Warszawa, dnia 23 grudnia 2011 r.

# UWAGI DO SPRAWOZDANIA Z PRACY ZESPOŁU DORAŹNEGO DS. POZYSKIWANIA DANYCH TELEKOMUNIKACYJNYCH ORAZ PROPONOWANYCH W NIM ROZWIĄZAŃ PRAWNYCH

Fundacja PANOPTYKON z uwagą zapoznała się ze *Sprawozdaniem z prac zespołu doraźnego ds. pozyskiwania danych telekomunikacyjnych* (dalej: **Sprawozdanie**), które zostało nam przekazane drogą elektroniczną 29 września 2011 r. Sprawozdanie podsumowuje wyniki prac Zespołu doraźnego ds. pozyskiwania danych telekomunikacyjnych (dalej: **Zespół**), działającego pod przewodnictwem Sekretarza Kolegium ds. Służb Specjalnych, oraz zawiera konkretne propozycje zmian legislacyjnych. Stanowi jednocześnie pogłębienie i uszczegółowienie strategii regulacyjnej zarysowanej w *Raporcie dotyczącym retencji danych telekomunikacyjnych* (dalej: **Raport**) z 4 lipca 2011 r. Zakres proponowanych zmian legislacyjnych obejmuje zmianę przepisów ustawy o Policji i ustaw kompetencyjnych innych służb, Kodeksu postępowania cywilnego, Kodeksu postępowania karnego (dalej: **k.p.k.**) i ustawy Prawo telekomunikacyjne, a także zmiany w przepisach dotyczących organizacji sądów powszechnych i wojskowych oraz prokuratury.

W niniejszej opinii przekazujemy nasze stanowisko dotyczące prawnego obowiązku retencji i udostępniania uprawnionym podmiotom danych telekomunikacyjnych oraz odnosimy się do propozycji rozwiązań prawnych zawartych w Sprawozdaniu. Problematyka retencji danych telekomunikacyjnych znajduje się od dawna w obszarze zainteresowań Fundacji PANOPTYKON. W przygotowanym kilka miesięcy temu raporcie pt. „Internet a prawa podstawowe. Ekspresowy przegląd problemów regulacyjnych”[1] podsumowaliśmy aktualne dylematy regulacyjne w tym obszarze, zarysowaliśmy możliwe scenariusze zmian prawnych i podsumowaliśmy nasze rekomendacje.

Aktualnie w Unii Europejskiej trwają prace nad rewizją Dyrektywy 2006/24/WE z 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności (dalej: **dyrektywa retencyjna**), których rozpoczęcie Komisja Europejska ogłosiła w komunikacie z 18 kwietnia 2011 r. W kontekście tego procesu na szczególną uwagę zasługuje opinia Europejskiego Inspektora Danych Osobowych[2] (dalej: **EIDO**), który uznał, że dyrektywa retencyjna nie spełnia europejskich standardów poszanowania praw i wolności obywatelskich, w szczególności prawa do prywatności i ochrony danych osobowych. Uwzględnienie wniosków z opinii EIDO i kierunków reformy europejskiego reżimu obowiązkowej retencji danych telekomunikacyjnych wydaje się konieczne w trakcie projektowania

[1] Raport jest dostępny pod adresem: http://wolnyinternet.panoptykon.org/sites/default/files/raport_na_www.pdf.

[2] Por. Opinia European Digital Rights z 14 maja 2011 r. (http://ebookbrowse.com/11-05-30-evaluation-report-drd-en-pdf-d133765453) oraz Peter Hustinx, European Data Protection Supervisor, *The moment of truth for the Data Retention Directive* – przemówienie na konferencji “Taking on the Data Retention Directive”, Bruksela, 3 grudnia 2010 r.

polskiej reformy prawa w tym obszarze. Wypracowane w Polsce rozwiązania mogłyby także posłużyć jako model podczas spodziewanych dyskusji o kształcie regulacji na szczeblu europejskim.

## I. Obowiązkowe zatrzymywanie danych telekomunikacyjnych

### 1. Utrzymanie obowiązku retencji

Kwestią fundamentalną, która nie może być pominięta, jest sama zasadność utrzymania obowiązkowej retencji danych telekomunikacyjnych. Zgodnie z zastrzeżeniami EIDO, obowiązkowa retencja danych może być uznana za dopuszczalną, jeśli zostanie wykazana jej proporcjonalność i niezbędność. O zastosowaniu tego środka w żadnym przypadku nie może przesądzać kryterium użyteczności.

Jak wielokrotnie podkreślaliśmy, ani Komisja Europejska, ani polskie władze nie przedstawiły jak dotąd dowodów na niezbędność i proporcjonalność tego narzędzia w zwalczaniu poważnej przestępczości. Zostały natomiast zebrane przekonywujące dowody wykazujące skuteczność alternatywnego mechanizmu: szybkiego i wybiórczego zamrażania danych[3]. Badania przeprowadzone w Niemczech przez Towarzystwo Wspierania Nauki im. Maxa Plancka potwierdziły niemalże 100-procentową skuteczność tej metody w dotarciu do potrzebnych danych[4]. Tak wysoka skuteczność mechanizmu „szybkiego zamrażania danych" wynika z praktyki operatorów telekomunikacyjnych, którzy ze względów komercyjnych lub w związku z realizacją zawartych umów, przetwarzają i gromadzą dane telekomunikacyjne swoich użytkowników przez okres co najmniej 3 miesięcy.

Niezbędna zatem jest szczegółowa i poparta rzetelnymi danymi analiza tego, na ile obligatoryjna retencja danych jest konieczna z punktu widzenia skuteczności postępowań i czy podobnych efektów nie można osiągnąć stosując dostępne alternatywy, np. zamrażanie danych. Przy przeprowadzaniu tej analizy, opartej na teście proporcjonalności, trzeba uwzględnić fakt, że mechanizm rutynowego zatrzymywania danych telekomunikacyjnych wszystkich obywateli odbywa się kosztem praw podstawowych. Czeski Sąd Konstytucyjny w wyroku stwierdzającym niezgodność krajowych przepisów o retencji danych z konstytucją, stwierdził, że: *odpowiednia kombinacja danych telekomunikacyjnych, zwłaszcza zebranych w dłuższym czasie, pozwala gromadzić szczegółowe informacje, na przykład na temat aktywności towarzyskiej, poglądów politycznych, skłonności czy słabości osób, pomimo że retencja danych nie obejmuje treści prowadzonej korespondencji*[5].

W Sprawozdaniu brakuje szczegółowej analizy, która uzasadniałaby konieczność utrzymania obowiązkowej retencji danych, jako narzędzia charakteryzującego się największą skutecznością

---

[3] Tzw. szybkie zamrożenie (*quick freeze*) polega na czasowym zachowaniu przez operatorów danych telekomunikacyjnych konkretnych osób na żądanie uprawnionego podmiotu (dłużej niż wynikałoby to ze zwyczajnej praktyki operatora). Samo „zamrożenie" odbywa się automatycznie na żądanie uprawnionych organów, jednak zatrzymane dane przekazywane są dopiero po potwierdzeniu potrzeby „szybkiego zamrożenia" przez sąd. W przypadku decyzji odmownej sądu dane są niezwłocznie usuwane. Ten mechanizm pozwala uniknąć gromadzenia i przechowywania danych wszystkich obywateli korzystających z usług telekomunikacyjnych, ograniczając te czynności do przypadków osób podejrzanych o popełnienie poważnych przestępstw.

[4] Za: Andrzej Adamski, *Retention of telecommunication data in Poland: does the legal regulation pass the proportionality test?*.

[5] Por. *Rozwiązania prawne w wybranych państwach UE dotyczące możliwości wykorzystywania danych objętych tajemnicą telekomunikacyjną w świetle dyrektywy 2006/24/WE* – ekspertyza zlecona przez Kancelarię Prezesa Rady Ministrów Ośrodkowi Studiów Wschodnich im. Marka Karpia.

w wykrywalności przestępstw w porównaniu z innymi metodami wykorzystywanymi przez policję i inne służby.

## 2. Okres retencji

Sprawozdanie zawiera propozycję skrócenia okresu retencji danych telekomunikacyjnych z 24 do 12 miesięcy. Naszym zdaniem to ograniczenie jest niewystarczające. Co więcej, wybór akurat tego okresu nie został poparty dostateczną analizą. W uzasadnieniu jest jedynie mowa o braku dostatecznego uzasadnienia dla zatrzymywania danych przez okres 24 miesięcy, natomiast nie pojawiają się konkretne argumenty za przyjęciem okresu 12-miesięcznego. Zgodnie z Raportem na temat ewaluacji dyrektywy retencyjnej opracowanym przez Komisję Europejską[6] tylko w Polsce wprowadzono obowiązkową retencję wszystkich typów danych telekomunikacyjnych przez maksymalny okres 2 lat. W 15 krajach czas ten wynosi 12 miesięcy, a w trzech (Cypr, Litwa, Luksemburg) jedynie 6 miesięcy. Warto również pamiętać, że kilka krajów w ogóle nie wdrożyło dyrektywy retencyjnej i polega wyłącznie na danych przechowywanych przez operatorów w celach komercyjnych (zwykle jest to okres od 3 do 6 miesięcy).

Termin roczny stanowi niejako „wypośrodkowanie" istniejących rozwiązań niepoparte dostateczną analizą, podczas gdy to po stronie państwa (na podstawie art. 31 ust. 3, art. 47 i 49 Konstytucji RP) istnieje obowiązek wykazania, że proponowane ograniczenie prawa do prywatności jest konieczne i proporcjonalne w demokratycznym państwie. Szczególne znaczenie w tym kontekście ma opinia zaprezentowana we wspomnianym raporcie Komisji Europejskiej, zgodnie z którą największe uzasadnienie (ze względu na przeanalizowane wzorce wykorzystywania danych w celach dochodzeniowych) ma 6-miesięczny okres retencji. Takie jest również zdanie niemieckiego Trybunału Konstytucyjnego. Z powyższych względów sugerujemy przyjęcie również w Polsce co najwyżej 6-miesięcznego okresu retencji. Ewentualnie, można poddać pod rozwagę zróżnicowanie czasu retencji w zależności od rodzaju zatrzymywanych danych (np. ustalić inne okresy zatrzymywania dla danych o komunikacji telefonicznej i internetowej)[7].

# II. Dostęp do danych telekomunikacyjnych

## 3. Cele uzasadniające dostęp do danych

### 3.1. Cele prewencyjne

Zespół proponuje utrzymanie celów prewencyjnych, czyli zapobiegania przestępstwom (ich katalog ma być dookreślony za pomocą kilku kryteriów), jako jednej z podstaw wykorzystywania retencji danych telekomunikacyjnych. Jak wielokrotnie podkreślaliśmy, jest to niezgodne z celami określonymi w dyrektywie retencyjnej, która wskazuje, iż celem retencji danych jest zwalczanie poważnych przestępstw. W czasie prac nad tą dyrektywą zasadność wykorzystywania retencji danych dla celów prewencyjnych była przedmiotem gorącej dyskusji[8]. Mimo widocznej tendencji do zaostrzenia prawa za względu na zagrożenie terrorystyczne, państwa członkowskie zgodziły się, że tak postawiony cel byłby zbyt szeroki i stwarzałby

[6] Report From the Commission to the Council And The European Parliament: Evaluation report on the Data Retention Directive (COM(2011) 225 final).

[7] Takie rozwiązanie wprowadzono np. w Słowenii.

[8] Report From the Commission to the Council And The European Parliament: Evaluation report on the Data Retention Directive (COM(2011) 225 final).

poważne pole do nadużyć. Na tym tle polskie przepisy stanowią wyraźny wyłom w europejskich standardach ochrony prywatności.

### 3.2. Kryterium górnej granicy zagrożenia karą pozbawienia wolności

W Sprawozdaniu została sformułowana propozycja ograniczenia możliwości korzystania z zatrzymywanych danych telekomunikacyjnych do rozpoznawania, zapobiegania i wykrywania przestępstw zagrożonych karą pozbawienia wolności, której górna granica wynosi co najmniej 3 lata**.** Odnosimy się do tej propozycji bardzo krytycznie.

Po pierwsze, przestępstwa których górna granica zagrożenia karą pozbawienia wolności wynosi co najmniej 3 lata stanowią zdecydowaną większość w polskim kodeksie karnym (dalej: **k.k.**). W przypadku przyjęcia proponowanych rozwiązań dane telekomunikacyjne wciąż będą bardzo szeroko wykorzystywane w pracy policji i innych służb. Natomiast zgodnie z duchem dyrektywy retencyjnej, dane zatrzymywane w ramach obowiązku retencji miały służyć jedynie do ścigania poważnych przestępstw (ang. *serious crimes*). W naszej opinii kryterium zagrożenia karą pozbawienia wolności, której górna granica wynosi co najmniej 3 lata, nie realizuje tego postulatu. Ograniczenie celów, w których można wykorzystywać dane retencyjne, jest kwestią fundamentalną z punktu widzenia realizacji zasady konieczności i proporcjonalności. Stwierdził to również w swoim orzeczeniu czeski Sąd Konstytucyjny, argumentując, że wykorzystywanie danych telekomunikacyjnych do wyjaśniania „zwykłych" przestępstw jest niezgodne z postulowaną przez EIDO zasadą proporcjonalności.

Po drugie, zaproponowane w Sprawozdaniu kryterium jest nieprecyzyjne. Retencja danych, jako źródło informacji i potencjalnych dowodów, może być wykorzystywana w pierwszych stadiach postępowania. Na tym etapie strona podmiotowa (np. nieumyślność, która może mieć wpływ na wysokość górnej granicy zagrożenia ustawowego), a nawet kwalifikacja prawna czynu zabronionego może być jeszcze nieznana.

Po trzecie, przyjęcie zaproponowanych rozwiązań może wywołać niezamierzony i niebezpieczny efekt w postaci nacisków na podniesienie granic ustawowego zagrożenia karą za drobne przestępstwa, w przypadku których korzystanie z zatrzymywanych danych telekomunikacyjnych nie będzie dopuszczalne.

Sugerujemy zatem inne określenie kryterium, od którego ma być uzależniona możliwość sięgnięcia po zatrzymywane dane telekomunikacyjne. Jedną z propozycji może być określenie rodzaju dóbr, w jakie godzi dany czyn zabroniony, tak jak zostało to ujęte w k.k. (np. życie i zdrowie, bezpieczeństwo powszechne) w połączeniu z kryterium dolnej granicy zagrożenia karą pozbawienia wolności. W tym kontekście trzeba by jednak rozważyć podniesienie dolnej granicy zagrożenia ustawowego (np. w Bułgarii przyjęto granicę 5 lat) oraz mieć na uwadze wspomniane powyżej ryzyko nacisków na zaostrzenie prawa. Inna możliwość to stworzenie zamkniętego katalogu przestępstw, których ma dotyczyć obowiązek przekazywania danych telekomunikacyjnych. Mimo pewnych ograniczeń takie rozwiązanie uważamy za najbardziej optymalne z punktu widzenia precyzji określenia, w jakich sytuacjach możliwe jest wkroczenie w konstytucyjnie chronione prawa i wolności jednostki.

Jak wskazuje w swoim wystąpieniu do Prezesa Rady Ministrów Donalda Tuska Rzecznik Praw Obywatelskich prof. Irena Lipowicz, przepisy ograniczające prawa i wolności powinny spełniać

kryterium konkretności[9]. Ze względu na niejasne granice, zaproponowane w Sprawozdaniu kryterium może być uznane za niezgodne z art. 8 ust. 2 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności (dalej: **Konwencja**). Zgodnie z nim, ingerencja władzy publicznej w korzystanie z prawa do prywatności jest niedopuszczalna z wyjątkiem przypadków przewidzianych przez ustawę. Przy czym, jak wskazał Europejski Trybunał Praw Człowieka w sprawie *Malone*, sformułowanie użyte w art. 8 ust. 2 Konwencji („przewidzianych przez ustawę") nie jest tożsame z prostym odwołaniem się do prawa krajowego, ale odnosi się także do jakości tego prawa. Prawo krajowe powinno być wystarczająco precyzyjne i wskazywać obywatelom konkretne okoliczności oraz warunki, w jakich organy egzekwowania prawa są uprawnione stosować niejawne techniki zdobywania informacji.

W kwestii kryterium górnej granicy zagrożenia karą pozbawienia wolności wypowiadała się również Helsińska Fundacja Praw Człowieka, podnosząc podobne zastrzeżenia.

### 3.3. Wyłączenie dotyczące danych użytkownika

Zgodnie ze Sprawozdaniem, proponowane kryterium górnej granicy ustawowego zagrożenia karą pozbawienia wolności nie ma dotyczyć udostępniania „danych telekomunikacyjnych dotyczących użytkownika". Sprawozdanie nie doprecyzowuje, jakie dane mieszczą się w tej kategorii, można jednak zakładać, że autorzy mieli na myśli tzw. dane subskrybenta (np. do kogo należy dany numer telefonu lub numer IP). Warto na gruncie projektowanych przepisów doprecyzować, jakie konkretnie dane będą wyłączone z istotnej ochrony w postaci wspomnianego kryterium.

### 3.4. Wyłom w ustawie o Policji i Straży Granicznej

Za wyjątkowo niepokojące uważamy poszerzenie celów, dla których można wykorzystywać zatrzymywane dane telekomunikacyjne, zaproponowane w stosunku do ustawy o Policji i ustawy o Straży Granicznej. Ma być to kolejny wyłom w zaproponowanym kryterium ustawowego zagrożenia karą pozbawienia wolności (por. pkt 3.2.). W odpowiednich przepisach – art. 20c ust. 1a ustawy o Policji i art. 10b ust. 1a ustawy o Straży Granicznej – przyjmuje się, że ograniczenie przez wspomniane kryterium nie obowiązuje w przypadku zapobiegania i wykrywania przestępstw, o których mowa w art. 19 ust. 1 ustawy o Policji i art. 9e ust. 1 ustawy o Straży Granicznej. Obydwa przepisy odnoszą się do bardzo szerokiego katalogu czynów zabronionych[10], co sprawia, że zaproponowane w Sprawozdaniu „podstawowe kryterium" górnej granicy zagrożenia karą pozbawienia wolności staje się ograniczeniem pozornym.

---

[9] Rzecznik Praw Obywatelskich Irena Lipowicz, list RPO do Premiera Donalda Tuska w sprawie pozyskiwania przez służby informacji objętych tajemnicą komunikowania się z 17 stycznia 2011 r. (http://www.sprawy-generalne.brpo.gov.pl/pdf/2010/12/662587/1540465.pdf).

[10] Art. 19 ust. 1. ustawy o Policji przewiduje, że „przy wykonywaniu czynności operacyjno-rozpoznawczych, podejmowanych przez Policję, w celu zapobieżenia, wykrycia, ustalenia sprawców, a także uzyskania i utrwalenia dowodów ściganych z oskarżenia publicznego, umyślnych przestępstw: 1) przeciwko życiu, określonych w art. 148-150 Kodeksu karnego, 2) określonych w art. 134, art. 135 § 1, art. 136 § 1, art. 156 § 1 i 3, art. 163 § 1 i 3, art. 164 § 1, art. 165 § 1 i 3, art. 166, art. 167, art. 173 § 1 i 3, art. 189, art. 204 § 4, art. 223, art. 228 § 1 i 3-5, art. 229 § 1 i 3-5, art. 230 § 1, art. 230a § 1, art. 231 § 2, art. 232, art. 245, art. 246, art. 252 § 1-3, art. 253, art. 258, art. 269, art. 280-282, art. 285 § 1, art. 286 § 1, art. 296 § 1-3, art. 296a § 1, 2 i 4, art. 296b § 1 i 2, art. 299 § 1-6 oraz w art. 310 § 1, 2 i 4 Kodeksu karnego, 3) przeciwko obrotowi gospodarczemu, określonych w art. 297-306 Kodeksu karnego, powodujących szkodę majątkową lub skierowanych przeciwko mieniu, jeżeli wysokość szkody lub wartość mienia przekracza pięćdziesięciokrotna wysokość najniższego wynagrodzenia za prace określonego na podstawie odrębnych przepisów, 4) skarbowych, jeżeli wartość przedmiotu czynu lub uszczuplenie należności publicznoprawnej przekraczają pięćdziesięciokrotną wysokość najniższego wynagrodzenia za prace określonego na podstawie odrębnych przepisów, 5) nielegalnego wytwarzania, posiadania lub obrotu bronią, amunicja, materiałami

### 3.5. Przestępstwa popełniane za pomocą środków komunikacji elektronicznej

W propozycji Zespołu jednym z kryteriów uzasadniających możliwość wykorzystania danych retencyjnych przez Policję i inne służby ma być sam fakt popełnienia przestępstwa za pomocą środków komunikacji elektronicznej. To kryterium wydaje się być niezwykle szerokie, szczególnie mając na uwadze ciągły rozwój technologii cyfrowych i elektronicznych form komunikacji. Przenoszenie się ludzkiej aktywności do świata cyfrowego powoduje także wzrost liczby typów przestępstw, jakie mogą zostać popełnione za pomocą środków komunikacji elektronicznej. Z pewnością nie wszystkie czyny zabronione popełniane w cyberprzestrzeni wyczerpują znamiona „poważnego przestępstwa" w rozumieniu dyrektywy retencyjnej. Zespół nie przedstawił dowodów, które uzasadniałyby konieczność wykorzystania retencji danych w przypadku wszystkich – bez wyjątku – przestępstw należących do tej szerokiej kategorii.

Nie jest wykluczone, że w przypadku różnych form cyberprzestępczości retencja danych powinna odgrywać większą rolę niż w przypadku pozostałych typów przestępstw. Należy jednak zweryfikować kryteria, które miałyby o tym decydować i doprecyzować zakres zastosowania tego narzędzia, np. ograniczyć go do cięższych przestępstw (zdefiniowanych przy pomocy kryterium dolnej granicy zagrożenia ustawowego) albo zastosować kryterium niezbędności (tj. jeśli danej okoliczności stanu faktycznego nie da się udowodnić przy użyciu innych środków), które miałoby charakter pomocniczy i zawężający.

### 3.6. Przestępstwa karno-skarbowe

W kontekście powyższych zastrzeżeń trudno odnieść się do propozycji poszerzenia katalogu przestępstw, które uzasadniają wykorzystywanie retencji danych, o niektóre przestępstwa karno-skarbowe. W pierwszej kolejności musi bowiem zostać doprecyzowany katalog

---

wybuchowymi, środkami odurzającymi lub substancjami psychotropowymi albo ich prekursorami oraz materiałami jądrowymi i promieniotwórczymi, 6) określonych w art. 8 ustawy z dnia 6 czerwca 1997 r. - Przepisy wprowadzające Kodeks karny (Dz. U. Nr 88, poz. 554 i Nr 160, poz. 1083 oraz z 1998 r. Nr 113, poz. 715), 7) określonych w art. 43-46 ustawy z dnia 1 lipca 2005 r. o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów (Dz. U. Nr 169, poz. 1411), 8) ściganych na mocy umów i porozumień międzynarodowych, gdy inne środki okazały się bezskuteczne albo zachodzi wysokie prawdopodobieństwo, że będą nieskuteczne lub nieprzydatne, sad okręgowy, na pisemny wniosek Komendanta Głównego Policji, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego albo na pisemny wniosek komendanta wojewódzkiego Policji, złożony po uzyskaniu pisemnej zgody właściwego miejscowo prokuratora okręgowego, może, w drodze postanowienia, zarządzić kontrolę operacyjną".

Art. 9e ust. 1 ustawy o Straży Granicznej przewiduje, że „przy wykonywaniu czynności operacyjno-rozpoznawczych, podejmowanych przez Straż Graniczną w celu zapobieżenia, wykrycia, ustalenia sprawców oraz uzyskania i utrwalenia dowodów, ściganych z oskarżenia publicznego, umyślnych przestępstw: 1) określonych w art. 163 § 1, art. 164 § 1, art. 165 § 1, art. 166 § 1 i 2, art. 167, art. 168, art. 171, art. 172, art. 173 § 1, art. 258, art. 264 § 2 i 3 i art. 299 § 1 Kodeksu karnego; 2) określonych w art. 270—275 Kodeksu karnego w zakresie dokumentów uprawniających do przekraczania granicy państwowej; 3) skarbowych, o których mowa w art. 134 § 1 pkt 1 Kodeksu karnego skarbowego, jeżeli wartość przedmiotu czynu lub uszczuplenie należności publicznej przekraczają pięćdziesięciokrotną wysokość najniższego wynagrodzenia za pracę określonego na podstawie odrębnych przepisów; 4) pozostających w związku z przekraczaniem granicy państwowej lub przemieszczaniem przez granicę państwową towarów oraz wyrobów akcyzowych podlegających obowiązkowi oznaczania znakami akcyzy, jak również przedmiotów określonych w przepisach o broni, amunicji oraz o materiałach wybuchowych, a także o przeciwdziałaniu narkomanii; 5) określonego w art. 147 ustawy z dnia 13 czerwca 2003 r. o cudzoziemcach; 6) określonych w art. 228, 229 i 231 Kodeksu karnego, popełnionych przez funkcjonariuszy lub pracowników Straży Granicznej w związku z wykonywaniem obowiązków służbowych; 6a) określonych w art. 229 Kodeksu karnego, popełnionych przez osoby niebędące funkcjonariuszami lub pracownikami Straży Granicznej w związku z wykonywaniem czynności służbowych przez funkcjonariuszy lub pracowników Straży Granicznej; 7) ściganych na mocy umów międzynarodowych, gdy inne środki okazały się bezskuteczne albo zachodzi wysokie prawdopodobieństwo, że będą nieskuteczne lub nieprzydatne, sąd okręgowy, na pisemny wniosek Komendanta Głównego Straży Granicznej, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, lub na pisemny wniosek komendanta oddziału Straży Granicznej, złożony po uzyskaniu zgody Komendanta Głównego Straży Granicznej i pisemnej zgody właściwego miejscowo prokuratora okręgowego, może, w drodze postanowienia, zarządzić kontrolę operacyjną".

przestępstw, których waga uzasadnia korzystanie z zatrzymywanych danych telekomunikacyjnych. Dopiero po dokonaniu takiej weryfikacji będzie można stwierdzić, w jakim zakresie i w stosunku do jakich przestępstw, uprawnienie do korzystania z retencji danych powinno przysługiwać także Wywiadowi Skarbowemu. W tym kontekście, inicjatywa Ministra Finansów, który postuluje, aby w tej kategorii znalazły się jedynie przestępstwa przynoszące poważne straty skarbowi państwa, wydaje się zmierzać w dobrym kierunku. Na przykład w Wielkiej Brytanii służby są uprawnione do korzystania z retencji danych w przypadku ścigania tak zdefiniowanych przestępstw.

### 3.7. Kryterium niezbędności

Na aprobatę zasługuje to, że podczas prac Zespołu poddano dyskusji i rozważano nowe (z punktu widzenia obowiązujących przepisów prawa) kryterium – niezbędności. Służy ono weryfikacji, czy danej okoliczności stanu faktycznego nie da się udowodnić przy użyciu innych (mniej ingerujących w prawa i wolności) środków. Zasadniczo kryterium niezbędności ściśle koresponduje z podstawowymi zasadami dopuszczalności ograniczeń praw człowieka (są one dopuszczalne tylko, jeśli sprostają testowi niezbędności i proporcjonalności). Istotą tego kryterium jest jego funkcja zawężająca (dobrze realizowania np. w regulacji prawnej przyjętej przez Estonię). W praktyce powinno być ono stosowane zarówno przez organy ścigania, w momencie podejmowania decyzji o korzystaniu z danych retencyjnych, jak i podmioty sprawujące kontrolę nad zasadnością wniosku o udostępnienie danych (por. pkt 4.1.) oraz kontrolujące praktyki przetwarzania danych przez policję i inne służby *ex post* (por. pkt 4.3.).

Kryterium niezbędności traci ten walor, jeśli zaczyna być wykorzystywane do poszerzenia podstaw wykorzystywania danych telekomunikacyjnych. Dokładnie w takim kontekście było ono dyskutowane w ramach prac Zespołu. Sugerowano dopuszczenie wykorzystywania retencji danych do wykrywania przestępstw spoza ustalonego katalogu, jeśli wymagałoby tego kryterium niezbędności. Tak skonstruowane przepisy stwarzałyby istotne ryzyko nadużyć i mogłyby wręcz zniweczyć efekt ograniczenia celów, w których mogą być pobierane dane telekomunikacyjne. Trudno wyobrazić sobie skuteczną procedurę weryfikacji (nawet przy zaangażowaniu sądu lub prokuratora), która zapobiegałaby nadużywaniu tej możliwości wyjścia poza ustawowy katalog przestępstw.

### 3.8. Zagrożenie zdrowia lub życia

Pozytywnie oceniamy wprowadzenie odpowiedniej klauzuli w ustawie o Policji, pozwalającej wykorzystywać dane objęte obowiązkiem retencji także w sytuacjach zagrożenia zdrowia lub życia. Dokonana zmiana uwzględnia sygnalizowany przez nas problem reagowania na nagłe przypadki, niemieszczące się w katalogu czynów zabronionych, np. zaginięcia. W celu uniknięcia nadużyć warto jednak doprecyzować, że chodzi tu jedynie o „bezpośrednie" zagrożenie życia lub zdrowia.

### 3.9. Dowodzenie w postępowaniu cywilnym

Zaproponowane w Sprawozdaniu ograniczenie możliwości wykorzystania danych telekomunikacyjnych jako środka dowodowego w postępowaniu cywilnym do sytuacji wyjątkowych, gdy ustalenie danej okoliczności stanu faktycznego w inny sposób jest niemożliwe lub nadto utrudnione, oceniamy pozytywnie przez kontrast do obecnej praktyki stosowania prawa. Uważamy jednak, że zasadne byłoby wprowadzenie całkowitego zakazu korzystania z danych retencyjnych w postępowaniu cywilnym. Temat ten powinien zostać dogłębnie przeanalizowany

i skonsultowany ze środowiskami prawniczymi, aby ocenić, na ile w postępowaniu cywilnym pojawiają się sytuacje uzasadniające tak daleko idącą ingerencję w życie prywatne obywateli (ze względu na zaangażowane interesy i wartości) oraz w jaki sposób zapewnić respektowanie wyjątkowego charakteru sięgania po dane telekomunikacyjne w postępowaniach cywilnych, jeśli okaże się, że całkowita rezygnacja z tego narzędzia nie jest możliwa.

## 4. Zasady kontroli nad dostępem do danych telekomunikacyjnych i ich wykorzystaniem

### 4.1. Weryfikacja zasadności korzystania z danych telekomunikacyjnych

W projektowanej procedurze bezwzględnie powinno się znaleźć rozwiązanie zakładające udział podmiotów zewnętrznych decydujących o zasadności korzystania z danych telekomunikacyjnych. Największe gwarancje ochrony praw i wolności jednostki zapewnia kontrola sprawowana przez sądy, która mogłaby zostać ukształtowana na wzór uregulowań dotyczących kontroli operacyjnej. Sędzia miałby orzekać, co do zasady *ex ante*, czy okoliczności opisane w skierowanym doń wniosku o udostępnienie danych spełniają kryterium niezbędności i proporcjonalności. W przypadkach niecierpiących zwłoki mogłaby zostać zastosowana kontrola sądowa *ex post*. Zwracamy przy tym uwagę na opinię Rzecznik Praw Obywatelskich prof. Ireny Lipowicz, zgodnie z którą brak kontroli sądowej *ex post* bądź *ex ante* stanowi naruszenie art. 45 ust. 1 i art. 77 ust. 2 Konstytucji RP – ograniczenie prawa do sądu[11].

W przypadku gdyby postulat wprowadzenia kontroli sądowej został uznany za niemożliwy do spełnienia ze względu na obciążenie sądów, możliwą do rozważenia alternatywą jest przyznanie odpowiednich uprawnień kontrolnych prokuratorom.

Zadaniem sędziego (prokuratora) byłaby ocena zasadności sięgania po dane telekomunikacyjne przede wszystkim z punktu widzenia adekwatności i niezbędności tego narzędzia w danym stanie faktycznym. Gdyby – tak jak proponuje się w Sprawozdaniu – umożliwić wykorzystywanie danych telekomunikacyjnych także w przypadku przestępstw spoza przyjętego katalogu (por. pkt 3.2.) wprowadzenie niezależnej kontroli sprawowanej przez sądy uważamy za niezbędne. W tym przypadku kontrola sądowa może stanowić ważną gwarancję poszanowania prawa. Istnieje bowiem obawa, że wprowadzenie uznaniowej przesłanki bez zapewnienia ścisłych mechanizmów kontrolnych otworzy policji i innym służbom możliwość obejścia prawnych ograniczeń i powrotu do arbitralnych praktyk w zakresie korzystania z zatrzymywanych danych telekomunikacyjnych.

Kolejną funkcją sędziego (prokuratora) mogłoby być monitorowanie samego procesu pozyskiwania danych, tak jak zostało to uregulowane w Niemczech w ustawie wdrażającej dyrektywę (obecnie prawo to nie obowiązuje w wyniku interwencji Sądu Konstytucyjnego)[12]. Postanowienie sądu o udzieleniu dostępu do danych retencyjnych jest ważne przez 2 miesiące. Sędzia przedłuża ten okres o kolejne 2 miesiące, jeśli – po rozważeniu wpływu dotychczas pozyskanych danych i innych dowodów na przebieg śledztwa – uzna taką potrzebę. W tym modelu sędzia zaznajamia się z materiałem dowodowym już na początku sprawy i jest w stanie rzetelnie ocenić wpływ metod wykorzystywanych przez służby na efekty postępowania.

[11] Szerzej na ten temat w wyroku Trybunału Konstytucyjnego z 10 maja 2000 r. (sygn. akt K 21/99, OTK z 2000 r., Nr 4, poz. 109).

[12] Por. *Rozwiązania prawne w wybranych państwach UE dotyczące możliwości wykorzystywania danych objętych tajemnicą telekomunikacyjną w świetle dyrektywy 2006/24/WE* – ekspertyza zlecona przez Kancelarię Prezesa Rady Ministrów Ośrodkowi Studiów Wschodnich im. Marka Karpia.

Dodatkowym argumentem za przyjęciem modelu kontroli sądowej jest to, że zaprojektowane przez Zespół rozwiązania prawne nie uwzględniają potrzeby ochrony tajemnicy zawodowej, jaka występuje w przypadku zawodów zaufania publicznego (dziennikarzy, lekarzy, prawników itd.). Pozostawienie decyzji o każdorazowym udostępnieniu danych retencyjnych w gestii sądu pozwoliłoby ograniczyć sytuacje ujawniania tajemnicy zawodowej do najbardziej uzasadnionych przypadków.

### 4.2. Rola wewnętrznych pełnomocników

Zespół proponuje wprowadzenie instytucji wewnętrznych pełnomocników ds. kontroli przetwarzania danych na wzór rozwiązania funkcjonującego w Centralnym Biurze Anty-korupcyjnym. Naszym zdaniem, ze względu na specyfikę służb, model kontroli ograniczony do kontroli wewnętrznej może okazać się nieefektywny. Istnieje duże prawdopodobieństwo, że pełnomocnik powołany przez szefa danej służby spośród pracujących w niej funkcjonariuszy, będzie pozostawał w sytuacji „nacisku" ze względu na rozmaite, w tym psychologiczne, uwarunkowania (np. koleżeństwo, poczucie lojalności). Nawet zapewnienie pełnomocnikowi prawnych gwarancji ochrony przed naciskami wewnętrznymi (np. zabezpieczenie przez arbitralnym zwolnieniem), nie zagwarantuje mu niezależności, jaką może mieć organ zewnętrzny.

Jednocześnie uważamy, że instytucja wewnętrznych pełnomocników może odegrać ważną i pozytywną funkcję kontrolną we współpracy z odpowiednio ukształtowanym zewnętrznym organem nadzoru. W szczególności wewnętrzny pełnomocnik może: uczulać funkcjonariuszy na ograniczenia wynikające z przepisów prawa (zasad ochrony danych osobowych, przepisów kompetencyjnych); kontrolować zakres i cele przetwarzania danych osobowych; przygotowywać raporty okresowe (np. szczegółową statystykę wykorzystywania danych telekomunikacyjnych) i ułatwiać prowadzenie kontroli zewnętrznej.

### 4.3. Zewnętrzny organ nadzoru

Jak wynika z Raportu, w polskich warunkach model kontroli zewnętrznej wydaje się być najlepszym rozwiązaniem. Z jednej strony – ze względu na względną niezależność od struktur politycznych władzy wykonawczej, z drugiej – z uwagi na profesjonalny charakter takiego podmiotu, gwarantujący zachowanie poufności i poszanowanie zasad ochrony danych osobowych. Dlatego postulujemy – obok proponowanego wprowadzenia instytucji wewnętrznych pełnomocników ds. kontroli przetwarzania danych – podjęcie działań zmierzających do utworzenia niezależnego organu kontrolującego pracę służb specjalnych z zewnętrz bądź nadanie odpowiednich uprawnień kontrolnych jednemu z istniejących organów, np. Generalnemu Inspektorowi Ochrony Danych Osobowych (dalej: **GIODO**), jeśli ze względów funkcjonalnych czy budżetowych to drugie rozwiązanie zostanie uznane za bardziej uzasadnione.

Zewnętrzny organ nadzoru mógłby być powoływany przez Sejm lub wyłaniany w wyniku innej procedury, o ile tylko stwarzałaby ona gwarancje jego instytucjonalnej niezależności. Istotną kompetencją zewnętrznego organu nadzoru powinno być również rozpatrywanie skarg obywateli na ewentualne nadużycia policji i innych służb w toku podejmowanych działań. Jedynie instytucjonalna niezależność może zagwarantować bezstronne rozstrzygnięcia w tego typu sprawach. Przy czym niezbędnym uzupełnieniem tej funkcji jest prawo obywateli do informacji (*ex post*) o pobieraniu dotyczących ich danych telekomunikacyjnych (por. pkt 4.5.).

### 4.4. Regularna weryfikacja zasadności przetwarzania danych

Proponowane w Sprawozdaniu skrócenie okresu weryfikacji danych przetwarzanych przez policję i inne służby do 5 lat jest krokiem w dobrym kierunku, jednak pozostaje rozwiązaniem niewystarczającym. Zważywszy na przeciętną długość trwania postępowań karnych oraz fakt, że dane telekomunikacyjne mają być pozyskiwane w pewnych przypadkach również na potrzeby postępowania przygotowawczego (które może zakończyć się umorzeniem sprawy), 5-letni okres weryfikacji wciąż stwarza duże ryzyko nadużyć.

Nie można przy tym wykluczyć, że możliwość przechowywania danych przez 5 lat, bez konieczności weryfikacji, zacznie być wykorzystywana do obchodzenia ograniczeń wynikających ze skróconego okresu retencji. Może bowiem dochodzić do pobierania nadmiarowych danych i ich przechowywania bez weryfikacji celów i podstaw przetwarzania, zgodnie z logiką gromadzenia danych „na wszelki wypadek". Dlatego uważamy, że okres weryfikacji danych powinien zostać znacząco skrócony, np. do 1 roku.

### 4.5. Prawo obywateli do informacji o wykorzystywaniu ich danych retencyjnych

Zgodnie z wyrokiem Trybunału Konstytucyjnego z 12 grudnia 2005 r. (sygn. K 32/04), państwo polskie powinno wprowadzić istotną gwarancję ochrony prawa do prywatności: w postaci prawa osoby, której dane osobowe były przetwarzane w ramach czynności operacyjnych, do informacji o tym fakcie oraz prawa do zapoznania się z materiałami postępowania, gdy czynności operacyjne nie są już prowadzone, a postępowanie zostało zakończone. Uważamy za konieczne zabezpieczenie tego ważnego uprawnienia w ramach planowanej reformy.

Ponadto – jak sygnalizowaliśmy wcześniej – wprowadzenie skutecznego mechanizmu kontroli zewnętrznej wymaga odpowiednich uregulowań gwarantujących prawo obywatela do informacji i wprowadzających skorelowane z tym prawem obowiązki po stronie policji oraz innych służb. Bez możliwości pozyskania informacji o pobieraniu danych telekomunikacyjnych, obywatel nie będzie w stanie ustalić zakresu ewentualnych nadużyć ani w sposób zasadny złożyć skargi na jakiekolwiek działanie służb.

Mankamentem proponowanych zmian jest również brak obowiązku podania uzasadnienia, dlaczego skorzystanie z danych telekomunikacyjnych w konkretnym przypadku było konieczne. Brak oficjalnego uzasadnienia utrudniałby zarówno realizację kontroli sądowej (prokuratorskiej) – podczas rozpatrywania wniosku o udostępnienie danych, jak i pracę zewnętrznego organu nadzoru – podczas rozpatrywania skargi konkretnej osoby lub w toku standardowej kontroli.

### 4.6. Szczegółowa sprawozdawczość

Pozytywnie przyjęliśmy propozycję wprowadzenia obowiązku sprawozdawczego spoczywającego na wewnętrznych pełnomocnikach ds. kontroli przetwarzania danych. Zgodnie ze Sprawozdaniem, pełnomocnicy mają zostać zobowiązani do przedstawiania opinii publicznej podstawowych informacji statystycznych o wykorzystywaniu danych telekomunikacyjnych. W naszej opinii ten obowiązek powinien jednak pójść dalej. Z punktu widzenia ochrony interesu społecznego, niezbędne jest prowadzenie i publikowanie szczegółowej statystyki, która nie będzie powielała obowiązku, jaki już dziś spoczywa na operatorach telekomunikacyjnych i Urzędzie Komunikacji Elektronicznej (dalej: **UKE**).

Obowiązek sprawozdawczy powinien zatem dotyczyć nie tylko liczby postępowań, w ramach których policja lub inne podmioty wykorzystywały dane telekomunikacyjne pozyskane dzięki

obowiązkowej retencji danych, ale także m.in.: liczby wewnętrznych postanowień lub decyzji o konieczności pozyskania danych telekomunikacyjnych (z wyszczególnieniem postanowień pierwszorazowych i przedłużających); rodzaju i źródła pozyskiwanych danych; rodzaju przestępstwa, w ściganiu którego skorzystano z tego narzędzia; okresu, jakiego dotyczyło zapytanie o dane telekomunikacyjne; liczby i rodzaju postępowań, które mimo pozyskanych danych zakończyły się niepowodzeniem (np. wskutek nieadekwatności danych do przedmiotu postępowania) itp.

Przebieg debaty na poziomie krajowym, jak i problemy Komisji Europejskiej z wykazaniem niezbędności obowiązkowej retencji danych telekomunikacyjnych pokazują, że konieczna jest o wiele dokładniejsza sprawozdawczość, ilustrująca korzyści, jakie – dzięki obowiązkowi zatrzymywania danych – udało się osiągnąć w konkretnych przypadkach. Ponadto obowiązek prowadzenia szczegółowej sprawozdawczości mógłby się okazać ważnym czynnikiem dyscyplinującym funkcjonariuszy do sięgania po dane telekomunikacyjne jedynie w uzasadnionych przypadkach.

## 5. Brak uregulowań zapewniających ochronę tajemnicy zawodowej

Propozycje zawarte w Sprawozdaniu nie przewidują żadnych mechanizmów zabezpieczających przed pozyskiwaniem i wykorzystywaniem informacji, które podlegają szczególnemu reżimowi prawnemu na gruncie przepisów o ochronie tajemnic ustawowo chronionych oraz art. 180 § 2 k.p.k. Zniesienie tej tajemnicy na gruncie k.p.k. jest możliwe wyłącznie, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a dana okoliczność nie może być ustalona na podstawie innego dowodu. Dotyczy to zawodów prawniczych, dziennikarzy, lekarzy i personelu medycznego, a także duchownych.

Brak odpowiednich uregulowań w tym zakresie oceniamy negatywnie. Uważamy, że w przypadku zawodów zaufania publicznego dopuszczenie wykorzystywania retencji danych w pełnym zakresie (czyli w przypadku zdecydowanej większości przestępstw oraz w ramach postępowania cywilnego) stwarza ryzyko podważenia zasady poufności, zagrożenie dla tajemnicy zawodowej oraz ochrony źródeł informacji dziennikarskich. Naszym zdaniem poszczególne przepisy regulujące cele i zasady pozyskiwania danych telekomunikacyjnych powinny przewidywać – jako zasadę – wyraźne wyłączenia w stosunku do grup, które obowiązuje tajemnica zawodowa. Przy czym należałoby umożliwić odstępstwa od tej zasady w szczególnie uzasadnionych przypadkach. Decyzję o wykorzystaniu danych telekomunikacyjnych chronionych tajemnicą zawodową powinien jednak bezwzględnie podejmować sąd, po dokładnym zbadaniu okoliczności sprawy i przeanalizowaniu możliwych konsekwencji.

## 6. Zwrot kosztów

Naszym zdaniem konieczne jest wprowadzenie obowiązku zwrotu kosztów ponoszonych przez operatorów w związku z realizacją ich obowiązków w zakresie retencji danych. Jeśli ze względu na politykę budżetową państwa nie jest możliwy pełny zwrot kosztów, należy rozważyć przynajmniej częściowe transfery[13]. Doświadczenie innych państw pokazuje, że wprowadzenie tego obowiązku ma znaczenie nie tylko dla interesów ekonomicznych operatorów, ale także dla poszanowania zasady niezbędności i proporcjonalności. Wprowadzenie przynajmniej częściowej rekompensaty – obciążającej budżet podmiotów, które o dane występują –

[13] Np. w Słowacji, mimo że koszty postępowania i udostępniania danych pokrywa sam operator, możliwe jest zakwalifikowanie zakupionego potrzebnego sprzętu do wydatków podatkowych.

przeciwdziałałoby sięganiu po dane retencyjne w sytuacjach nieuzasadnionych. Skutki braku tego typu „zachęty do samoograniczenia", w połączeniu z brakiem zewnętrznej kontroli nad pozyskiwaniem danych retencyjnych i szeroko zakrojonymi celami retencji danych, obserwujemy od ponad 2 lat. Na podstawie statystyk generowanych przez UKE wiemy, że w 2009 r. służby, policja, sądy i prokuratura sięgnęły po dane obywateli ponad milion razy, natomiast w 2010 r. ta liczba wzrosła już o ¼.

* * *

Wyrażamy nadzieję, że zaproponowane przez Zespół rozwiązania staną się w najbliższym czasie przedmiotem konsultacji społecznych i aktywnej debaty z udziałem wszystkich zainteresowanych podmiotów. Liczymy, że zanim propozycje zawarte w Sprawozdaniu zostaną przyjęte przez Radę Ministrów, zostanie przeprowadzona dodatkowa analiza we wskazanym przez nas zakresie, dotycząca zarówno zasadności utrzymania obowiązku retencji danych jak i konkretnych „parametrów" tego obowiązku (w szczególności sposobu skonstruowania katalogu przestępstw i postępowań, których miałaby on dotyczyć).

Naszym zdaniem omawiane projekty przepisów nie regulują w sposób precyzyjny celu pobierania danych telekomunikacyjnych, a proponowane przez Zespół wyjątki od wypracowanego kryterium górnej granicy zagrożenia karą pozbawienia wolności, sprowadzają się w istocie do prób jego obejścia. Ponadto omawiane propozycje rozwiązań prawnych nie spełniają standardów określonych w zaleceniach Komisji Europejskiej oraz EIDO w zakresie proporcjonalności i niezbędności korzystania z danych retencyjnych. Przede wszystkim pozyskiwanie danych telekomunikacyjnych objętych obowiązkiem retencji nie podlega żadnej zewnętrznej formie kontroli, w szczególności nie podlega kontroli sądowej. W związku z powyższym zaproponowane przez Zespół rozwiązania prawne uważamy za zmierzające we właściwym kierunku, ale niedostateczne.

Jednocześnie chcielibyśmy uczulić członków Zespołu, że prace nad omawianą materią powinny być oparte na dogłębnej i szczegółowej analizie, zgodnie ze standardami nowoczesnego prawodawstwa i w myśl zasady tworzenia prawa w oparciu o dowody. Przestrzeganie tych zasad jest szczególnie istotne w przypadku prób uregulowania tak newralgicznej sfery życia obywateli, jak ich prywatność, oraz ingerencji państwa w sferę podstawowych praw i wolności.