyjnego skierowanego do polskiego ustawodawcy, a także do Rady Ministrów. Chodziło o to, by zapytać, czy to, co 8 kwietnia stało się w Luksemburgu, nie ma aby bezpośredniego przełożenia na obowiązki ustawodawcze w Polsce.

Wniosek ten motywowany był przede wszystkim tym, na co już tutaj wskazywano. Otóż jest bardzo prawdopodobne, że dotychczasowa polska regulacja nie była zgodna ze wspomnianą dyrektywą unijną. W wielu miejscach nasze prawo nie stało na takim poziomie, jaki przewidywała dyrektywa. Kluczowym przykładem jest tutaj katalog przestępstw, w sprawie których można kierować do operatorów zapytanie o dane retencyjne.

Drugim czynnikiem, który wpłynął na wystosowanie przez nas tego pisma, było to, co w analogicznej sytuacji zrobił słowacki sąd konstytucyjny. Zostało to tam zainicjowane nie przez rzecznika praw obywatelskich, ale przez grupę parlamentarzystów, którzy zadawali te same pytania co my. Otóż 23 kwietnia słowacki trybunał zawiesił obowiązywanie przepisów implementujących dyrektywę retencyjną. Co prawda nie ma jeszcze uzasadnienia i nie wiemy, czy faktycznie była to konsekwencja

wyroku luksemburskiego, ale można się tego domyślać, bo od wyroku do decyzji sądu słowackiego upłynęły tylko dwa tygodnie.

O tym, jakie skutki wywołuje wyrok w sprawie Digital Rights Ireland, już dzisiaj mówiono. Jeśli chodzi o meritum, to ta sprawa została już przeanalizowana. Wskazano, które elementy są kluczowe i które niedociągnięcia mogą mieć wpływ na to, jak będzie wyglądać przyszła regulacja w tym zakresie. Konkluzja jest taka: dotychczasowy poziom ochrony danych osobowych jest za niski i trzeba go podnieść już na poziomie Unii Europejskiej. Aczkolwiek może się stać tak, że poziom ten nie zostanie podniesiony na poziomie Unii Europejskiej i wówczas to krajowy ustawodawca stanie przed pytaniem, co zrobić z tym problemem. Teraz właśnie piłka jest po stronie krajów członkowskich. Co polski ustawodawca mógłby z tym zrobić? Czy w ogóle musi zrobić cokolwiek? Może po prostu powinniśmy poczekać na rozstrzygnięcie polskiego Trybunału Konstytucyjnego i dopiero wówczas zacząć się martwić. Było to już dzisiaj analizowane. Jeśli zadamy sobie pytanie, kto jest adresatem tego wyroku, to zrozumiemy, że nie jest to tylko sąd austriacki czy sąd irlandzki. Okazuje się, że w równym stopniu adresatem tamtego wyroku jest między innymi polski Trybunał Konstytucyjny. Wynika to z zasady lojalności. Prawdopodobnie tak właśnie należałoby więc rozumieć skutki tego wyroku prejudycjalnego.

I teraz właściwie przechodzę już do ostatniego elementu mojej wypowiedzi. Otóż możemy potraktować ten wyrok jako sygnał mówiący, że nasza regulacja krajowa również okaże się niezgodna z Kartą Praw Podstawowych. Ten argument jest jednak o tyle niebezpieczny, że stosowanie Karty Praw Podstawowych w odniesieniu do państw członkowskich, zgodnie z art. 51, jest możliwe tylko w tym zakresie, w jakim państwa te stosują prawo Unii Europejskiej. Pytanie brzmi: jakie prawo Unii Europejskiej stosujemy, skoro dyrektywy już nie ma? Doktor Taborowski proponuje w tym zakresie kilka rozwiązań. Przede wszystkim mówi on, że to, co nazywamy retencją danych telekomunikacyjnych i dostępem do nich, tak naprawdę stanowi wyjątek od ogólnych zasad ochrony danych osobowych, które są regulowane na poziomie Unii Europejskiej. Drugi argument, którego używa pan doktor, jest taki, że retencja tych danych i obowiązki nakładane na operatorów telekomunikacyjnych będą miały przełożenie na kształt i funkcjonowanie rynku wewnętrznego, a to również należy do kompetencji Unii Europejskiej, która ma w tym zakresie odpowiednie regulacje. Mamy więc podstawy ku temu, by stwierdzić, że polska regulacja powinna być rozpatrywana właśnie z punktu widzenia Karty Praw Podstawowych. A jak należy to robić? Otóż przykład dał nam Trybunał Sprawiedliwości, który 8 kwietnia wyznaczył odpowiednią ścieżkę rozumowania.

Ciekawy wydaje mi się również jeszcze jeden element. Otóż w tej sprawie istotna może być nie tylko Karta Praw Podstawowych, ale również polska konstytucja. Art. 53 Karty Praw Podstawowych przewiduje bowiem, że akt ten nie może być chroniony na poziomie niższym niż konstytucje krajowe. Skoro więc wyrok z 8 kwietnia dość wysoko zawieszają poprzeczkę w zakresie retencji danych telekomunikacyjnych, to powinniśmy się spodziewać, że

polski Trybunał Konstytucyjny nie będzie tego standardu zaniżać. Wynika to właśnie z art. 53, czytanego niejako od końca. Moim zdaniem w świetle polskiej konstytucji kluczowe jest to, że Trybunał Sprawiedliwości Unii Europejskiej w Luksemburgu zachował się jak rasowy sąd zajmujący się prawami człowieka – no, prawie jak trybunał w Strasburgu – bo od początku do końca przeprowadzał test proporcjonalności. Nie powinno być więc dla państwa zaskoczeniem, jeśli dokładnie to samo zrobi polski Trybunał Konstytucyjny. Będzie się on posługiwał tą samą metodą i będzie musiał przeanalizować te same argumenty za i przeciw. Być może da to inny wynik, bo Trybunał Konstytucyjny inaczej wyważy te wartości, ale w mojej ocenie powinniśmy spodziewać się wyroku negatywnego, stwierdzającego niezgodność obecnych przepisów z konstytucją.

Podsumowując, chciałabym powiedzieć, że dzisiejsza debata i argumenty, które zostały w niej podniesione, wskazują, że mamy do czynienia nie tylko z rekomendacją, ale wręcz obowiązkiem podjęcia działań w tym zakresie. No, lepiej zrobić cokolwiek, niż nie zrobić niczego. Wszystkie argumenty, które zostały dzisiaj przedstawione, wskazują, że obowiązek ten staje się coraz bardziej wyraźny i już wkrótce będzie realnie spoczywał czy to na Radzie Ministrów, która nadzoruje służby, czy też na ustawodawcy, a więc na Sejmie i Senacie. Problem ten prawdopodobnie już za chwilę okaże się naglący, więc lepiej zacząć myśleć nad nim już teraz, a nie dopiero wtedy, kiedy Trybunał Konstytucyjny wyda wyrok o niekonstytucyjności tych przepisów. Bardzo dziękuję państwu za uwagę.

Generalny Inspektor Ochrony Danych Osobowych Wojciech Wiewiórowski:

Bardzo serdecznie dziękuję.

Proszę państwa, 21 maja 2011 r. Naczelna Rada Adwokacka zorganizowała konferencję „Retencja danych: troska o bezpieczeństwo czy inwigilacja obywateli?”. Była to próba przyjrzenia się bardzo niepełnym jeszcze i nie do końca przeanalizowanym danym statystycznym, które zaczęły się wtedy pojawiać. Chodziło o skonfrontowanie dyskusji, która toczyła się w różnych mediach, z tym, co tak naprawdę sądzą na ten temat prawnicy.

W związku z tym chciałbym poprosić o wystąpienie pana mecenasa Pietrzaka reprezentującego Naczelną Radę Adwokacką, który zajmie się problemem skutecznych środków indywidualnej kontroli legalności korzystania z danych telekomunikacyjnych przez władze publiczne.

Państwo adwokaci zaproponowali dyskusję na temat przyszłościowych rozwiązań już w 2011 r., kiedy dane były jeszcze bardzo niedokładne. Dziś mamy troszkę inną sytuację, bo jesteśmy już po kontrolach, które zostały przeprowadzone przez Najwyższą Izbę Kontroli. Ich wyniki były prezentowane również polskiemu ustawodawcy, tak że mamy już troszeczkę lepszy obraz tego, jak realizacja obowiązków związanych z prawem telekomunikacyjnym i retencją danych wygląda od strony praktycznej.

Panie Mecenasie, zapraszam.

Przewodniczący Komisji Praw Człowieka w Naczelnej Radzie Adwokackiej Mikołaj Pietrzak:

Panie Przewodniczący! Panie Ministrze! Panowie Senatorowie! Szanowni Państwo!

W imieniu Naczelnej Rady Adwokackiej bardzo dziękuję za zaproszenie i za możliwość zabrania głosu na dzisiejszym seminarium.

Proszę państwa, satysfakcja, jaka płynie z faktu, że Naczelna Rada Adwokacka już w 2011 r. zauważyła pewne niebezpieczeństwa, które ostatnio zostały rozpoznane także przez Trybunał Sprawiedliwości, jest satysfakcją gorzką. Nie chciałbym powtarzać argumentów i tez, które padły już dzisiaj ze strony moich przedmówców, tak więc skupię się na analizie znaczenia tego orzeczenia pod kątem praw i wolności jednostki, ponieważ to do ich ochrony powołana jest przecież adwokatura.

Proszę państwa, w sytuacji, kiedy władza publiczna ingeruje w dowolne konstytucyjnie czy konwencyjnie chronione prawa i wolności jednostki, normą jest to, że jednostce tej przyznaje się jakieś środki zaradcze, tak żeby mogła ona skontrolować legalność i zasadność tego rodzaju ingerencji. Zazwyczaj środkiem tym jest możliwość wystosowania, w takiej czy innej postaci, indywidualnej petycji do sądu. Nie zawsze zajmują się tym sądy administracyjne, ale w każdym razie zwykle istnieje możliwość zwrócenia się w tej sprawie do jakiegoś niezależnego organu.

W przypadku sięgnięcia po dane telekomunikacyjne takiej kontroli jednak nie ma. Jednostka jest tutaj absolutnie bezradna, ponieważ nie dostaje żadnych informacji o tym, że była kontrolowana czy też że pozyskano jej dane, a nawet jeżeli zdobędzie tego rodzaju informacje, to i tak nie przysługuje jej żadne prawo do zweryfikowania legalności i zasadności wykorzystania tych danych przez służby. O tym także traktowało orzeczenie Trybunału Sprawiedliwości Unii Europejskiej, w którym była mowa o braku proceduralnych gwarancji osłaniających jednostkę przed nadużyciami.

Prowadzi to do pytania, jak mają wyglądać przyszłe gwarancje dla jednostki. Jak chronić jednostkę przed nadużyciami? Naturalną odpowiedzią ze strony adwokatury jest to, by otworzyć drogę sądową. Argument ten, który przecież nie pada na tej sali po raz pierwszy, często spotyka się jednak z krytyką ze strony służb specjalnych i władzy publicznej. Pada odpowiedź, że nie da się tego zrobić, bo przypadków, w których sięga się po dane telekomunikacyjne, jest zbyt wiele, by można było wszystkie indywidualnie skontrolować.

Proszę państwa, nie ulegajmy tego rodzaju argumentacji. Jest ona zbudowana na pewnym fałszywym obrazie polegającym na wrzucaniu wszystkich danych telekomunikacyjnych do jednego worka. Taką argumentację napiętnował także Trybunał Sprawiedliwości, który nakazuje inaczej traktować dane abonenckie, inaczej tak zwane bilingi, a jeszcze inaczej dane dotyczące BTS, czyli dane pozwalające ustalić, gdzie się kto znajdował w momencie wykonywania połączenia. To zróżnicowanie pozwala także na nadanie innego reżimu gwarancyjnego każdej z tych kategorii danych. Oczywiście sięgnięcie po dane abonenckie,

na przykład ustalenie, kto wykupił dany numer telefonu, jest mniejszą ingerencją w prawa i wolności jednostki niż ustalenie, kiedy i do kogo dana osoba dzwoniła, jak długo trwała rozmowa, a przede wszystkim gdzie abonent w trakcie tej rozmowy się znajdował. Na to wszystko uwagę zwrócił Trybunał Sprawiedliwości. Niektóre służby ujawniają informacje o tym, w jakim stopniu korzystają z danych telekomunikacyjnych, a inne nie, ale musimy to oceniać, uwzględniając podział na rodzaje tych danych. Oczywiście można argumentować, że jeżeli chodzi o sięganie po dane abonenckie, to reżim gwarancyjny może być mniejszy. Przedstawiciele służb specjalnych i Policji mówią, że jest to po prostu zajrzenie do książki telefonicznej. No, jest w tym pewna logika, ale sięganie po dane dotyczące połączeń i miejsca pobytu jest już zupełnie czym innym.

Wyprzedzając dalszą dyskusję, chciałbym zauważyć, że argumenty, które zazwyczaj padają ze strony obecnych tutaj w dniu dzisiejszym przedstawicieli służb specjalnych, wskazują na to, że są to dane, które... Przepraszam, jestem w niezręcznej sytuacji, ponieważ muszę te argumenty antycypować. Chodzi o to, że są to dane, które służby muszą dostawać błyskawicznie, w związku z czym nie można tego kontrolować. Proszę państwa, kodeks postępowania karnego przewiduje przecież instytucję kontroli ex post, na przykład w przypadku podsłuchu procesowego. Jeżeli więc trzeba pilnie sięgnąć po dane telekomunikacyjne, to przecież istnieje możliwość wykonania tej czynności, ale potem trzeba ją poddać kontroli zasadności i legalności. To jest możliwe, polskie prawo przewiduje takie sytuacje. Podkreślam jednak jeszcze raz, że nie wszystkie przypadki sięgania po dane telekomunikacyjne – mam na myśli dane abonenckie – muszą podlegać tego rodzaju reżimowi.

Padają też takie argumenty, że nie możemy ujawniać sięgnięcia po dane telekomunikacyjne określonej osoby w przypadku wywiadu i kontrwywiadu, ponieważ tym samym odtajnilibyśmy działalność służącą bezpieczeństwu państwa. No, są przecież systemy, w których stosuje się swego rodzaju reprezentację zaoczną, za pośrednictwem specjalnie do tego celu wyznaczonych rzeczników. Jeżeli mamy do czynienia z sytuacją, w której pewne osoby nie mogą bronić się bezpośrednio ani być reprezentowane przez wybranego przez siebie pełnomocnika, to może powinniśmy stworzyć system, w którym interesy tych osób reprezentować będą niezależni strukturalnie rzecznicy. To jest wykonalne, choć oczywiście musielibyśmy się zastanowić, czy miałyby to podlegać rzecznikowi praw obywatelskich, prokuratorowi generalnemu czy GİODO. A może do tego celu powinni być wyznaczani indywidualni adwokaci czy radcowie prawni?

Nieprawdą jest też to, że informacje dotyczące siatki połączeń i miejsca pobytu danej osoby w trakcie rozmowy telefonicznej nie mają większego znaczenia. Trybunał świetnie zilustrował to w swoim orzeczeniu. Argumenty, które przedstawię, padały już w 2011 r., ponieważ są one oczywiste dla każdego, kto w dzisiejszych czasach zajmuje się procesami karnymi. Otóż bardzo często w procesie karnym najważniejszym dowodem nie jest już to, co kto powiedział w trakcie podsłuchiwanej rozmowy telefonicznej. To nie treść rozmowy jest istotna dla ustalenia winy lub jej braku. Ważniejsze jest to, gdzie się kto znajdował,

a także jak długo i z kim rozmawiał. To są często informacje o dużo donioślejszym znaczeniu niż treść samej rozmowy, dlatego potencjalnie mogą one naruszać prawa i wolności jednostki jeszcze bardziej niż klasyczna kontrola operacyjna, czyli podsłuch.

Żebyśmy mogli mówić o skutecznej kontroli indywidualnej w duchu orzeczenia Trybunału Sprawiedliwości Unii Europejskiej, musimy jasno określić cele, w jakich dopuszczalne będzie sięgnięcie po retencjonowane dane telekomunikacyjne, a także zakres przedmiotowy tych danych. Bez doprecyzowania przesłanek materialnych dotyczących korzystania z nich przez służby specjalne i policyjne nawet wspomniane wcześniej instrumenty proceduralne, czyli na przykład sądowe, będą wyłącznie pozorne. Dlaczego? Ponieważ żeby skontrolować legalność, zasadność i celowość wykorzystania danych, te trzy cechy muszą odnosić się do jakiegoś normatywnego reżimu. Musimy określić materialne przesłanki dopuszczalności sięgania po retencjonowane dane telekomunikacyjne. Chodzi tutaj chociażby o rodzaj przestępczości, jakiej chcemy w ten sposób zapobiegać. O tym także mówił Trybunał Sprawiedliwości.

(Wypowiedź poza mikrofonem)

W takim razie bardzo dziękuję. Wiele z tego, co chciałem powiedzieć, już tutaj padło, w związku z czym nie będę zajmował państwu więcej czasu. Nie ma sensu powtarzać tych samych argumentów. Uprzejmie dziękuję.

Generalny Inspektor Ochrony Danych Osobowych Wojciech Wiewiórowski:

Bardzo dziękuję, Panie Mecenasie.

Proponuję, żebyśmy przeszli już do dyskusji. Zapraszam państwa do zadawania pytań, jak również do wygłaszania komentarzy w tej sprawie.

Ze względów czysto organizacyjnych proszę tylko o, po pierwsze, krótkie wypowiedzi – już po dwóch minutach będę pokazywał, że mówią państwo za długo – a po drugie, o to, żeby najpierw się przedstawiać.

Widzę, że zgłasza się pan generał Bieńkowski.

Przewodniczący Michał Seweryński:

Jeśli można, to jeszcze ja powiem dwa słowa. Bywalcy posiedzeń naszej komisji o tym wiedzą, ale na samym początku powinienem powiedzieć, że całe nasze posiedzenie jest bezpośrednio transmitowane w internecie. Tak że będzie można skorzystać z tego, co zostało tam utrwalone. Może nie wszyscy państwo o tym wiedzą, więc chciałem tylko uprzedzić.

Dyrektor Departamentu Porządku i Bezpieczeństwa Wewnętrznego w Najwyższej Izbie Kontroli Marek Bieńkowski:

Marek Bieńkowski, dyrektor Departamentu Porządku i Bezpieczeństwa Wewnętrznego w Najwyższej Izbie Kontroli.

Szanowny Panie Przewodniczący! Szanowni Państwo!

Chciałbym, żebyśmy zgodzili się co do tego, co pan minister Wiewiórowski powiedział na początku tego spotkania. Proszę państwa, orzeczenie Trybunału Sprawiedliwości Unii Europejskiej to coś niezwykle interesującego, chociażby z tego względu, że jest ono dosyć radykalne. Niemniej jednak jego wydanie wcale nie powoduje, że rozpoczynamy dyskusję nad tym problemem od początku. Zgadzam się z tezą, że my w Polsce jesteśmy gdzieś w połowie drogi. No, nie popiszę się skromnością, ale jeśli obiektywnie zapoznamy się z wynikami kontroli NIK, to przekonamy się, że wspomniane orzeczenie w istocie potwierdza te ustalenia i rekomendacje, które zgłaszaliśmy państwu już blisko rok temu. To nie jest nic nowego.

Będę mówił króciutko. Bardzo cenne jest to, że w orzeczeniu, podobnie jak w podsumowaniu wyników naszej kontroli, stwierdzono, iż retencja danych jest wręcz niezbędna, jeśli chodzi o skuteczne zwalczanie niektórych rodzajów przestępstw. Co do tego jesteśmy zgodni. Wspominam o tym, bo gdy słucha się pewnych wypowiedzi na posiedzeniach komisji senackiej, która zajmuje się tym problemem... Zresztą ja reprezentuje NIK również przed Trybunałem Konstytucyjnym. Otóż służby chcą jak gdyby narzucić wszystkim opinię, że my dążymy do tego, by w ogóle zaprzestać korzystania z tego instrumentu. Oczywiście jest to nieprawdą. Nikt zdrowo myślący nie powie, że w Polsce nie powinniśmy stosować tego instrumentu wtedy, gdy jest to konieczne.

Stwierdziliśmy również, że konieczne jest przygotowanie katalogu spraw, których miałyby dotyczyć retencja danych telekomunikacyjnych. I to jest kwestia do dyskusji. Przypominam, że jeśli ktoś ma inne zdanie w tej sprawie, to pan przewodniczący wyznaczył konkretny termin, do którego można zgłaszać swoje propozycje i uwagi dotyczące między innymi tego właśnie katalogu.

Proszę państwa, moim zdaniem istotą rzeczy jest to, czy... No, rzeczywiście jesteśmy epatowani liczbami. Trudno powiedzieć, czy milion osiemset zapytań rocznie to dużo, czy mało. Oczywiście jeśli porównamy, tak jak zrobił to pan profesor, te nasze prawie dwa miliony z danymi unijnymi, to wyjdzie nam, że jest to dokładnie 50% zapytań ze wszystkich innych krajów Unii Europejskiej, niemniej jednak dla mnie o wiele bardziej interesujące byłoby uzyskanie odpowiedzi, czy ten instrument jest efektywny. Dopiero wtedy moglibyśmy to wszystko porównać i ocenić, czy jest on stosowany sensownie, czy też nie.

Stwierdziliśmy również, że konieczna jest kontrola zewnętrzna. Oczywiście jeśli chodzi o formę tej kontroli, to myślę, że powinna się odbyć pogłębiona dyskusja na ten temat.

Zwróciliśmy też uwagę na to, że w Polsce bardzo mocno szwankuje sprawozdawczość i metodologia badań. Moim zdaniem istnieje różnica między liczbą zapytań a liczbą udzielonych odpowiedzi. Warto o tym pomyśleć.

Myślę, że należy dalej toczyć tę dyskusję i mówić o prawnych konsekwencjach tego orzeczenia Trybunału Sprawiedliwości Unii Europejskiej. Konkludując, chciałbym uspokoić służby specjalne, że nikt nie zamierza pozbawić ich instrumentu, o którym dziś mówimy. Niemniej jednak myślę, że nie czekając na rozstrzygnięcia unijne, powinniśmy nadal spokojnie i merytorycznie pracować nad polskimi rozwiązaniami w tych obszarach, które zakwestionował Trybunał Sprawiedliwości. Dziękuję bardzo.

**Generalny Inspektor
Ochrony Danych Osobowych
Wojciech Wiewiórowski:**

Dziękuję bardzo, Panie Dyrektorze.
Zapraszam do zabrania głosu kolejnej osoby.

Nagle zapadła cisza. Wszyscy są zamyśleni, a przecież widziałem, że jakieś komentarze pojawiały się już w trakcie wypowiedzi prelegentów.

O, widzę, że pan mecenas Pietrzak chciałby wziąć udział w debacie.

**Przewodniczący Komisji Praw Człowieka
w Naczelnej Radzie Adwokackiej
Mikołaj Pietrzak:**

Korzystając z chwilowego zastoju, chciałbym uzupełnić swoją wypowiedź o jedną uwagę. Mianowicie mówiąc o kontroli indywidualnej wykonywanej przez sądy, mam na myśli kontrolę kontrydiktoryjną. Dlaczego? Dobrym punktem odniesienia jest tutaj sposób, w jaki sądy kontrolują – czy też pozornie kontrolują – podsłuchy. Przed Trybunałem Konstytucyjnym prezes sądu okręgowego z jakiegoś powodu nie chciał nam przekazać danych dotyczących liczby tych podsłuchów, ale z tego, co wiemy z innych sądów, wynika, że ogromna, przerażająca większość wniosków kierowanych do sądów przez służby specjalne i służby policyjne – cały czas mam na myśli kontrolę operacyjną, czyli podsłuchy – jest akceptowana. I służby specjalne chętnie się tym faktem. Ich zdaniem to jest bardzo dobre zjawisko, bo świadczy o tym, że ich wnioski są tak dobrze napisane. Ja jednak dopatruję się w tym zupełnie innego zjawiska. Otóż ta kontrola sądowa jest pozorna. Dlaczego? Ponieważ w takim postępowaniu nie ma drugiej strony. Wniosek do sądu kieruje władza publiczna, ale nie ma tam miejsca dla osoby podsłuchiwanej ani dla kogoś, kto mógłby zabrać głos w jej imieniu. Jeżeli sąd zaakceptuje taki wniosek, to nikt nie złoży zażalenia, bo nie ma odpowiedniego mechanizmu. Jeżeli zaś sąd nie uwzględni wniosku, to zażalenie ma gwarantowane, a jego orzeczenie może zostać, nie daj Boże, uchylone. Dlatego proszę, byśmy kreując mechanizm gwarancji procesowej dla jednostki, uwzględnili konieczność wysłuchania drugiej strony. *Audiatur et altera pars*. Jeżeli jednostka nie będzie reprezentowana chociażby przez wspomnianego specjalnego rzecznika, który pod jej nieobecność może występować w jej imieniu, to ten proces kontrolny będzie równie pozorny jak teraz w przypadku kontroli operacyjnej. Dziękuję.

**Generalny Inspektor
Ochrony Danych Osobowych
Wojciech Wiewiórowski:**

Dziękuję bardzo.

Zapraszam do debaty. Podczas spotkań Polskiej Platformy Bezpieczeństwa Wewnętrznego słyszałem też bardzo dobrze uargumentowane głosy sprzeciwu wobec takiego stanowiska, tak więc zachęcam również do tego,

żeby polemizować ze stwierdzeniami, które się tutaj pojawiały. Zwłaszcza że nawet sami prelegenci nie byli zgodni, jeżeli chodzi o spojrzenie na aspekty praktyczne.

Spoglądam na pozostałych prelegentów i widzę, że jako pierwszy rękę podnosi pan profesor Adamski.

**Kierownik Katedry Prawa Karnego
i Polityki Kryminalnej
na Wydziale Prawa i Administracji
na Uniwersytecie Mikołaja Kopernika
w Toruniu Andrzej Adamski:**

Aspekty praktyczne są oczywiście niezwykle ważne nie tylko ze względów poznawczych, ale także z uwagi na rozstrzygnięcia, jakie mają zapaść – miejmy nadzieję, że w możliwie szybkim czasie – w Trybunale Konstytucyjnym. Jeden z elementów zasady proporcjonalności, która niewątpliwie będzie, jak słyszeliśmy w jednej z wypowiedzi, pewnym, że tak powiem, wzorcem procedowania w tej sprawie, zakłada, że kryterium konieczności – nie legalności, ale właśnie konieczności – użycia środka głęboko ingerującego w sferę praw i wolności obywatelskich wymaga empirycznego dowodu ich skuteczności. No, jeżeli mamy do wyboru łagodniejszą wersję tego środka, a z badań wynika, że daje ona podobne rezultaty, to wniosek wydaje się oczywisty.

Obawiam się, że w naszych polskich realiach przeprowadzenie w tym zakresie poprawnych pod względem metodologicznym badań byłoby niezwykle skomplikowane. Spójrzmy jednak na różnego rodzaju zagraniczne raporty, zwłaszcza pewnej niemieckiej organizacji pozarządowej, która bardzo angażuje się w tę problematykę. Zawierają one cały zestaw badań sprawdzających, czy instytucja retencji danych rzeczywiście daje pozytywne efekty, jeżeli chodzi o obniżenie poziomu przestępczości bądź podwyższenie wskaźników wykrywalności poważnych przestępstw. Otóż dane te, niezależnie od tego, czy pochodzą z Republiki Federalnej Niemiec, z Czech czy z Austrii, właściwie prezentują się podobnie i dają podstawy do sformułowania konkluzji, że nie ma korelacji pomiędzy stosowaniem retencji danych a poprawą wskaźników dotyczących poziomu przestępczości. Co więcej, czasami widać korelację, że tak powiem, negatywną. Zdarza się tak, że w okresie po wprowadzeniu retencji danych wykrywalność przestępstw jest gorsza, a poziom przestępczości wyższy. I to jest pierwsza kwestia, jeżeli chodzi o analizę tego zjawiska. No, ponieważ zajmuję się kryminologią w Polsce od ładnych paru lat, wiem, że polski system rejestracji przestępstw nie jest niestety porównywalny z niemieckim systemem opracowanym przez Bundeskriminalamt, która to instytucja działa według bardzo rygorystycznych zasad. Tak więc nawet gdybyśmy spróbowali przeprowadzić jakiś test na wzór wspomnianych badań zagranicznych, wiarygodność naszych polskich danych budziłaby spore wątpliwości.

Konkluzje wynikające z tych badań są niezwykle sugestywne również w odniesieniu do zasady proporcjonalności. Mam na myśli głównie badania przeprowadzone przez wykwalifikowanych kryminologów z Instytutu Maxa

Plancka we Freiburgu, którzy zajmują się tego rodzaju analizami w sposób profesjonalny. Otóż badania te pokazały, że proporcje, z jakimi mamy do czynienia w RFN, wyglądają następująco: odsetek postępowań karnych, w których dane telekomunikacyjne odegrały istotną rolę, wynosi 0,01%. Z kolei informacje, które są gromadzone w ramach retencji danych telekomunikacyjnych, w 97% dotyczą niewinnych obywateli. Brakujące 3% to ten margines, w stosunku do którego użycie określenia „niewinny obywatel” nie jest zbyt adekwatne. Tak więc z tego rodzaju danych empirycznych wynika bardzo proste spostrzeżenie. Ta równowaga jest tak mocno zachwiana, że mówienie o zachowaniu zasady proporcjonalności wydaje się mieć charakter raczej anegdotyczny.

Podsumowując, myślę, że powinniśmy przeprowadzić tego rodzaju test również w Polsce, bo rozstrzygnięcia trzeba szukać w sferze tak zwanych twardych faktów. To tyle. Dziękuję bardzo.

(Dyrektor Departamentu Porządku i Bezpieczeństwa Wewnętrznego w Najwyższej Izbie Kontroli Marek Bieńkowski: Nie zgadzam się z panem.)

Generalny Inspektor Ochrony Danych Osobowych Wojciech Wiewiórowski:

Dziękuję bardzo, Panie Profesorze.
Teraz pan dyrektor Bieńkowski. Proszę bardzo.

Dyrektor Departamentu Porządku i Bezpieczeństwa Wewnętrznego w Najwyższej Izbie Kontroli Marek Bieńkowski:

Panie Profesorze, są pewne rodzaje przestępstw – klasycznym przykładem jest tutaj uporczywe nękanie – których nie da się udowodnić w procesie, jeśli nie zastosuje się wspomnianego mechanizmu dotyczącego retencji danych. W związku z tym byłbym daleki od oceniania tego mechanizmu w kontekście całej przestępczości.

Niemniej jednak ja też myślę, że warto popracować nad metodyką badań, które dałyby nam odpowiedź na te wszystkie pytania. Wcześniej przywołał pan dosyć interesujący przykład holenderski. My w Polsce nie mamy wiedzy, w ilu wyrokach rocznie uwzględnia się zastosowanie tego rodzaju mechanizmu, a myślę, że byłaby to interesująca wiedza.

Wsluchuję się też w głosy koleżanek i kolegów ze służb i myślę, że trzeba będzie dojść do jakiegoś kompromisu. No, są takie sytuacje, które nie mieszczą się w kategoriach tej uchylonej dyrektywy. Myślę na przykład o takiej sytuacji, kiedy poszukuje się osoby, której po prostu nie sposób znaleźć bez zastosowania danych dotyczących BTS.

Problem jest bardzo złożony, ale diskutujmy o jego rozwiązaniu. Nie zakładajmy, że i tak nie znajdziemy dobrej metodologii, która przybliżyłaby nas do... No, chodzi o to, że warto dyskutować o efektywności stosowania tego mechanizmu. Dziękuję.

Kierownik Katedry Prawa Karnego i Polityki Kryminalnej na Wydziale Prawa i Administracji na Uniwersytecie Mikołaja Kopernika w Toruniu Andrzej Adamski:

Ad vocem. Oczywiście zgadzam się z panem. Ja też jestem przekonany, że są takie kategorie przestępstw, w przypadku których bez tego instrumentu w ogóle nie można wykryć sprawców. Nazwy tych przestępstw mają zwykle przedrostek „cyber”. Prawda? To jest jasne. Powiedziałem tylko tyle, że ogólne dane ze statystyki policyjnej nie wyglądają zbyt dobrze. Dziękuję bardzo.

Generalny Inspektor Ochrony Danych Osobowych Wojciech Wiewiórowski:

Pani Szymielewicz.

Prezes Zarządu Fundacji „Panoptikon” Katarzyna Szymielewicz:

Dziękuję bardzo

Ja też chciałabym wypowiedzieć się ad vocem tej dyskusji, bo wydaje mi się ona ciekawa. Dotykamy tutaj ważnego problemu, z którym borykamy się w Polsce, a o którym Trybunał Sprawiedliwości Unii Europejskiej, o ile mi wiadomo, w swoim wyroku się nie wypowiedział. Mianowicie chodzi o sprawozdania. Wydaje mi się, że bardzo niepokojące przykłady tego, jak źle można je przygotowywać, zobaczyliśmy już wówczas, kiedy Komisja Europejska poprosiła państwa członkowskie o przedstawienie danych na poparcie tezy, że retencja danych jest potrzebna. To było dwa lata temu, kiedy Komisja prowadziła ewaluację dyrektywy. Zresztą od początku było wiadomo, że zostanie ona przeprowadzona właśnie wówczas, bo wynikało to z samej dyrektywy. Komisja miała nadzieję, że dzięki temu, że w dyrektywie uwzględniono obowiązek sprawozdawczy, uda się zgromadzić przekonujące dowody na to, że retencja jest niezbędna, i odpowiedzieć na pytanie, w jakim zakresie należy ją stosować. I co się okazało? Państwo na pewno o tym wiecie, ale warto to powtórzyć. Otóż żaden kraj nie był w stanie przedstawić wyczerpującej analizy tego, o czym tu rozmawiamy, czyli wykazać, w których sytuacjach wykrycie przestępstwa bez tego instrumentu faktycznie byłoby niemożliwe. Jedyne, co usłyszeliśmy, to anegdota, że w tej oto sprawie dane te okazały się bardzo cenne, a bez nich Policja zapewne byłaby bezradna. Nie były to dowody, ale jedynie anegdotyczne przykłady oraz statystyki, z których niewiele wynikało.

Ta korelacja, jak wszyscy wiemy, nie jest bezpośrednia. To, że jakieś przestępstwo zostało wykryte dzięki retencjonowanym danym, nie znaczy, że nie zostałyby wykryte bez tego instrumentu albo z wykorzystaniem innego narzędzia, o którym jeszcze nie rozmawialiśmy. Może więc warto o tym powiedzieć. Chodzi o zamrażanie danych. Przecież nie mówimy tutaj o sytuacji zero-jedynkowej. Oprócz retencji i braku retencji jest jeszcze coś pomiędzy, a mianowicie możliwość szybkiego zamrożenia danych,

które przechowują operatorzy i inne firmy. Istnieje bardzo wiele firm, które posiadają takie czy inne dane, więc mogłyby one zamrażać te informacje na życzenie Policji i przechowywać nawet tak długo jak w przypadku retencji. Chodziłoby jednak o dane tylko tych osób, które są podejrzane, a nie o owe pozostałe 97%.

Tak więc jest to poważny problem. Trybunał nie mówił o tej kwestii, ale my musimy rozmawiać o tym, jak przebudować naszą sprawozdawczość, tak aby nie było więcej takich absurdów, jakie Najwyższa Izba Kontroli drobniawo opisała w swoim raporcie, zresztą doskonałym. Tak więc myślę, że nie powinno zabraknąć tego w naszej dyskusji. Dziękuję.

Generalny Inspektor Ochrony Danych Osobowych Wojciech Wiewiórowski:

Dziękuję bardzo.

Czy ktoś jeszcze chciałby zabrać głos?

Widzę, że pan na końcu się zgłasza. Proszę bardzo.

Dyrektor Departamentu Postępowań Karnych w Agencji Bezpieczeństwa Wewnętrznego Jan Bilkiewicz:

Pułkownik Jan Bilkiewicz, dyrektor Departamentu Postępowań Karnych w ABW.

Ja też miałem przyjemność brać udział we wspomnianym posiedzeniu Trybunału Konstytucyjnego, który w tej chwili rozstrzyga kwestie związane z retencją danych czy też kontrolą operacyjną, tylko że pan mecenas Pietrzak prawdopodobnie był na innej części tego spotkania niż my. W związku z tym nie chcę, żeby te rozwiązania, o których pan mówił, pozostały bez komentarza. To nieprawda, że służby – czy to specjalne, czy policyjne – opierają się przed tego typu uregulowaniem przepisów dotyczących retencji. Jeżeli chodzi o rozwiązanie, o którym mówił pan mecenas, polegające na wprowadzeniu w niektórych przypadkach zgody następczej, to my sami je zaproponowaliśmy.

(Generalny Inspektor Ochrony Danych Osobowych Wojciech Wiewiórowski: Chodzi o kontrolę następczą?)

Tak, o kontrolę. To my to zaproponowaliśmy.

Powtórzę to, co mówił pan generał Bieńkowski. Z całą pewnością najpierw powinniście państwo wysłuchać nas jako praktyków, a rozwiązanie znajdziecie już sami. Przypominam, że my jesteśmy tylko wykonawcami. Wy dajecie nam określone zadania, a służby je wykonują. Stalking, o którym mówił pan generał Bieńkowski, jest tutaj dobrym przykładem. My tylko wskazujemy pewne kwestie, które powinniście państwo brać pod uwagę, przygotowując założenia do nowej ustawy.

Jeżeli chodzi o kontrolę operacyjną, to nie wiem, jakim prawem pan mecenas powiedział, że polskie sądy i prokuratury nieodpowiednio kontrolują służby czy Policję. Chcę panu powiedzieć, że w Prokuraturze Generalnej od lat funkcjonuje komórka, która dokonuje oceny naszych wniosków i ma w tym zakresie wypracowane metody działania. I to jest to pierwsze sito powodujące, że do sądu dochodzą

tylko nieliczne wnioski, które zresztą i tak mogą zostać odrzucone. Ten system kontroli jest wielowarstwowy. Pan chce stworzyć wrażenie, że nie ma tutaj żadnej kontroli, ale w rzeczywistości mamy system kontroli wieloetapowej, jaki nie funkcjonuje w przypadku żadnej innej działalności aniżeli właśnie kontrola operacyjna.

Jeżeli pan uznaje, że dostęp do danych dotyczących BTS narusza prywatność obywatela bardziej niż podsłuchiwanie prowadzonej przez niego rozmowy, to chcę panu powiedzieć, że jest pan w błędzie. Dzięki BTS możemy określić miejsce pobytu danej osoby, na przykład na Mokotowie, z dokładnością do 3 km. O czym my w ogóle rozmawiamy? Chcę pan powiedzieć, że dane dotyczące BTS są bardziej drażliwe niż treść rozmowy prowadzonej pomiędzy stronami? Nie rozumiem tego.

No, jeżeli będą tutaj padały tego typu argumenty, to za chwilę się okaże, że kontrola operacyjna, którą stosujemy... Jeszcze raz zaznaczam, że to wszystko jest kontrolowane przez prokuraturę i przez sąd, nie mówiąc już o kontroli wewnętrznej, która nie musi być tutaj dostrzegana. Jakie jeszcze środki kontroli powinniśmy pana zdaniem zastosować? Mamy kontrolę dwustopniową, realizowaną przez prokuratora, który dba o interesy obywateli, i przez sąd, który dodatkowo jeszcze kontroluje działania prokuratora i służb. Tak więc jeżeli chce pan mówić, że nie ma żadnej kontroli, to proszę bardzo. To tyle. Chciałem to tylko sprostować.

Generalny Inspektor Ochrony Danych Osobowych Wojciech Wiewiórowski:

Bardzo dziękuję za ten głos.

Myślę, że jest to dobry moment na to, żebyśmy zaczęli podsumowywać tę debatę. Otóż ja podsumuję ją stwierdzeniem, że na temat pewnych braków w polskich przepisach dotyczących tej sprawy dyskutujemy od wielu lat. Przepisy te zmieniano już dwukrotnie i za każdym razem ogłaszano sukces polegający na pozbyciu się błędów, które pojawiły się w momencie implementacji dyrektywy retencyjnej. Po pewnym czasie nasza dyskusja wraca jednak do punktu wyjścia, czyli do pytania, na ile działania, o których tutaj mówimy, są potrzebne. No, wbrew pozorom większość osób stwierdza, że Policja i służby muszą mieć, przynajmniej w pewnym zakresie, dostęp do danych telekomunikacyjnych.

Kolejna kwestia to katalog przestępstw, w przypadku których mogą być podejmowane tego typu działania. Przypominam, że swego czasu generalny inspektor ochrony danych osobowych zapytał służby oraz Policję o to, jakie przestępstwa kwalifikowane są jako przestępstwa poważne, na co od różnych służb dostał bardzo różne odpowiedzi. Były wśród nich takie stwierdzenia, że wszystkie działania, którymi zajmuje się dana służba, dotyczą poważnych przestępstw, ale dostaliśmy również informację, że w różnych służbach istnieją różne instrukcje w tej sprawie, tak więc można powiedzieć, że służby te czekają na jakieś odgórne wskazania. I to jest jeden z punktów, co do którego wszyscy chyba się zgadzają. Nie może być tak, że przepisujemy coś z nieistniejącej już dyrektywy i uznajemy, że sprawa jest załatwiona. Niezbędne jest określenie tego, o jakiego rodzaju przestępstwa tutaj chodzi.

No i zostaje nam jeszcze, jak słusznie podkreśliła przedstawicielka Helsińskiej Fundacji Praw Człowieka, kwestia testu proporcjonalności. Pewne standardy w tym zakresie wyznaczył Trybunał Sprawiedliwości Unii Europejskiej w Luksemburgu, ponieważ tak naprawdę test ten przeprowadza się tak samo zarówno pod kątem Karty Praw Podstawowych, jak i pod kątem zasad wynikających z konstytucji poszczególnych krajów. Może po raz pierwszy wyrażę tutaj swoją własną opinię. Otóż mam wrażenie, że wolności chronione w Karcie Praw Podstawowych i wolności, które są objęte ochroną w art. 47, art. 49 i art. 51 Konstytucji Rzeczypospolitej Polskiej, wbrew pozorom są bardzo zbliżone, prawie identyczne. Oznacza to, że wspomniany test da się przeprowadzić również u nas, tak więc mam nadzieję, że wkrótce do tego dojdzie. Zresztą nawet to, ile czasu Trybunał Konstytucyjny przeznaczą na rozważenie kwestii związanych ze zgłoszonymi skargami, wskazuje, jak poważnie nasi sędziowie zajęli się tym zagadnieniem.

Jeszcze raz powracam do tego, co powiedziałem na samym początku. Ze względu na prace nad zmianami w prawie, które już się rozpoczęły, bardzo się cieszę, że mogliśmy przedyskutować tę sprawę właśnie na posiedzeniu państwa komisji.

Panie Profesorze, oddaję panu głos.

Przewodniczący Michał Seweryński:

Dziękuję, Panie Ministrze.

Proszę państwa, senacka Komisja Praw Człowieka, Praworządności i Petycji – właśnie dlatego, że nazywa się tak, a nie inaczej – sprawą, która jest przedmiotem dzisiejszej debaty, zajęła się już dość dawno temu. Muszę zaznaczyć, że zainteresowaliśmy się nią głównie z inspiracji Najwyższej Izby Kontroli. Zresztą kiedyś otrzymaliśmy sprawozdanie na ten temat, odbyliśmy jeszcze dodatkowe, specjalne posiedzenie z udziałem prezesa NIK.

Wszyscy mamy świadomość, że mówimy o sprawach niezwykle ważnych. Myślę, że dzisiejsza debata przyczyniła się do ugruntowania tej opinii. Na jednej szali naszych rozważań musimy położyć zapewnienie bezpieczeństwa państwu i obywatelom – bo przecież środki, o których mówimy, stosowane są w tym właśnie celu – a na drugiej prawo obywateli do tego, żeby ich życie prywatne nie było przedmiotem nadmiernego zainteresowania ze strony państwa. No, powstaje tutaj pytanie o dopuszczalny zakres takiego zainteresowania. Przecież obywatel na ogół w ogóle nie ma pojęcia, że wokół niego koncentrują się działania jakichś służb.

No i musimy jeszcze uwzględnić błyskawiczny postęp techniczny, który sprawia, że uzyskiwanie tego rodzaju danych staje się coraz łatwiejsze. I nie dotyczy to tylko uprawnionych do tego służb. Kiedy patrzy się na to z punktu

widzenia obywateli, widać, że mają oni prawo czuć się bezradni. Nie tylko zagrożeni, ale wręcz bezradni, bo nikt nie jest w stanie się przed tym obronić. Dzisiaj nawet jakaś pojedyncza utalentowana osoba może przy pomocy bardzo niewyszukanych środków uzyskać całkowity wgląd w to, o czym mówimy i piszemy. Ludzie, którzy chcieliby uzyskać dostęp do naszych danych, mają do dyspozycji coraz to nowsze, coraz to bardziej wyrafinowane środki. Stajemy się coraz bardziej transparentni dla tych, którzy się nami interesują. Żyjemy w kraju praworządnym, więc musimy bronić się przed tym za pomocą środków prawnych. Przypuszczam jednak, że istnieje ogromna dysproporcja pomiędzy tymi środkami, które może nam zagwarantować prawo, a środkami technicznymi, które są do dyspozycji ludzi chcących zbierać informacje na nasz temat. Wyważenie tych dwóch spraw jest niezwykle istotne w każdym państwie demokratycznym.

Nie przypadkiem Najwyższa Izba Kontroli zwraca na to uwagę w swoim rocznym sprawozdaniu i nie przypadkiem uchylona została dyrektywa retencyjna. No, okazuje się, że próba regulacji na szczeblu europejskim również zawiodła. To jest właściwie przyznanie się do tego, że ta regulacja była nietrafiona, nieskuteczna, niedobra. Teraz to zadanie spada na nas. Musimy szukać jakiejś ochrony na gruncie prawa krajowego. Myślę, że nasza dzisiejsza debata wielu osobom powinna dać do myślenia. Poszerzyliśmy zakres naszej wiedzy na temat tej sprawy, więc instytucje, które są już w jakiś sposób włączone w proces ulepszania prawa w tej dziedzinie, będą miały trochę lepszą podstawę do działania. Poza tym wkrótce musi zapaść jakieś orzeczenie Trybunału Konstytucyjnego, a nasza komisja prowadzi bardzo zaawansowane prace dotyczące inicjatywy ustawodawczej w tej sprawie. No, dane, które przedstawiła Najwyższa Izba Kontroli, są takie, że parlament nie może pozostać wobec nich obojętny.

Powiem państwu, że mieliśmy nawet specjalne spotkanie z prezesem Najwyższej Izby Kontroli. Odbyło się ono u pana marszałka Senatu, co dowodzi wagi tej sprawy. Obie strony uznały, że ta inicjatywa ustawodawcza powinna zostać nie tylko podjęta, ale i doprowadzona do końca. Tak więc liczę na to, że w dalszej fazie prac naszej komisji zechcą państwo przyjąć zaproszenie do współpracy. Będziemy mogli wtedy doprecyzować ten projekt, o którym mówimy, bo sprawa rzeczywiście jest niezwykle doniosła.

Ciągle jednak stawiam sobie pytanie, co możemy osiągnąć za pomocą środków prawnych, skoro po drugiej stronie stoi taka potężna technika, która przekracza nawet naszą wyobraźnię.

Dziękuję wszystkim referentom. Dziękuję panu ministrowi, który zachęcił nas, żebyśmy odbyli taką debatę. Naturalnie dziękuję również panom senatorom. Dziękuję wszystkim państwu.

Zamykam posiedzenie komisji.

(Koniec posiedzenia o godzinie 15 minut 49)

Kancelaria Senatu

Opracowanie:

Biuro Prac Senackich, Dział Stenogramów

Druk i łamanie: Biuro Informatyki, Dział Edycji i Poligrafii