RZECZNIK PRAW OBYWATELSKICH

Adam Bodnar

Warszawa, 4 stycznia 2016 r.

VII.501.178.2015.MW

Pani
Anna Streżyńska
Minister Cyfryzacji
ul. Królewska 27
00-060 Warszawa

Do Sejmu wpłynął poselski projekt ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk nr 154). Projekt ustawy przewiduje nowelizację: ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2015 r., poz. 355 ze zm.), ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2014 r. poz. 1402 ze zm.), ustawy z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2015 r. poz. 553 ze zm.), ustawy z dnia 21 sierpnia 1997 r. – Prawo o ustroju sądów wojskowych (Dz. U. z 2012 r. poz. 952 ze zm.), ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych (Dz. U. z 2015 r. poz. 133 ze zm.), ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. z 2013 r. poz. 568 ze zm.), ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2015 r., poz. 1929 ze zm.), ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422 ze zm.), ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243 ze zm.), ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2014 r. poz. 253 ze zm.), ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2014 r. poz. 1411 ze zm.), ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej (Dz. U. z 2013 r. poz. 1404 ze zm.). Zgodnie z uzasadnieniem dołączonym do projektu ustawy, jej celem jest dostosowanie przepisów ww. ustaw do wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r. (sygn. akt K 23/11).

Analiza projektu ustawy wskazuje jednak, że wykracza on poza wskazany wyżej cel i przewiduje również uregulowanie innych zagadnień, istotnych z punktu widzenia praw i wolności obywatelskich. Jest to m.in. problematyka dostępu przez Policję i inne wymienione służby do danych internetowych w ramach czynności operacyjno-rozpoznawczych. Rzecznik Praw Obywatelskich, działając na podstawie art. 16 ust. 1 w zw. z art. 8 ustawy z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. z 2014 r., poz. 1648 ze zm.), uznał za konieczne przedstawienie Ministrowi Cyfryzacji oceny w zakresie zgodności projektowanych przepisów ustawy z Konstytucją RP w odniesieniu do uzyskiwania i przetwarzania danych internetowych.

Ocena proponowanych rozwiązań prawnych wymaga odwołania się do wzorców prawnych wyrażonych w Konstytucji RP, a mianowicie do ochrony godności człowieka (art. 30 Konstytucji RP), wolności człowieka (art. 31 ust. 1 i 2 Konstytucji RP), ochrony życia prywatnego (art. 47 Konstytucji RP), wolności i ochrony tajemnicy komunikowania się (art. 49 Konstytucji RP) oraz ochrony informacji o sobie (art. 51 Konstytucji RP). Do pełnej rekonstrukcji wzorców kontroli konieczne jest uwzględnienie także art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności, sporządzonej w Rzymie dnia 4 listopada 1950 r. (Dz. U. z 1993 r., nr 61 poz. 284 ze zm. wynikającymi z protokołów; dalej jako: Konwencja), a także art. 7 i 8 Karty Praw Podstawowych Unii Europejskiej, której w art. 6 Traktatu o Unii Europejskiej przyznano moc prawną równą traktatom (Dz. U. z 2009 r., nr 203, poz. 1569). Prawidłowe ustalenie treści wskazanych wzorców oceny wymaga także analizy orzecznictwa Trybunału Konstytucyjnego, Europejskiego Trybunału Praw Człowieka (ETPC) oraz Trybunału Sprawiedliwości Unii Europejskiej (TSUE).

Status człowieka w demokratycznym państwie prawa opiera się na poszanowaniu jego przyrodzonej i niezbywalnej godności (art. 30 Konstytucji RP), a także wynikającej z niej swobody decydowania o swym postępowaniu, zgodnie z własną wolą (art. 31 ust. 1 i 2 Konstytucji RP). Godność człowieka, zgodnie z art. 30 Konstytucji RP, jest nienaruszalna i nie może podlegać żadnym ograniczeniom. Ustawodawca może jednak ingerować w wolność człowieka, na zasadach uregulowanych w art. 31 ust. 3 Konstytucji RP.

Konstytucyjna ochrona wolności człowieka odnosi się przede wszystkim do sfery jego prywatności. Ustrojodawca statuuje prywatność jednostki jako wolność konstytucyjnie chronioną, co oznacza swobodę działania jednostek aż do granic ustanowionych w ustawie. Wyłącznie jednoznaczna regulacja ustawowa może nakładać ograniczenia w zakresie podejmowania określonych zachowań mieszczących się w ramach konkretnej wolności (wyrok TK z 30 lipca 2014 r. o sygn. akt K 23/11). Państwo ma obowiązek prawnego poszanowania i ochrony konstytucyjnych

wolności człowieka, a także powstrzymanie się od ingerowania w wolności zarówno przez państwo, jak i podmioty prywatne. Standard ten odnosi się w szczególności do wolności osobistych, do których – obok wyrażonej w art. 47 Konstytucji RP prywatności – zaliczają się również wolność komunikowania się (art. 49 Konstytucji RP), czy szeroko rozumiana autonomia informacyjna (art. 51 Konstytucji RP). Ochrona prywatności i autonomii informacyjnej jest konsekwencją ochrony przyrodzonej i niezbywalnej godności człowieka (wyrok TK z 12 grudnia 2005 r. o sygn. akt K 32/04).

Jak przyjmuje się w orzecznictwie, art. 47 i 51 Konstytucji RP chronią tę samą wartość konstytucyjną – sferę prywatności. Autonomia informacyjna stanowi istotny element składowy prawa do ochrony prywatności, a polega na samodzielnym decydowaniu o ujawnianiu innym podmiotom informacji dotyczących własnej osoby, a także na sprawowaniu kontroli nad tymi informacjami, nawet jeśli znajdują się w posiadaniu innych osób (wyroki TK z 19 lutego 2002 r., o sygn. akt U 3/01; z 30 listopada 2002 r. o sygn. akt K 41/02 czy też z 13 grudnia 2011 r. o sygn. akt K 33/08). Trybunał Konstytucyjny podkreślał, że art. 51 Konstytucji RP ustanawia szczególny środek ochrony tych samych wartości, które chronione są za pośrednictwem art. 47 Konstytucji RP (wyrok TK z 12 listopada 2002 r. o sygn. akt SK 40/01).

Z ochroną prywatności i autonomii informacyjnej koresponduje też prawo do ochrony tajemnicy komunikowania się, ustanowione w art. 49 Konstytucji RP. Zdaniem Trybunału Konstytucyjnego, konstytucyjną ochroną wynikającą z art. 49 Konstytucji RP objęta jest treść komunikowana bezpośrednio, jak i za pomocą środków komunikowania na odległość (wyroki TK z 20 czerwca 2005 r. o akt sygn. K 4/04 oraz z 2 lipca 2007 r. osygn. akt K 41/05).

Trybunał Konstytucyjny wyraźnie podkreślił, że konstytucyjną ochroną wynikającą z art. 47, art. 49 i art. 51 ust. 1 Konstytucji RP objęte są „wszelkie sposoby przekazywania wiadomości, w każdej formie komunikowania się, bez względu na fizyczny ich nośnik (np. rozmowy osobiste i telefoniczne, korespondencja pisemna, faks, wiadomości tekstowe i multimedialne, poczta elektroniczna). Ochrona konstytucyjna obejmuje nie tylko treść wiadomości, ale także wszystkie okoliczności procesu porozumiewania się, do których zaliczają się dane osobowe uczestników tego procesu, informacje o wybieranych numerach telefonów, przeglądanych stronach internetowych, dane obrazujące czas i częstotliwość połączeń, czy umożliwiające lokalizację geograficzną uczestników rozmowy, wreszcie dane o numerze IP czy numerze IMEI” (wyrok TK z 30 lipca 2014 r. o sygn. akt K 23/11). W tym samym wyroku **Trybunał Konstytucyjny podkreślił również wyraźnie, że w ramach konstytucyjnie**

gwarantowanej wolności człowieka i jego autonomii informacyjnej mieści się również ochrona przed niejawnym monitorowaniem jednostki.

Z kolei Konwencja o ochronie praw człowieka i podstawowych wolności w art. 8 ust. 1 statuuje prawo do poszanowania życia prywatnego i rodzinnego, mieszkania i korespondencji. W art. 8 ust. 2 Konwencja wyraźnie wskazuje, że ingerencja władzy publicznej w korzystanie z tego prawa jest niedopuszczalna, z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności osób. Przepis art. 8 ust. 1 Konwencji dotyczy zatem szeroko rozumianego prawa do poszanowania prywatnej sfery życia człowieka, stanowiąc tym samym najbardziej ogólną afirmację autonomii jednostki w zakresie kształtowania wszelkich aspektów jej życia oraz własnej osobowości. Istotą tego prawa jest zapewnienie każdej jednostce sfery prywatności (autonomii) chronionej przed ingerencją zewnętrzną, pochodzącą zarówno od państwa, jak i podmiotów prywatnych (zob. np. L. Garlicki, *uwaga 21 do art. 8*, [w:] L. Garlicki, P. Hofmański, A. Wróbel (red.), „Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności. Tom I. Komentarz do artykułów 1-18", Warszawa 2010, s. 491). **W świetle orzecznictwa ETPC kwestie związane z wkroczeniem państwa w sferę prywatności wynikającą z zastosowania środków niejawnego pozyskiwania informacji o osobach były rozpatrywane przede wszystkim jako ingerencja w „życie prywatne" i „korespondencję". Pojęcie „życia prywatnego", o którym mowa w art. 8 ust. 1 Konwencji, nie może być zatem redukowane do spraw ściśle osobistych i wewnętrznych człowieka, lecz powinno być rozumiane także w wymiarze społecznym, jako możność rozwijania kontaktów z innymi i interakcji ze światem zewnętrznym. Z kolei „korespondencja" obejmuje rozmaite sposoby wymiany wiadomości między oznaczonymi podmiotami, zarówno w postaci pisemnej, jak i za pośrednictwem faksu, poczty elektronicznej czy innych kanałów transmisji danych w ramach sieci internetowej.**

Podobną treść wyrażają postanowienia Karty Praw Podstawowych Unii Europejskiej, która w art. 7 statuuje prawo do prywatności, natomiast w art. 8 wyodrębnia prawo do ochrony danych osobowych. Prawo do ochrony danych osobowych jest również chronione w Unii Europejskiej na mocy art. 16 Traktatu o funkcjonowaniu Unii Europejskiej.

W oparciu o wskazane wyżej wzorce kontroli, poszczególne trybunały wypracowały minimalne wymagania, jakie łącznie muszą spełniać przepisy ograniczające wolności i prawa,

regulujące czynności operacyjno-rozpoznawcze. Ilustrując to stwierdzenie przykładami, **Rzecznik Praw Obywatelskich pragnie odnieść się do orzecznictwa ETPC, który wielokrotnie podkreślał, że ingerencję w życie prywatne i korespondencję stanowią nie tylko indywidualne środki niejawnej kontroli skierowane przeciwko oznaczonym podmiotom, ale też strategiczny monitoring połączeń i pozyskiwanie związanych z tym danych osobowych komunikujących się podmiotów**. Kwestia ta była rozpatrywana w sprawie *Weber i Saravia przeciwko Niemcom*, w której zakwestionowano niemieckie przepisy regulujące strategiczny monitoring połączeń telekomunikacyjnych, polegający na utrwalaniu rozmów telefonicznych nieoznaczonego kręgu rozmówców, a następnie identyfikowaniu, za pomocą słów kluczy, informacji zawartych w tych rozmowach, które mogą potencjalnie identyfikować sprawców przestępstw lub plany ich popełnienia. W ocenie ETPC doszło do ingerencji w „tajemnicę telekomunikacyjną" (ang. *secrecy of telecomunications*) chronioną przez art. 8 Konwencji. W świetle orzecznictwa ETPC ingerencją w sferę prywatności jednostki jest też gromadzenie i przechowywanie danych na temat jednostek przez służby państwowe, niezależnie od sposobu, w jaki zostały zgromadzone (zob. orzeczenia ETPC z 4 maja 2000 r. w sprawie *Rotaru przeciwko Rumunii*, skarga nr 28341/95, § 43-44 uzasadnienia oraz 2 września 2010 r. w sprawie *Uzun przeciwko Niemcom*, § 46 uzasadnienia). ETPC zwracał więc uwagę, że wystarczające dla stwierdzenia ingerencji w prawo zagwarantowane przez art. 8 Konwencji jest zgromadzenie danych o jednostkach, bez względu na to, w jaki sposób będą one w przyszłości wykorzystane. Tym niemniej ETPC nie zanegował w ogóle dopuszczalności niejawnego pozyskiwania informacji o osobach przez władze publiczne, lecz wręcz wskazywał na ich niezbędność, jako narzędzia umożliwiającego efektywne zagwarantowanie bezpieczeństwa oraz ochronę instytucji demokratycznego państwa przed wyrafinowanymi formami zagrożeń, zwłaszcza szpiegostwem czy terroryzmem (zob. m.in. orzeczenie ETPC z 6 września 1978 r. w sprawie *Klass i inni przeciwko Niemcom*).

Należy jednocześnie podkreślić, że również Trybunał Konstytucyjny, jak i Trybunał Sprawiedliwości Unii Europejskiej nie zanegowały konieczności przyznania właściwym organom kompetencji do pozyskiwania wiedzy, zbierania i gromadzenia informacji o obywatelach w sposób niejawny (zob. przykładowo wyrok TK z 30 lipca 2014 r. o sygn. akt K 23/11 czy też wyrok TSUE z 8 kwietnia 2014 r. w połączonych sprawach C-293/12 *Digital Rights Ireland* i C -594/12 *Kärtner Landesregierung i in.*; orzeczenie ETPC z 29 czerwca 2006 r. w sprawie *Weber i Saravia przeciwko Niemcom*).

Uwzględniając zatem dotychczasowe ustalenia Trybunału Konstytucyjnego, Europejskiego Trybunału Praw Człowieka, a także Trybunału Sprawiedliwości Unii Europejskiej dotyczące

przepisów regulujących niejawne pozyskiwanie przez władze publiczne w demokratycznym państwie prawa informacji o jednostkach, **możliwe jest zestawienie minimalnych wymagań, jakie muszą spełniać przepisy ograniczające konstytucyjne wolności i prawa.** Takiego zestawienia dokonał m.in. Trybunał Konstytucyjny w wyroku z 30 lipca 2014 r. w sprawie K 23/11. **Przypomnieć należy w szczególności te z nich, które bezpośrednio odnoszą się do analizowanych przez Rzecznika Praw Obywatelskich przepisów projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw** i które następnie powołane zostaną w dalszej części opinii Rzecznika (zob. również A. Grzelak, *Ochrona danych osobowych we współpracy państw członkowskich UE w zwalczaniu przestępczości. W stronę standardu europejskiego*, Warszawa 2015, s. 97 i n.). **W szczególności:**

— **w ustawie muszą być sprecyzowane przesłanki niejawnego pozyskiwania informacji o osobach, którymi są: wykrywanie i ściganie wyłącznie poważnych przestępstw oraz zapobieganie im; ustawa powinna wskazywać rodzaje takich przestępstw** (zob. np. postanowienie TK z 15 listopada 2010 r. o sygn. akt S 4/10; orzeczenia ETPC z: 29 czerwca 2006 r. w sprawie *Weber i Saravia przeciwko Niemcom*, skarga 54934/00; 10 lutego 2009 r. w sprawie *Iordachi i inni przeciwko Mołdawii*, skarga nr 25198/02);

— **ustawa musi określać kategorie podmiotów, wobec których mogą być podejmowane czynności operacyjno-rozpoznawcze** (zob. wyrok TK z 12 grudnia 2005 r. o sygn. akt K 32/04; orzeczenia ETPC z: 16 lutego 2000 r. w sprawie *Amann przeciwko Szwajcarii*, skarga nr 27798/95; 10 lutego 2009 r. w sprawie *Iordachi i inni przeciwko Mołdawii*, skarga nr 25198/02);

— **czynności operacyjno-rozpoznawcze winny być subsydiarnym środkiem pozyskiwania informacji lub dowodów o jednostkach, gdy nie da się ich uzyskać w inny, mniej dolegliwy dla nich sposób** (zob. wyroki TK z: 12 grudnia 2005 r. o sygn. akt K 32/04; 23 czerwca 2009 r. o sygn. akt K 54/07);

— **w ustawie należy określić maksymalny okres prowadzenia czynności operacyjno-rozpoznawczych wobec jednostek, który nie może przekraczać ram koniecznych w demokratycznym państwie prawa**;

— **niezbędne jest precyzyjne unormowanie w ustawie procedury zarządzenia czynności operacyjno-rozpoznawczych, obejmującej w szczególności wymóg uzyskania zgody niezależnego organu na niejawne pozyskiwanie informacji** (zob. np. wyrok TK z 12 grudnia 2005 r. o sygn. akt K 32/04; orzeczenia ETPC z: 29 czerwca 2006 r. w sprawie *Weber*

i Saravia przeciwko Niemcom, skarga 54934/00; 2 września 2010 r. w sprawie *Uzun przeciwko Niemcom*, skarga nr 35623/05);

— **konieczne jest precyzyjne określenie w ustawie zasad postępowania z materiałami zgromadzonymi w toku czynności operacyjno-rozpoznawczych, zwłaszcza zasad ich wykorzystania oraz niszczenia danych zbędnych i niedopuszczalnych** (zob. np. wyrok TK z 12 grudnia 2005 r. o sygn. akt K 32/04);

— **niezbędne jest zagwarantowanie bezpieczeństwa zgromadzonych danych przed nieuprawnionym dostępem ze strony innych podmiotów**;

— **w ustawie musi zostać unormowana procedura informowania jednostek o niejawnym pozyskaniu informacji na ich temat, w rozsądnym czasie po zakończeniu działań operacyjnych i zapewnienie na wniosek zainteresowanego poddania sądowej ocenie legalności zastosowania tych czynności; odstępstwo jest dopuszczalne wyjątkowo** (zob. np. postanowienie TK z 25 stycznia 2006 r. o sygn. akt S 2/06);

— **musi też być zagwarantowana transparentność stosowania czynności operacyjno-rozpoznawczych przez poszczególne organy władzy publicznej, przejawiające się w publicznej jawności i dostępności zagregowanych danych statystycznych, nadających się do porównania, o ilości i rodzaju stosowanych czynności operacyjno-rozpoznawczych**.

Już po dokonaniu powyższego zestawienia pojawiły się kolejne wyroki TSUE i ETPC, które dotyczyły problematyki masowego gromadzenia informacji. W tym kontekście należy przywołać wyrok TSUE z 6 października 2015 r. w sprawie C-362/14 w sprawie *Maximillian Schrems,* gdzie TSUE co prawda dokonał oceny ważności konkretnej decyzji Komisji Europejskiej, tym niemniej odniósł się do problemu braku środków prawnych przysługujących obywatelowi w przypadku przekazywania jego danych do państwa trzeciego, nawet w celach związanych z ochroną bezpieczeństwa publicznego, w którym nie są spełnione minimalne wymogi związane z ochroną danych osobowych. Unieważniona decyzja nie określała żadnych ograniczeń w zakresie dostępu amerykańskich organów publicznych do danych osobowych przekazywanych na jej podstawie. TSUE w szczególności wyjaśnił, że **uregulowanie umożliwiające organom publicznym uzyskanie powszechnego dostępu do treści wiadomości elektronicznych należy uznać za naruszenie zasadniczej istoty prawa podstawowego do poszanowania życia prywatnego** (pkt 94 wyroku TSUE w sprawie C-362/14 *Maximillian Schrems*).

Rzecznik Praw Obywatelskich pragnie również zwrócić uwagę na sprawę, którą rozstrzygnął Europejski Trybunał Praw Człowieka w dniu 4 grudnia 2015 r. (*Zakharov przeciwko Rosji*, skarga nr 47413/06). ETPC uznał w swoim wyroku, że doszło do naruszenia art.

8 Konwencji o ochronie praw człowieka i podstawowych wolności, a system niejawnej kontroli rozmów telefonicznych z telefonów komórkowych obowiązujący w Rosji narusza prawo do poszanowania życia prywatnego i korespondencji. Chociaż skarżący nie wykazał, by jego rozmowy były podsłuchiwane lub by operatorzy przekazywali jego dane nieuprawnionym osobom, to jednak ETPC postanowił o przeprowadzeniu abstrakcyjnej analizy tego prawa. Z wyroku wynika, że ETPC zwrócił w szczególności uwagę na naruszenie standardów konwencyjnych poprzez brak jakiegokolwiek sprecyzowania okoliczności, w jakich organy władzy mogą podsłuchiwać rozmowy obywateli, brak prawnego nakazu zakończenia podsłuchu, gdy ustały przesłanki uzasadniające jego stosowanie, brak uregulowania procedur przechowywania i niszczenia zarejestrowanych danych, co w praktyce oznaczało bezterminowe przechowywanie takich danych, brak procedur zezwalania na prowadzenie niejawnej kontroli, nieuregulowanie zasad nadzoru nad prowadzeniem takiej kontroli, wreszcie brak uregulowania zasad informowania obywateli o prowadzeniu kontroli oraz środkach prawnych przysługującym obywatelom w razie podsłuchiwania ich telefonów komórkowych.

Warto przypomnieć również, że w ETPC zawisła również sprawa ze skargi Big Brother Watch (*Big Brother Watch i inni przeciwko Wielkiej Brytanii*, skarga nr 58170/13), w której Trybunał wypowie się na temat blankietowego gromadzenia danych internetowych, dokonywanego przez brytyjskie służby wywiadowcze, do celów związanych z szeroko pojętym zwalczaniem przestępczości.

Przechodząc do zasygnalizowanego problemu, który jest przedmiotem analizy Rzecznika Praw Obywatelskich w niniejszej opinii, a mianowicie do kwestii dostępu Policji oraz innych służb do danych internetowych należy rozpocząć od wskazania, że **Internet jest jednym z narzędzi, które umożliwiają korzystanie z wolności i praw podmiotowych**. Z tego też względu, ocena przepisów umożliwiających ingerencję w prawa i wolności, odnoszące się do korzystania przez jednostki z Internetu, powinna być przeprowadzona z uwzględnieniem treści normatywnej właściwych przepisów Konstytucji RP (tak również wskazywał Trybunał Konstytucyjny w wyroku z 30 lipca 2014 r. o sygn. akt K 23/11). Dotyczy to również tych regulacji, które odnoszą się do kompetencji organów państwa w zakresie ochrony bezpieczeństwa.

Rzecznik Praw Obywatelskich podziela pogląd, wyrażony również przez Trybunał Konstytucyjny w powołanej wyżej sprawie, że specyfika nowych technologii i ocena zagrożeń z nimi związanych uzasadnia powierzenie wyspecjalizowanym organom władzy publicznej, jakimi są służby policyjne i służby ochrony państwa, adekwatnych uprawnień, dzięki którym

będą one w stanie zapobiegać przestępstwom i je wykrywać, ścigać ich sprawców, a także dostarczać informacji na temat zagrożeń dóbr prawnie chronionych. Skala wykorzystania nowych technologii wymaga wyposażenia służb w stosowne uprawnienia i stworzenia im warunków, umożliwiających efektywną walkę z naruszeniami prawa. W warunkach globalnej przestępczości istotna jest także prewencja w przypadku zagrożeń, których wystąpienie może wyrządzić nieodwracalne straty dla dóbr prawnie chronionych. Odpowiednikiem wyrażonego w art. 5 Konstytucji RP obowiązku państwa, polegającego na strzeżeniu niepodległości i nienaruszalności terytorium, a także zapewnieniu bezpieczeństwa państwa, jest prawo obywateli do ochrony ich bezpieczeństwa przed zagrożeniami, w tym przed przestępczością. W związku z tym, należy podkreślić, że wykorzystanie niejawnych metod pracy operacyjnej umożliwia ograniczenie skali przestępczości, co przekładać się będzie na wzrost poczucia bezpieczeństwa obywateli i swobodę w zakresie korzystania z przysługujących im wolności.

Czynności operacyjno-rozpoznawcze są niewątpliwie instrumentem wykrywania zagrożeń i ścigania naruszeń prawa. W obecnym stanie prawnym obejmują one m.in. kontrolę operacyjną, a także gromadzenie i przetwarzanie danych telekomunikacyjnych, co zostało uregulowane w art. 19 oraz w art. 20 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2015 r., poz. 355 ze zm.). Czynności operacyjno-rozpoznawcze znacznie ułatwiają walkę z tradycyjną przestępczością, a analiza materiałów zgromadzonych w kontroli operacyjnej, czy analiza danych telekomunikacyjnych umożliwia uzyskanie materiałów o ogromnym znaczeniu dla wykrycia zagrożeń i sprawców przestępstw. Nowe technologie są także jedynym sposobem umożliwiającym walkę z szeroko pojętą cyberprzestępczością – w wielu przypadkach zastosowanie czynności operacyjno-rozpoznawczych stanowi jedyny sposób zapobieżenia przestępstwu lub wykrycia sprawców.

Umożliwienie służbom policyjnym i służbom ochrony państwa pozyskiwania wiedzy o treści, czasie i formie komunikowania się jednostek, a także monitorowania ich aktywności w Internecie, popada w kolizję z prawem do ochrony prywatności, ochroną tajemnicy komunikowania się czy też z autonomią informacyjną. Samo istnienie przepisów uprawniających organy władzy wykonawczej do takiego rodzaju czynności postrzegane jest jako ingerencja w konstytucyjnie chroniony status człowieka i obywatela, którego źródłem jest przyrodzona i niezbywalna godność (tak również TK w wyroku z 30 lipca 2014 r. o sygn. akt K 23/11). **Niezależnie od konkretnych form wkroczenia w sferę życia prywatnego, sama świadomość znajdowania się pod ciągłym nadzorem władz publicznych może zniechęcać jednostki do swobodnego korzystania z przysługujących im praw, bowiem może rodzić**

obawy, że organy władzy publicznej będą w nieuprawniony sposób gromadzić i wykorzystywać posiadane informacje.

Rzecznik Praw Obywatelskich przypomina jednak, że chociaż czynności operacyjno-rozpoznawcze popadają w konflikt z prawem do ochrony prywatności i innymi wskazanymi wolnościami, to jednak mogą być uznane za konieczne w demokratycznym państwie prawa, z uwagi na ochronę bezpieczeństwa państwa, porządku publicznego bądź ochronę wolności i praw innych osób (art. 31 ust. 3 Konstytucji RP, art. 8 ust. 2 Konwencji o ochronie praw człowieka i obywatela, art. 52 ust. 1 Karty Praw Podstawowych UE). Dopuszczalność gromadzenia i przetwarzania danych dotyczących osób zależy zatem od przestrzegania konstytucyjnych wymagań, mających chronić jednostki przed nadużyciem w stosowaniu prawa i nadmiernym wkroczeniem w sferę ich prywatności, a także zabezpieczać przed wpływaniem służb policyjnych i ochrony państwa na demokratyczny mechanizm sprawowania władzy.

Należy zatem podkreślić, że uregulowanie podstaw prawnych praktyki gromadzenia i przetwarzania danych internetowych musi spełniać określone wymagania. Wszelkie przypadki ograniczenia prawa do prywatności i innych omawianych wolności muszą być uregulowane przepisami prawa, jasno i precyzyjnie określającymi sposób i zasady ich stosowania tak, by obywatele byli uprzedzeni o wdrożeniu tych środków. Prawo dopuszczające ingerencję powinno jednak ograniczać możliwości stosowania nadzorowania tylko do tych obszarów i w tym zakresie, gdy jest to rzeczywiście niezbędne do osiągnięcia prawnie usprawiedliwionego celu.

Analiza projektu ustawy dokonana przez Rzecznika Praw Obywatelskich wskazuje, że - w odniesieniu do konkretnych propozycji uregulowania zasad gromadzenia danych internetowych przez służby policyjne i inne służby - projekt nie spełnia jednak kryteriów uzasadniających ograniczenie praw i wolności obywatelskich, wynikających z Konstytucji RP, a także z przywołanych umów międzynarodowych, co podaje w wątpliwość zgodność projektu z art. 30, art. 47, art. 49, art. 51 w zw. z art. 31 ust. 3 Konstytucji RP, a także z art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności. Poniżej wskazano podstawowe zastrzeżenia i wątpliwości dotyczące tych rozstrzygnięć, które nie spełniają powyższych standardów.

Projekt przewiduje dopuszczalność uzyskiwania przez poszczególne służby danych internetowych i przetwarzanie ich bez wiedzy i zgody osoby, której dotyczą, w celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskiwania i utrwalenia dowodów przestępstw albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub

ratowniczych (dodawane art. 20c ust. 1 ustawy o Policji, art. 10b ustawy o Straży Granicznej, art. 36b ustawy o kontroli skarbowej, art. 30 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 32 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, art. 18 ustawy o Centralnym Biurze Antykorupcyjnym, art. 75d ustawy o Służbie Celnej). **W przeciwieństwie do obowiązującego w obecnej chwili art. 18 ust. 6 ustawy o świadczeniu usług drogą elektroniczną,** który przewiduje, że usługodawca udziela informacji o danych, o których mowa w ust. 1-5 tego przepisu, organom państwa na potrzeby prowadzonych przez nie postępowań, **projektowane przepisy zakładają <u>całkowitą dowolność</u> po stronie organów państwa.** Co więcej, co należy podkreślić, zgodnie z dodawanym do art. 19 ustawy o Policji przepisami ust. 6 a i 6 b, czynności przewidziane w art. 20c ustawy o Policji nie stanowią kontroli operacyjnej, a ich realizacja nie wymaga zgody sądu.

Pojęcie „danych internetowych" definiowane jest poprzez odwołanie się do art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r., poz. 1422 ze zm.). Pojęcie to obejmuje zatem:

1) dane osobowe usługobiorcy niezbędne do nawiązania, ukształtowania treści, zmiany lub rozwiązania stosunku prawnego, między innymi nazwisko i imiona usługobiorcy, numer ewidencyjny PESEL, lub – gdy numer ten nie został nadany – numer paszportu, dowodu osobistego lub innego dokumentu potwierdzającego tożsamość, adres zameldowania na pobyt stały, adres do korespondencji, dane służące do weryfikacji podpisu elektronicznego usługobiorcy, adresy elektroniczne usługobiorcy;

2) inne dane niezbędne ze względu na właściwość świadczonej usługi lub sposób jej rozliczenia;

3) inne dane dotyczące usługobiorcy, które nie są niezbędne do świadczenia usługi drogą elektroniczną, przekazane za zgodą usługobiorcy;

4) tzw. dane eksploatacyjne, charakteryzujące sposób korzystania z usługi świadczonej drogą elektroniczną, w tym oznaczenia identyfikujące usługobiorcę, oznaczenia identyfikujące zakończenie sieci telekomunikacyjnej lub system teleinformatyczny, z którego korzystał usługobiorca, informacje o rozpoczęciu, zakończeniu oraz zakresie każdorazowego korzystania z usługi świadczonej drogą elektroniczną, informacje o skorzystaniu przez usługobiorcę z usług świadczonych drogą elektroniczną.

Rzecznik Praw Obywatelskich pragnie podkreślić, że wymienione w tym przepisie kategorie danych są określone bardzo ogólnie, co może powodować niejasności i prowadzić do zbyt szerokiego pojmowania tych pojęć, a w efekcie do nadmiernej ingerencji w prawa podstawowe. W szczególności **wykładnia przepisów nie pozwala jednoznacznie ustalić, czy tak ujęte sformułowanie nie obejmuje również treści przekazywanych komunikatów** (por. K. Klafkowska-Waśniowska, *Komentarz do art. 18 ustawy o świadczeniu usług drogą elektroniczną*, [w:] D. Lubasz, M. Namysłowska (red.), „Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz do ustaw", LexisNexis 2011, pkt 7). Przypomnieć należy, że prawo określające granice ingerencji państwa w prawa człowieka i obywatela musi spełniać wymogi jakościowe, być dostępne oraz przewidywalne dla jednostek – z prawa muszą wynikać okoliczności i warunki, w których władze publiczne będą sięgać po określone dane. Precyzja regulacji prawnej ma zapobiegać ryzyku arbitralności działań, z natury rzeczy pozostających poza zasięgiem kontroli publicznej. **Niejasności związane z zakresem danych internetowych, które mogą być gromadzone przez służby, powoduje, że nie można uznać, by spełniony był wymóg precyzyjności prawa**.

Trzeba również podkreślić, że wskazany szeroki zakres informacji, do których będą mieć dostęp służby policyjne, będzie pozwalał na szerokie i precyzyjne odtworzenie różnych aspektów życia prywatnego. Może również prowadzić do budowania profilu osobowego osób uczestniczących w procesie komunikacji, a co za tym idzie – do ustalenia ich trybu życia, przynależności do organizacji społecznych czy politycznych, osobistych upodobań czy skłonności osób poddanych obserwacji. Uzyskiwanie i przetwarzanie danych internetowych nie będzie też miało związku z żadnym toczącym się postępowaniem. Należy podkreślić, że obowiązujący art. 18 ust. 6 ustawy o świadczeniu usług drogą elektroniczną zawiera podstawę prawną zobowiązującą usługodawców do udzielania informacji o wskazanych wyżej danych organom państwa, ale wyraźnie wskazuje, że musi to mieć związek z prowadzonymi przez nie postępowaniami.

Dopuszczalność ingerencji w prawo do prywatności i inne wskazane wolności wymaga, by ustawa określała precyzyjnie przesłanki niejawnego pozyskiwania informacji o osobach, którymi są wykrywanie i ściganie wyłącznie poważnych przestępstw oraz zapobieganie im. Z orzecznictwa ETPC i TSUE wynika jasno, że chodzi wyłącznie o poważne przestępstwa. Tymczasem projektowana ustawa bardzo ogólnie określa cel uzyskiwania i przetwarzania danych, jako „rozpoznawanie, zapobieganie, zwalczanie, wykrywanie albo uzyskanie i utrwalenie dowodów przestępstw". Dotyczy zatem wszelkich przestępstw, a nie wyłącznie poważnych. Użyte pojęcie nie

tylko nie są precyzyjne, ale przede wszystkim nie spełniają wskazanego wyżej kryterium. Tak ujęty cel gromadzenia i przetwarzania danych może bowiem oznacza brak selektywności zarówno na etapie rozpoczęcia pozyskiwania danych internetowych, czyli możliwości uzyskiwania przez służby danych w postępowaniach w sprawie bliżej nieokreślonych czynów zabronionych, bez względu na ich szkodliwość społeczną. Oznacza ponadto, że nie zagwarantowano, by gromadzenie i przetwarzanie danych internetowych było subsydiarnym środkiem pozyskiwania informacji lub dowodów o jednostkach. **Brak subsydiarności proponowanych przepisów otwiera możliwość wykorzystywania danych internetowych nie tylko wówczas, gdy jest to rzeczywiście konieczne do wykrywania lub zapobiegania przestępstwom, ale także wtedy gdy jest to po prostu najprostsze i najwygodniejsze.**

Projekt ustawy nie przewiduje żadnego ograniczenia czasowego w zakresie gromadzenia i przetwarzania danych. Zakłada się jedynie, że wyłącznie dane, które nie mają znaczenia dla postępowania karnego (a zostały przekazane prokuratorowi), podlegają niezwłocznemu komisyjnego i protokolarnemu zniszczeniu. Pozostałe dane, nieprzekazane prokuratorowi, będą mogły być w praktyce przechowywane bez ograniczeń czasowych. Projekt nie zawiera także żadnych przepisów regulujących szczegółowo postępowanie z materiałami zebranymi niezgodnie z prawem. Ponownie, nie można uznać, by proponowane przepisy spełniały kryterium proporcjonalności i konieczności ograniczenia wolności i praw człowieka i obywatela.

Przepisy dopuszczające ingerencję poprzez uregulowanie czynności operacyjno-rozpoznawczych muszą także precyzyjnie unormować procedurę ich zarządzenia, w tym wymóg uzyskania zgody niezależnego organu na niejawne pozyskiwanie informacji. **Projekt zakłada, że usługodawca świadczący usługi drogą elektroniczną będzie zobowiązany udostępniać nieodpłatnie dane internetowe nie tylko upoważnionym funkcjonariuszom, ale także za pośrednictwem sieci telekomunikacyjnej, z użyciem bezpiecznego łącza**. Projekt nie wyjaśnia, czy usługodawca będzie zobowiązany do zawarcia stosownego porozumienia z właściwą służbą i jakie będzie miał praktyczne możliwości odmowy zawarcia takiego porozumienia.

Trzeba również podkreślić, że obowiązki nałożone na usługodawców świadczących usługi drogą elektroniczną, będą w praktyce dotyczyć wyłącznie usługodawców mających siedzibę na terenie Rzeczypospolitej Polskiej (art. 3 ustawy o świadczeniu usług drogą elektroniczną). Fakt, że obowiązki określone w ustawie dotyczyć będą wyłącznie ograniczonego kręgu podmiotów, nie umniejsza wagi podniesionych przez Rzecznika Praw Obywatelskich. Wręcz przeciwnie, pozwala na stwierdzenie, że taka regulacja może prowadzić do sytuacji, w której niemożliwe będzie w ogóle

sięgnięcie po dane internetowe posiadane przez usługodawców z siedzibą poza terytorium RP lub będzie się odbywać w ogóle bez żadnej podstawy prawnej. To oznacza, że **proponowane rozwiązania mogą nie stanowić efektywnego środka zapobiegania i zwalczania przestępczości**..

Poważne wątpliwości Rzecznika Praw Obywatelskich budzą procedury kontrolne. W przepisach dotyczących poszczególnych służb wskazuje się na właściwość sądu okręgowego w tzw. trybie następczym. Kontrola ta ma polegać na analizie półrocznych sprawozdań przedkładanych sądom przez służby. Wydaje się, że przy dużej skali pozyskiwanych danych oraz stosunkowo dużym odstępie czasowym, kontrola ta może mieć w istocie charakter iluzoryczny i nie spełniać wymogów wynikających z Konstytucji RP, a także ze wskazanych umów międzynarodowych. W szczególności projektowana regulacja nie pozwala na udzielenie odpowiedzi, jaki rodzaj i zakres danych będzie przekazywanych przez Policję, czy kwalifikacja prawna będzie się odnosić do konkretnych przypadków, czy też ogólnie do całości danych statystycznych. Projektowane przepisy nie zakładają także możliwości uzupełniania informacji, w tym nie określają czy sądowi będą przekazywane akta postępowania, w tym informacje dotyczące inwigilacji konkretnych osób. Wreszcie proponowane przepisy nie określają konsekwencji dokonywanej kontroli (tj. czy polegać one mają wyłącznie na zniszczeniu przetwarzanych materiałów, czy też także np. na podjęciu postępowań dyscyplinarnych lub karnych wobec funkcjonariuszy odpowiedzialnych za inicjowanie i realizację nielegalnej inwigilacji).

Ponadto, **projekt ustawy nie zakłada istnienia żadnej procedury, w wyniku której o pozyskiwaniu danych internetowych kiedykolwiek dowiedziałby się podmiot, którego dane były przetwarzane**. W przekonaniu Rzecznika Praw Obywatelskich, obywatel powinien mieć prawo do podjęcia stosownych środków prawnych w zakresie działań prowadzonych względem niego, również w odniesieniu do informacji gromadzonych przez właściwe służby. Jest to również wymóg jasno określony przez Trybunał Konstytucyjny (postanowienie z 25 stycznia 2006 r. o sygn. akt S 2/06). Co więcej, projektodawca nie przewidział żadnych przepisów określających szczegółowo kategorie podmiotów, wobec których mogą być podejmowane czynności operacyjno-rozpoznawcze.

W związku z powyższym należy zauważyć, że **poselski projekt ustawy o Policji oraz niektórych innych ustaw (druk nr 154) w zakresie dostępu służb policyjnych i innych służb ochrony państwa budzi poważne zastrzeżenia konstytucyjne**. Mając na uwadze, że dotyczy on problematyki pozwalającej na poważną ingerencję w prawa i wolności człowieka i obywatela, wymaga on ponownego przeanalizowania i wprowadzenia zmian prowadzących do realizacji

przesłanek wynikających z Konstytucji RP, a także z Konwencji o ochronie praw człowieka i podstawowych wolności oraz Karty Praw Podstawowych Unii Europejskiej.

Mając powyższe na względzie, z uwagi na to, że przedmiotowa problematyka pozostaje w zakresie zainteresowania kierowanego przez Panią Minister resortu, działając na podstawie art. 16 ust. 1 ustawy z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. z 2014 r., poz. 1648 ze zm.), przedkładam uprzejmie powyższą ocenę Rzecznika Praw Obywatelskich, wraz z prośbą o zajęcie w tej sprawie stanowiska.

Podpis na oryginale