



819/14/PL
WP 215

**Opinia 04/2014 w sprawie inwigilacji komunikacji elektronicznej na
potrzeby wywiadu i bezpieczeństwa narodowego**

Przyjęta w dniu 10 kwietnia 2014 r.

Grupa Robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności. Zadania grupy określone są w art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE.

Obsługę sekretariatu zapewnia Dyrekcja C (Prawa Podstawowe i Obywatelstwo Unii Europejskiej) Dyrekcji Generalnej ds. Sprawiedliwości Komisji Europejskiej, B-1049 Bruksela, Belgia, biuro nr MO-59 02/013.

Strona internetowa: http://ec.europa.eu/justice/data-protection/index_en.htm

Streszczenie

Od lata 2013 r. szereg mediów międzynarodowych, opierając się głównie na dokumentach ujawnionych przez Edwarda Snowdena, szeroko informował o inwigilacji prowadzonej przez służby wywiadowcze, zarówno w Stanach Zjednoczonych jak i w Unii Europejskiej. Informacje te dały początek międzynarodowej debacie dotyczącej wpływu inwigilacji prowadzonej na tak dużą skalę na prywatność obywateli. Sposób wykorzystywania przez służby wywiadowcze danych dotyczących naszej codziennej komunikacji, a także treści przekazywanych komunikatów, uwypukla potrzebę wyznaczenia granic prowadzonej inwigilacji.

Prawo do prywatności i do ochrony danych osobowych to prawo podstawowe gwarantowane przez Międzynarodowy Pakt Praw Obywatelskich i Politycznych, europejską konwencję praw człowieka i Kartę praw podstawowych Unii Europejskiej. Oznacza to, że poszanowanie praworządności w sposób konieczny wiąże się z zapewnieniem najwyższego możliwego poziomu ochrony tego prawa.

Na podstawie przeprowadzonej przez siebie analizy Grupa Robocza stwierdza, że programy tajnej, masowej i nieograniczonej inwigilacji są niezgodne z naszymi fundamentalnymi aktami prawnymi i nie mogą być uzasadnione walką z terroryzmem ani innymi poważnymi zagrożeniami dla bezpieczeństwa narodowego. W społeczeństwie demokratycznym ograniczenia praw podstawowych wszystkich obywateli byłyby możliwe do zaakceptowania jedynie wówczas, gdyby taki środek był bezwzględnie konieczny i proporcjonalny.

W związku z tym Grupa Robocza zaleca szereg środków mających zagwarantować praworządność i jej poszanowanie.

Po pierwsze, Grupa Robocza wzywa do zapewnienia większej przejrzystości w odniesieniu do sposobu funkcjonowania programów inwigilacji. Przejrzystość przyczynia się do wzmocnienia i przywrócenia zaufania między obywatelami, rządami i podmiotami prywatnymi. Taka przejrzystość obejmuje lepsze informowanie osób fizycznych w przypadkach, gdy służbom wywiadowczym udzielono dostępu do ich danych. W celu lepszego informowania osób fizycznych o skutkach, jakie może mieć korzystanie z usług komunikacji elektronicznej *online* i *offline* oraz o sposobach lepszego zabezpieczenia się, Grupa Robocza zamierza zorganizować w drugiej połowie 2014 r. konferencję na temat inwigilacji z udziałem wszystkich zainteresowanych stron.

Ponadto Grupa Robocza zdecydowanie opowiada się za bardziej efektywnym nadzorem nad inwigilacją. Skuteczny i niezależny nadzór nad służbami wywiadowczymi, w tym nad przetwarzanymi przez nie danymi osobowymi, ma kluczowe znaczenie dla zagwarantowania, aby w ramach takich programów nie dochodziło do nadużyć. Dlatego też Grupa Robocza uważa, że skuteczny i niezależny nadzór nad służbami wywiadowczymi wiąże się z faktycznym zaangażowaniem organów ochrony danych.

Poza tym Grupa Robocza zaleca egzekwowanie dotychczasowych zobowiązań państw członkowskich UE i stron EKPC w celu zagwarantowania prawa do poszanowania życia prywatnego i ochrony danych osobowych. Grupa Robocza przypomina również, że

administratorzy danych podlegający jurysdykcji UE mają obowiązek przestrzegania właściwych przepisów UE dotyczących ochrony danych. Grupa Robocza przypomina także, że organy ochrony danych mogą zawieszać przepływ danych oraz powinny decydować zgodnie ze swoimi kompetencjami krajowymi, czy w danej sytuacji należy zastosować sankcje.

Podstawy prawnej uzasadniającej przekazanie danych organowi państwa trzeciego do celów masowej i nieograniczonej inwigilacji nie mogą stanowić ani zasady bezpiecznego transferu danych osobowych, ani standardowe klauzule umowne, ani wiążące reguły korporacyjne. W rzeczywistości wyjątki przewidziane w powyższych instrumentach są ograniczone pod względem zakresu i powinny być interpretowane w sposób zawężający. Nie powinny być nigdy stosowane ze szkodą dla poziomu ochrony gwarantowanego przez przepisy UE i instrumenty regulujące przekazywania danych.

Grupa Robocza wzywa instytucje UE do sfinalizowania negocjacji w sprawie pakietu reform dotyczących ochrony danych. Z zadowoleniem przyjmuje w szczególności wniosek Parlamentu Europejskiego dotyczący nowego art. 43a, przewidującego obowiązek informowania osób fizycznych w przypadku, gdy w ciągu ostatnich dwunastu miesięcy organowi publicznemu udzielono dostępu do ich danych. Przejrzystość w odniesieniu do takich praktyk znacznie zwiększy zaufanie.

Ponadto Grupa Robocza uważa, że zakres wyłączenia dotyczącego bezpieczeństwa narodowego powinien zostać sprecyzowany w celu zagwarantowania pewności w odniesieniu do zakresu zastosowania prawa UE. Dotychczas prawodawca europejski nie przyjął jasnej definicji bezpieczeństwa narodowego, również orzecznictwo sądów europejskich nie oferuje wartości dowodowej w tym zakresie.

Na koniec Grupa Robocza zaleca szybkie podjęcie negocjacji dotyczących międzynarodowej umowy w sprawie udzielenia osobom fizycznym odpowiednich gwarancji ochrony danych w trakcie prowadzenia działań wywiadowczych. Grupa Robocza popiera również opracowanie globalnego instrumentu opartego na możliwych do wyegzekwowania ogólnych zasadach w zakresie prywatności i ochrony danych.

GRUPA ROBOCZA DS. OCHRONY OSÓB FIZYCZNYCH W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

powołana na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.,

uwzględniając art. 29 i art. 30 ust. 1 lit. c) oraz ust. 3) wspomnianej dyrektywy,

uwzględniając swój regulamin wewnętrzny, a w szczególności jego art. 12 i 14,

PRZYJMUJE NINIEJSZĄ OPINIĘ:

1. Wprowadzenie

Od lata 2013 r. szereg mediów międzynarodowych, opierając się głównie na dokumentach ujawnionych przez Edwarda Snowdena, szeroko informował o inwigilacji elektronicznej prowadzonej przez służby wywiadowcze, zarówno w Stanach Zjednoczonych (USA) jak i w Unii Europejskiej (UE) oraz w innych krajach na całym świecie. Informacje te dały początek międzynarodowej debacie dotyczącej wpływu inwigilacji elektronicznej prowadzonej na tak dużą skalę na prywatność obywateli. Pojawiły się również pytania o to, na jak daleko posunięte działania powinno zezwalać służbom wywiadowczym prawo pod względem gromadzenia i wykorzystywania informacji o naszym życiu codziennym. W niniejszej opinii przedstawiono wyniki analizy prawnej przeprowadzonej przez organy ochrony danych w UE, współpracujące w ramach Grupy Roboczej Art. 29 (Grupa Robocza), w odniesieniu do konsekwencji programów inwigilacji elektronicznej dla zabezpieczenia prawa podstawowego do ochrony danych i prywatności.

Głównym zadaniem organów ochrony danych jest zagwarantowanie wszystkim osobom fizycznym prawa podstawowego do ochrony danych oraz zapewnienie, aby administratorzy danych przestrzegali wszystkich odnośnych przepisów prawnych. Jednakże wiele organów ochrony danych ma jedynie ograniczone uprawnienia nadzorcze w odniesieniu do służb wywiadowczych lub nie ma ich wcale. Do celów nadzoru nad takimi służbami, w tym nad przetwarzaniem danych osobowych, państwa członkowskie wprowadziły inne mechanizmy. Grupa Robocza dokonała zatem inwentaryzacji różnych mechanizmów stosowanych w UE w zakresie nadzoru nad służbami wywiadowczymi, której wyniki stanowią część niniejszej opinii.

Opinia ta nie odnosi się do scenariuszy związanych z przechwytywaniem danych osobowych w komunikacji przewodowej. Na obecnym etapie Grupa Robocza nie dysponuje wystarczającymi informacjami dotyczącymi tej domniemanej praktyki, które umożliwiłyby ocenę właściwych ram prawnych, nawet w sposób hipotetyczny.

2. Metadane

Ocena ewentualnego naruszenia przepisów dotyczących ochrony danych wymaga w pierwszej kolejności jasnego określenia, z jakim działaniem mamy do czynienia.

Przedstawiciele organów rządowych często wspominają o gromadzeniu metadanych, sugerując, że jest to praktyka o mniejszej wadze niż gromadzenie treści. Nie jest to prawidłowe założenie. Metadane to wszystkie dane dotyczące mającej miejsce komunikacji, z wyjątkiem treści rozmowy. Mogą one obejmować numer telefonu lub adres IP osoby wykonującej połączenie lub wysyłającej wiadomość pocztą elektroniczną, czas i miejsce komunikacji, temat, nazwę adresata itd. Ich analiza może prowadzić do ujawnienia szczególnie chronionych danych dotyczących osób, np. w przypadku połączeń z niektórymi numerami informacyjnymi ośrodków medycznych lub religijnych. Jak stwierdził Europejski Trybunał Praw Człowieka w sprawie Malone¹, przetwarzanie metadanych, w tym przypadku „metering”, stanowi integralny element komunikacji odbywającej się za pośrednictwem telefonu. W rezultacie „ujawnianie tych informacji policji bez zgody abonenta stanowi [...] ingerencję w prawo gwarantowane przez art. 8.” Trybunał podtrzymuje to stanowisko od lat.

Należy również zaznaczyć, że często informacje można łatwiej pozyskać z metadanych niż z faktycznej treści komunikatów². Ze względu na ich ustrukturyzowany charakter łatwo jest je gromadzić i analizować. Zaawansowane narzędzia obliczeniowe umożliwiają analizę dużych zbiorów danych w celu uchwycenia ukrytych w nich wzorców i powiązań, w tym danych osobowych, przyzwyczajzeń i zachowań. Nie odnosi się to do rozmów, które mogą odbywać się w dowolnej formie lub języku.

Zgodnie z art. 2 lit. a) dyrektywy 95/46/WE dane osobowe to „wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (»osoby, której dane dotyczą«); osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio”. Podobna definicja zawarta jest w art. 2 lit. a) Konwencji Rady Europy nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych. Dlatego też w Europie, inaczej niż w innych krajach, metadane są danymi osobowymi i powinny być chronione³.

W wyroku wydanym niedawno w sprawie dotyczącej zatrzymywania danych Trybunał Sprawiedliwości Unii Europejskiej potwierdził, że „Całokształt tych danych [telekomunikacyjnych] może dostarczyć bardzo precyzyjnych wskazówek dotyczących życia prywatnego osób, których dane są zatrzymywane”⁴. Ponadto w tym samym wyroku Trybunał stwierdził, że „obowiązek zatrzymywania przez określony czas związanych z życiem prywatnym danej osoby i jej komunikacją danych [...] stanowi samoistną ingerencję w prawa zagwarantowane w art. 7 karty. Za dodatkową ingerencję w to prawo podstawowe należy też uznać możliwość uzyskania dostępu do tych danych przez właściwe organy krajowe. [...] Okoliczność, że zatrzymywanie i późniejsze wykorzystywanie danych jest dokonywane bez poinformowania o tym abonenta lub zarejestrowanego użytkownika, może [...] wywołać u

¹ ETPC, Malone przeciwko Zjednoczonemu Królestwu, 2 sierpnia 1984 r.

² ACLU przeciwko Clapperowi, sprawa nr 13-3994 (WHP) – pisemne oświadczenie prof. Edwarda W. Feltena przed sądem rejonowym Stanów Zjednoczonych dla rejonu Southern District of New York

³ Jest to stosowana od długiego czasu wykładnia przepisów o ochronie danych. W opinii 4/2007 w sprawie pojęcia danych osobowych Grupa Robocza stwierdziła już, że także „w przypadkach gdy dostępne czynniki identyfikujące nie pozwalają *prima facie* na wyodrębnienie konkretnej osoby, osoba ta może mimo to być »możliwa do zidentyfikowania« ponieważ informacje te, w połączeniu z innymi informacjami (którymi administrator danych dysponuje lub nie), pozwalają na odróżnienie tej osoby od innych”.

⁴ Zob. ETS, sprawy połączone C-293/12 i C-594/12, 8 kwietnia 2014 r., pkt 27.

osób, których danych są zatrzymywane czy też wykorzystywane, poczucie, iż ich życie prywatne podlega stałemu nadzorowi.”⁵.

3. Główne zagadnienia

Informacje przedstawione przez Edwarda Snowdena oznaczały dla wielu bolesne przebudzenie. Nigdy przedtem nie ujawniono istnienia tak wielu różnych programów inwigilacji prowadzonych przez służby wywiadowcze i umożliwiających gromadzenie informacji praktycznie o każdym. Niektóre przypadki wyszły na jaw wcześniej, ale teraz po raz pierwszy debatę można było oprzeć na obszernych dowodach wskazujących na powszechność takich działań. Sposób wykorzystania przez służby wywiadowcze danych dotyczących naszej codziennej komunikacji, a także treści przekazywanych komunikatów, uwypukla potrzebę wyznaczenia granic prowadzonej inwigilacji.

Przed programami masowej inwigilacji nie są obecnie w stanie uchronić się nawet osoby zachowujące w sieci ostrożność. Biorąc pod uwagę liczne wyzwania prawne, techniczne i praktyczne, także organy ochrony danych na całym świecie nie mogą zapewnić satysfakcjonującej ochrony. Niezbędne są zatem zmiany.

W poniższych rozdziałach Grupa Robocza Art. 29 poddaje analizie masowe gromadzenie danych przez służby wywiadowcze w świetle ich programów inwigilacji. Z punktu widzenia prawa należy wprowadzić rozróżnienie między programami inwigilacji prowadzonymi przez służby wywiadowcze państw członkowskich a programami prowadzonymi przez służby wywiadowcze państw trzecich z wykorzystaniem danych obywateli UE.

Programy inwigilacji prowadzone przez państwa członkowskie UE zasadniczo nie będą podlegać prawu UE na podstawie wyłączenia dotyczącego bezpieczeństwa narodowego, które wpisano do traktatów europejskich, a także – w następstwie takiej decyzji umawiających się państw członkowskich – do szeregu rozporządzeń i dyrektyw UE, w tym do dyrektywy o ochronie danych 95/46/WE. Nie oznacza to jednak, że takie programy podlegają wyłącznie prawu krajowemu. Analiza przeprowadzona przez Grupę Roboczą Art. 29 pokazuje, że wprawdzie nie ma zastosowania prawo UE w ogóle, a w szczególności dyrektywa o ochronie danych, jednak służby wywiadowcze, wykonując swoje obowiązki zgodnie z prawem, muszą nadal przestrzegać większości zasad ochrony danych⁶ wynikających z europejskiej konwencji praw człowieka i Konwencji Rady Europy nr 108 w zakresie ochrony danych osobowych. Zasady te często są również zawarte w krajowych konstytucjach państw członkowskich. W żadnych okolicznościach programy inwigilacji oparte na nieograniczonym, masowym gromadzeniu danych osobowych nie mogą spełniać wymogów konieczności i proporcjonalności, ustanowionych wspomnianymi zasadami ochrony danych. Ograniczenia praw podstawowych należy interpretować w sposób zawężający, zgodnie z orzecnictwem Europejskiego Trybunału Praw Człowieka (ETPC)⁷ i Trybunału Sprawiedliwości Unii

⁵ Zob. ETS, sprawy połączone C-293/12 i C-594/12, 8 kwietnia 2014 r., pkt 34, 35 i 37.

⁶ Główne zasady ochrony danych to: uczciwe i zgodne z prawem przetwarzanie danych, ograniczenie celu, konieczność i proporcjonalność, dokładność, przejrzystość, poszanowanie praw osób fizycznych i odpowiednie bezpieczeństwo danych.

⁷ Zob. ETPC, Delcourt, 17 stycznia 1970 r., oraz Klass, 6 września 1978 r.

Europejskiej (ETS)⁸. Oznacza to między innymi, że wszelkie ingerencje muszą być konieczne i proporcjonalne w odniesieniu do celu, który ma zostać osiągnięty. Należy również pamiętać, że nie zakłada się automatycznie zasadności i słuszności przedstawionego przez organ krajowy argumentu dotyczącego bezpieczeństwa narodowego. Powyższe musi zostać dowiedzione.

Grupa Robocza podkreśla, że obowiązkiem rządów państw członkowskich jest wywiązywanie się ze wszystkich poczynionych zobowiązań krajowych i międzynarodowych, w tym zobowiązań wynikających z Międzynarodowego Paktu Praw Obywatelskich i Politycznych. Uchybienie temu obowiązkowi nie tylko narusza prawa podstawowe obywateli tych państw, lecz także osłabia zaufanie społeczeństwa do praworządności.

W odniesieniu do programów inwigilacji prowadzonych przez państwa trzecie sytuacja jest bardziej skomplikowana. W przypadku gromadzenia danych, bezpośrednio ze źródła znajdującego się w UE lub po przekazaniu ich do wspomnianego państwa trzeciego (bądź też do innego państwa trzeciego), przepisy UE mogą nadal mieć zastosowanie w odniesieniu do danych ujawnianych w ramach programów inwigilacji. W rzeczywistości wyłączenie dotyczące bezpieczeństwa narodowego wspomniane powyżej ma zastosowanie tylko do bezpieczeństwa narodowego państwa członkowskiego UE, a nie do bezpieczeństwa narodowego państwa trzeciego. Oczywiście mogą wystąpić sytuacje, w których interes bezpieczeństwa narodowego państwa trzeciego jest zbieżny z interesem państwa członkowskiego i w których uzasadniona może być wspólna inwigilacja. Także w tym przypadku organy publiczne prowadzące inwigilację muszą być w stanie wykazać, dlaczego i w jaki sposób interesy bezpieczeństwa narodowego są zbieżne i powodują wyłączenie przepisów UE.

Spełnione muszą być wszystkie warunki dotyczące przesyłania danych osobowych za granicę określone w dyrektywie 95/46/WE: to oznacza przede wszystkim, że odbiorca zapewnia odpowiedni poziom ochrony i że dane muszą być przekazane zgodnie z pierwotnym celem, dla którego były zgromadzone. Przekazywanie danych musi zatem spełniać wymóg posiadania odpowiedniej podstawy prawnej dla uczciwego i zgodnego z prawem przetwarzania.

Żaden z dostępnych instrumentów, które można wykorzystać jako alternatywną podstawę dla przekazywania danych osobowych do krajów, których nie uznano za zapewniające odpowiedni poziom ochrony (zasady bezpiecznego transferu danych osobowych, standardowe klauzule umowne i wiążące reguły korporacyjne), nie umożliwia organom publicznym państwa trzeciego dostępu do danych osobowych przekazywanych na podstawie wspomnianych instrumentów, jeśli taki dostęp ma zostać wykorzystany do celów nieograniczonej, masowej inwigilacji. W rzeczywistości wyłączenia przewidziane we wspomnianych instrumentach są ograniczone pod względem zakresu i powinny być

⁸ Zob. ETS, sprawy połączone C-293/12 i C-594/12, 8 kwietnia 2014 r., w którym to wyroku Trybunał stwierdził, że zatrzymywanie danych o ruchu bez „jakiegokolwiek zróżnicowania, ograniczenia lub wyjątku” „wyjątkowo szeroko i mocno ingeruje w te podstawowe dla porządku prawnego Unii prawa, przy czym przepisy mające zagwarantować to, że ingerencja ta nie będzie rzeczywiście wykraczać poza to, co ściśle niezbędne, nie regulują precyzyjnie tej kwestii” (pkt 57 w połączeniu z pkt 65).

interpretowane zawężająco (tj. powinny być stosowane w określonych sprawach i w określonych dochodzeniach). Ponieważ wymienione instrumenty mają na celu przede wszystkim zapewnienie ochrony danych osobowych pochodzących z UE, nie powinny być one nigdy stosowane ze szkodą dla poziomu ochrony gwarantowanego przez przepisy UE i instrumenty regulujące przekazywanie danych. Grupa Robocza podkreśla ponadto, że zgodnie z dyrektywą o ochronie danych osobowych obecna ocena poziomu ochrony danych w państwach trzecich zasadniczo nie obejmuje ich przetwarzania do celów egzekwowania prawa lub inwigilacji.

Przedsiębiorstwa muszą mieć świadomość, że mogą naruszać prawo europejskie, jeśli służby wywiadowcze państw trzecich zyskują dostęp do danych obywateli europejskich przechowywanych na ich serwerach lub podporządkowują się nakazowi udostępnienia danych osobowych w dużej ilości. Pod tym względem przedsiębiorstwa mogą znaleźć się w trudnej sytuacji, podejmując decyzję, czy zastosować się do nakazu udostępnienia danych osobowych w dużej ilości, czy też nie: niezależnie od dokonanego wyboru mogą naruszyć przepisy europejskie lub prawo państwa trzeciego. Nie należy wykluczać działań egzekucyjnym przeciwko takim firmom w szczególności w przypadkach, gdy administratorzy danych chętnie i świadomie współpracowali z służbami wywiadowczymi, udostępniając im dane. Przedsiębiorstwa muszą zachowywać maksymalną przejrzystość i zapewnić, aby osoby, których dane dotyczą, miały świadomość, że po przekazaniu ich danych osobowych do uznanych za niezapewniające odpowiedniego poziomu ochrony państw trzecich na podstawie instrumentów dostępnych do celów takich transferów, mogą podlegać inwigilacji ze strony organów publicznych państw trzecich lub organom tym może zostać udzielony dostęp do ich danych, w zakresie, w jakim takie wyjątki są przewidziane wspomnianymi powyżej instrumentami. Główny nacisk kładzie się jednak na znalezienie skutecznego rozwiązania na szczeblu politycznym. Poszanowanie praw podstawowych przez służby wywiadowcze mogłaby zapewniać międzynarodowa umowa przewidująca właściwe gwarancje.

Zapewnienie, aby służby wywiadowcze naprawdę przestrzegały ograniczeń nałożonych na programy inwigilacji wymaga wprowadzenia w przepisach wszystkich państw członkowskich realnych mechanizmów nadzoru. Powinny do nich należeć w pełni niezależne kontrole przetwarzania danych prowadzone przez niezależny organ, a także uprawnienia umożliwiające skuteczne egzekwowanie przepisów. Oprócz skutecznego i efektywnego nadzoru parlamentarnego cel ten może osiągnąć organ ochrony danych lub inny odpowiedni niezależny organ, zależnie od mechanizmów nadzoru przyjętych w państwie członkowskim. W przypadku gdyby nadzór miał być prowadzony przez inny organ, Grupa Robocza zachęca do utrzymywania regularnych kontaktów między takim organem a krajowym organem ochrony danych w celu zapewnienia spójnego i konsekwentnego stosowania zasad ochrony danych.

Należy podkreślić, że mechanizmy nadzoru powinny nie tylko istnieć na papierze, lecz muszą być także konsekwentnie stosowane. Informacje ujawnione przez Edwarda Snowdena pokazały, że chociaż na papierze istnieje wiele mechanizmów kontroli i równowagi, w tym kontrola sądowa planowanych programów gromadzenia danych, wątpliwa jest skuteczność stosowania tych zabezpieczeń. Jeśli zabezpieczenia przed nieuzasadnionym dostępem nie mają zastosowania do wszystkich programów inwigilacji lub do wszystkich osób fizycznych,

nie tworzą one systemu, który Grupa Robocza mogłaby uznać za system gwarantujący realny nadzór.

4. Nadzór nad służbami wywiadowczymi

W minionych latach eksperci z różnych podmiotów przeprowadzali liczne analizy mechanizmów nadzoru nad służbami bezpieczeństwa i służbami wywiadowczymi w państwach trzecich, jednak mniej takich analiz dotyczyło krajowych służb wywiadowczych w poszczególnych państwach członkowskich. Aby uzyskać jaśniejszy obraz różnych stosowanych w Europie mechanizmów nadzoru nad krajowymi służbami wywiadowczymi, Grupa Robocza przesłała wszystkim organom ochrony danych (w tym dwóm obserwatorom spoza UE) kwestionariusz w celu zebrania informacji o stosowanych w ich krajach praktykach nadzorczych w tym zakresie⁹.

W szczególności przeanalizowania warte są dwie kwestie:

1. istnienie kompleksowego nadzoru w obrębie ramach prawnych stanowiących podstawę działania krajowych służb bezpieczeństwa i wywiadowczych;
2. rola (lub brak roli) krajowego organu nadzorczego ds. ochrony danych w takich ramach.

W niniejszej opinii Grupa Robocza odpowiada także na wniosek wiceprzewodniczącej Komisji Europejskiej Viviane Reding dotyczący zbadania, jaka mogłaby być rola organów ochrony danych¹⁰.

4.1. Przegląd odnośnych krajowych mechanizmów nadzoru

Działania w zakresie inwigilacji omawiane w niniejszej opinii oraz w załączonym dokumencie roboczym prowadzone są głównie przez służby wywiadowcze w związku z ich zadaniem polegającym na ochronie bezpieczeństwa narodowego. Zależnie od tradycji prawnych danego państwa i struktur odpowiedzialnych za sprawy bezpieczeństwa narodowego, występuje znaczne zróżnicowanie modeli nadzoru. W 26 z 27 państw członkowskich, które odpowiedziały na kwestionariusz¹¹, służby wywiadowcze istnieją i działają na podstawie przepisów określających ich kompetencje, strukturę i obowiązki. Jedno z państw członkowskich nie posiada służb wywiadowczych, a bezpieczeństwo państwa zapewnia krajowa policja¹².

Większość respondentów wskazała na istnienie od jednego do trzech organów ds. bezpieczeństwa i wywiadu na poziomie krajowym. Ogólnie rzecz biorąc, występuje podział na wewnętrzne i zewnętrzne (zagraniczne) zagrożenia dla bezpieczeństwa narodowego, co

⁹ Na kwestionariusz odpowiedziało 27 krajowych organów ochrony danych z UE, regionalny organ ochrony danych z Saksonii (Niemcy) oraz organy ochrony danych spoza UE, mianowicie ze Szwajcarii i z Serbii.

¹⁰ List wiceprzewodniczącej Reding do przewodniczącego Grupy Roboczej Art. 29, 30 sierpnia 2013 r.

¹¹ Austria, Belgia, Bułgaria, Cypr, Republika Czeska, Dania, Estonia, Finlandia, Francja, Niemcy, Grecja, Węgry, Włochy, Łotwa, Litwa, Luksemburg, Malta, Niderlandy, Polska, Portugalia, Rumunia, Słowacja, Słowenia, Hiszpania, Szwecja, Zjednoczone Królestwo.

¹² Irlandia.

skutkuje również podziałem zadań między organy cywilne (ministerstwo spraw wewnętrznych lub sprawiedliwości) i wojskowe (ministerstwo obrony). W trzech państwach zintegrowano różne struktury, tworząc system ochrony podległy bezpośrednio szefowi rządu (np. premierowi).

Dane osobowe są przetwarzane na podstawie prawa obowiązującego na poziomie państwa członkowskiego, a nadzór bazuje albo na przepisach ogólnych o ochronie danych (zwanym dalej „przepisami ogólnymi ODO”), albo na jednym bądź większej liczbie aktów prawnych regulujących kwestię przetwarzania danych osobowych przez jedną lub więcej służb wywiadowczych.

4.2. Rola krajowego organu nadzorczego ds. ochrony danych

Z oceny odnośnych ustawodawstw krajowych wynika jasno, że w wielu krajach przepisy ogólne ODO nie mają zastosowania do działalności służb wywiadowczych oraz że rola organu ochrony danych pod względem nadzoru jest ograniczona, a w niektórych przypadkach w ogóle nie odgrywa on takiej roli. Często prawo przewiduje określone zasady ochrony danych, niekoniecznie jednak obejmujące odpowiedni nadzór ze strony organu ochrony danych.

W dwóch państwach spoza UE, które zgodziły się odpowiedzieć na kwestionariusz¹³ przetwarzanie danych osobowych przez służby wywiadowcze regulowane jest przepisami ogólnymi ODO. Na podstawie ogólnych przepisów ODO podlegają one nadzorowi ze strony krajowego organu ochrony danych.

Tam, gdzie mają zastosowanie, przepisy ogólne ODO zasadniczo przewidują szereg wyłączeń (odstępstw od jednej lub większej liczby zasad) dotyczących przetwarzania danych przez służby wywiadowcze. Wyłączenia te zwykle odnoszą się do podstawowych obowiązków administratorów danych i osób, których dane dotyczą¹⁴. Ograniczenia mogą odnosić się do prawa do bycia poinformowanym i prawa dostępu, przysługującego osobie, której dane dotyczą i zwykle wykonywanego za pośrednictwem organu ochrony danych.

W odniesieniu do nadzoru nad przetwarzaniem danych wydaje się, że tylko w czterech państwach członkowskich krajowe przepisy ogólne dotyczące ochrony danych (lub akt prawny ustanawiający ogólny organ nadzorczy ds. ochrony danych) przewidują w zasadzie te same uprawnienia nadzorcze w stosunku do służb wywiadowczych, co w stosunku do wszystkich innych administratorów danych¹⁵. W trzynastu państwach członkowskich kompetencje nadzorcze organu ochrony danych obejmują krajowe służby bezpieczeństwa i wywiadowcze, lecz w niektórych przypadkach do nadzoru nad takimi służbami mają zastosowanie specjalne przepisy lub procedury, w tym możliwość nałożenia sankcji¹⁶. W dziewięciu państwach członkowskich organ ochrony danych nie ma uprawnień

¹³ Serbia (jedna służba cywilna, dwie wojskowe), Szwajcaria (jedna służba cywilna, jedna wojskowa).

¹⁴ Np. Belgia, Bułgaria, Cypr, Niemcy, Węgry, Grecja. W przypadku niektórych państw członkowskich nie udało się uzyskać informacji o wyłączeniach.

¹⁵ Bułgaria, Węgry, Słowenia, Szwecja.

¹⁶ Austria, Belgia, Cypr, Estonia, Finlandia, Francja, Niemcy, Irlandia, Włochy, Łotwa, Luksemburg, Polska, Szwecja.

nadzorczych w stosunku do służb wywiadowczych odgrywających rolę administratorów danych¹⁷.

Tylko w Szwecji i Słowenii organ ochrony danych sprawuje pełny nadzór nad przestrzeganiem odpowiednich obowiązków w zakresie ochrony danych. Tam, gdzie niektóre inne krajowe organy ochrony danych dysponują uprawnieniami w odniesieniu do służb wywiadowczych, kontrolują one zgodność z właściwymi przepisami ogólnymi dotyczącymi ochrony danych, rozpatrują skargi i wykonują prawo dostępu do danych na rzecz odnośnych osób fizycznych. Mają również prawo do prowadzenia dochodzeń z własnej inicjatywy lub na wniosek osób trzecich, a także do prowadzenia kontroli na miejscu. W niektórych państwach członkowskich uprawnienia te mogą podlegać pewnym ograniczeniom, takim jak obowiązek przestrzegania podczas dochodzenia specjalnych zasad bezpieczeństwa ze względu na wymogi tajemnicy państwowej.

4.3. Rola innych mechanizmów niezależnego nadzoru

Dwadzieścia państw członkowskich oświadczyło, że ich przepisy przewidują nadzór parlamentarny lub kontrolę nad działalnością służb wywiadowczych, zarazem określając kompetencje organów ochrony danych w zakresie przetwarzania danych¹⁸, a także specjalne wewnętrzne systemy kontrolne¹⁹. Wydaje się jednak, że państwa członkowskie rozumieją kontrolę parlamentarną na różne sposoby, przy czym w niewielu przypadkach wiąże się ona z faktycznym istnieniem organu odpowiedzialnego za nadzór nad ochroną danych (w tym za ocenę przestrzegania praw osób, których dane dotyczą, oraz zgodności zarówno z przepisami ogólnymi dotyczącymi ochrony danych jak i z przepisami szczegółowymi)²⁰.

Istniejące systemy nadzoru są skrajnie zróżnicowane i obejmują następujące rozwiązania:

- Komisja parlamentarna, której zadanie może być zdefiniowane szeroko – jako nadzór nad organami wywiadowczymi i bezpieczeństwa w ogóle – lub jako nadzór nad określoną służbą wywiadowczą.
- Parlamentarny nadzór lub kontrola obok innych (niebędących organem ochrony danych) niezależnych organów nadzoru. Kontrola parlamentarna sprawowana jest przez rzecznika praw obywatelskich, delegację parlamentarną lub komisję parlamentarną.
- Komisja parlamentarna jest jedynym organem nadzorczym poza strukturą władzy wykonawczej. Zadania parlamentu są tu sformułowane albo w sposób raczej ogólny, albo w taki, że dostęp do otwartych spraw nie jest przewidziany.

¹⁷ Republika Czeska, Dania, Malta, Niderlandy, Portugalia, Rumunia, Słowacja, Hiszpania, Zjednoczone Królestwo.

¹⁸ Np. w Finlandii oprócz organu ochrony danych odpowiedzialny w tym zakresie jest też rzecznik praw obywatelskich, jednak jego kompetencje wynikają ze specjalnych przepisów dotyczących służb bezpieczeństwa i wywiadowczych.

¹⁹ Wspomniane dwadzieścia państw członkowskich to: Austria, Bułgaria, Cypr, Republika Czeska, Estonia, Finlandia, Francja, Niemcy, Grecja, Węgry, Włochy, Łotwa, Luksemburg, Polska, Portugalia, Rumunia, Słowacja, Słowenia, Hiszpania, Zjednoczone Królestwo.

²⁰ Opinia nie obejmuje analizy informacji o kontroli kierowniczej (ministerialnej) i ogólnej politycznej, przedstawionych przez kilka państw.

- Obowiązek nadzoru spoczywa wyłącznie na specjalnym organie. Chociaż kompetencje mogą być określane za pomocą aktów prawnych o ochronie danych, do niedawna obserwowano też przypadki, w których taki organ działał w granicach określonych prawem miękkim.
- Ogólnemu nadzorowi parlamentarnemu towarzyszy specjalistyczna kontrola sądowa.
- Oprócz ogólnego organu ochrony danych funkcjonuje zasada łączonej kontroli sprawowanej przez przedstawicieli władzy wykonawczej i parlamentu, przy czym przewodniczącym specjalnej komisji jest sędzia, a pozostali członkowie wywodzą się z różnych partii politycznych zasiadających w parlamencie minionej i obecnej kadencji. Istnieją procedury konsultacji z organem ochrony danych.
- Inspirację dla usprawnienia elementów nadzoru można również czerpać z systemów, w których ustanowiono specjalny organ zajmujący się nadzorem nad służbami wywiadowczymi pod kątem ochrony danych: komisję nadzoru nad danymi, w której skład wchodzi trzech prokuratorów wyznaczonych przez prokuratora generalnego, nadzorującą służby wywiadowcze wraz z parlamentarną radą nadzoru.

Istnieje możliwość wniesienia sprawy do organu ochrony danych w celu ustalenia, czy ma ona związek z bezpieczeństwem narodowym, a w razie stwierdzenia takiego związku dana sprawa musi zostać przekazana dwóm niezależnym komisarzom sprawującym nadzór sądowy nad krajowymi służbami wywiadowczymi, przy czym nakazy prowadzenia inwigilacji niejawnej wydaje sekretarz stanu. Wspiera ich specjalny trybunał ds. roszczeń osób, których dane dotyczą.

- Odpowiedni akt prawny przewiduje współpracę między specjalnym organem nadzorczym a ogólnym organem ochrony danych: niezależny komisarz ds. ochrony prawnej musi wydać zezwolenie, jeśli służby bezpieczeństwa lub wywiadowcze zamierzają prowadzić określone działania (np. tajne dochodzenia, nadzór wideo nad określonymi osobami). Komisarz ds. ochrony prawnej ma poza tym obowiązek przedłożenia organowi ochrony danych skargi, jeśli uważa, że doszło do naruszenia praw wynikających z przepisów ogólnych dotyczących ochrony danych.

Organ ochrony danych ma prawo do nadzoru, z pewnymi ograniczeniami, nad służbami wywiadowczymi, lecz za nadzór nad inwigilacją komunikacji i rozpatrywanie skarg odpowiada specjalny organ parlamentarny. Członków odnośnego komitetu wyznacza komisja kontroli parlamentarnej. Przewodniczącym musi być osoba posiadająca kwalifikacje do sprawowania urzędu sądowego.

5. Zalecenia

A. Większa przejrzystość

1. Potrzebna jest większa przejrzystość w odniesieniu do sposobu funkcjonowania programów oraz działań i decyzji nadzorców

Grupa Robocza uważa za istotne, aby państwa członkowskie zapewniły maksymalną przejrzystość w zakresie swojego zaangażowania w programy gromadzenia i wymiany danych do celów wywiadowczych, najlepiej na forum publicznym, lecz w razie konieczności co najmniej wobec swoich parlamentów krajowych i właściwych organów nadzorczych. Organom ochrony danych zaleca się udostępnianie swojej wiedzy fachowej na poziomie krajowym w celu przywrócenia równowagi między interesami bezpieczeństwa narodowego a podstawowym prawem do poszanowania życia prywatnego osób fizycznych.

Należy wprowadzić pewną formę ogólnej sprawozdawczości z działań w zakresie inwigilacji, także w myśl spoczywającego na państwach członkowskich obowiązku zapewnienia przejrzystości, jaki wynika z orzecznictwa Europejskiego Trybunału Praw Człowieka²¹. Każde naruszenie praw podstawowych musi być przewidywalne, w związku z czym programy takie muszą opierać się na jasnych, szczegółowych i dostępnych przepisach. Zachęca się krajowe organy ochrony danych do zwrócenia na to stanowisko uwagi swoich odnośnych rządów.

2. Większa przejrzystość po stronie administratorów danych

Przedsiębiorstwa muszą zachowywać maksymalną przejrzystość i zapewniać, aby osoby, których dane dotyczą, miały świadomość, że po przekazaniu ich danych osobowych do uznanych za niezapewniające odpowiedniego poziomu ochrony państw trzecich na podstawie instrumentów dostępnych do celów takich transferów, mogą podlegać inwigilacji ze strony organów publicznych państw trzecich lub organom tym może zostać udzielony dostęp do ich danych, w zakresie, w jakim takie wyjątki są przewidziane tymi instrumentami. Grupa Robocza zdaje sobie sprawę, że administratorzy danych mogą dostać polecenie wstrzymania się od informowania osoby, której dane dotyczą, o nakazie wydanym przez organ publiczny. Grupa przyjmuje z zadowoleniem podjęte niedawno wysiłki mające na celu zapewnienie osobom, których dane dotyczą, lepszych i obszerniejszych informacji o wnioskach otrzymywanych przez administratorów danych i zachęca przedsiębiorstwa do dalszego doskonalenia polityki informacyjnej.

3. Maksymalizacja świadomości publicznej

Osoby, których dane dotyczą, muszą być świadome konsekwencji, jakie może mieć korzystanie z usług komunikacji elektronicznej *online* i *offline*, a także jakie są sposoby lepszego zabezpieczania się. Odpowiadają za to wspólnie organy ochrony danych, inne organy publiczne, przedsiębiorstwa, a także społeczeństwo obywatelskie. W tym celu Grupa Robocza zamierza zorganizować w drugiej połowie 2014 r. konferencję, w trakcie której wszystkie zainteresowane strony przedyskutują możliwe podejścia.

²¹ Zob. także Europejski Trybunał Praw Człowieka, sprawa nr 48135/06 – Inicjatywa Młodych na rzecz Praw Człowieka przeciwko Serbii (25 czerwca 2013 r.), s. 6.

B. Skuteczniejszy nadzór

1. Utrzymanie spójnego systemu prawnego dla służb wywiadowczych, w tym przepisów dotyczących ochrony danych

W następstwie informacji ujawnionych przez Edwarda Snowdena stało się jasne, że służby wywiadowcze państw członkowskich UE codziennie przetwarzają duże ilości danych osobowych. Dane te są również udostępniane innym służbom w UE i poza nią. Grupa Robocza uważa za istotne, aby w państwach członkowskich istniały spójne ramy prawne działania służb wywiadowczych, w tym przepisy dotyczące przetwarzania danych zgodnie z zasadami ochrony danych ustanowionymi prawem europejskim i międzynarodowym. Prawa osób, których dane dotyczą, powinny być zagwarantowane w możliwie największym stopniu, przy jednoczesnym zapewnieniu ochrony interesu publicznego.

Ponadto Grupa Robocza zaleca, aby krajowe ramy prawne obejmowały jasne przepisy dotyczące współpracy i wymiany danych osobowych z organami ścigania w celu zapobiegania przestępstwom, zwalczania ich i ścigania, w tym dotyczące przekazywania takich danych organom w innych państwach członkowskich UE i w państwach trzecich.

2. Zapewnienie skutecznego nadzoru nad służbami wywiadowczymi

W krajowych ramach prawnych działania służb wywiadowczych szczególną uwagę należy zwrócić na stosowane mechanizmy nadzoru. Właściwy, skuteczny i niezależny nadzór ma w społeczeństwie demokratycznym podstawowe znaczenie. Grupa Robocza uważa zatem, że wykorzystanie dobrych praktyk zaczerpniętych z różnych mechanizmów nadzoru stosowanych obecnie w państwach członkowskich powinno stanowić element mechanizmów nadzoru we wszystkich tych państwach. Wzywa się krajowe organy ochrony danych do wprowadzenia następujących aspektów do krajowej debaty dotyczącej nadzoru nad służbami wywiadowczymi:

- silna wewnętrzna kontrola zgodności z krajowymi ramami prawnymi w celu zapewnienia rozliczalności i przejrzystości;
- skuteczna kontrola parlamentarna zgodna z tradycjami parlamentarnymi poszczególnych państw. Krajowe organy ochrony danych powinny zachęcać parlamenty dysponujące już uprawnieniami w zakresie nadzoru nad służbami wywiadowczymi do czynnej realizacji tych zadań;
- skuteczny, solidny i niezależny nadzór zewnętrzny, sprawowany albo przez specjalny organ przy udziale organu ochrony danych albo przez sam organ ochrony danych, mający prawo regularnego dostępu do danych i innej odpowiedniej dokumentacji z własnej inicjatywy (z urzędu), a także obowiązek rozpatrywania otrzymanych skarg. Nie może być wymagana uprzednia zgoda służb wywiadowczych na poddanie ich nadzorowi.

C. Skuteczne stosowanie obowiązujących przepisów

1. Egzekwowanie dotychczasowych zobowiązań państw członkowskich UE i umawiających się stron EKPC w celu zagwarantowania prawa do poszanowania życia prywatnego i ochrony danych

Wszystkie państwa członkowskie są stronami europejskiej konwencji praw człowieka. W związku z tym muszą przestrzegać warunków określonych w art. 7 i 8 EKPC w odniesieniu do własnych programów inwigilacji. Na tym ich obowiązki się nie kończą. Art. 1 EKPC wymaga od stron zapewnienia każdej osobie podlegającej ich jurysdykcji praw i wolności określonych w konwencji. W obu scenariuszach przeciwko każdemu państwu członkowskiemu UE, a także każdej stronie EKPC, może zostać wniesiona do ETPC skarga dotycząca naruszenia prawa europejskich podmiotów prawnych do poszanowania życia prywatnego.

2. Administratorzy danych podlegający jurysdykcji UE mają obowiązek przestrzegania właściwych europejskich przepisów o ochronie danych

Administratorzy danych mający siedzibę w UE lub korzystający z urządzeń znajdujących się w państwie członkowskim muszą przestrzegać swoich obowiązków wynikających z prawa UE, nawet jeśli prawo innych krajów, w których prowadzą działalność, jest sprzeczne z prawem UE. W tym zakresie organy ochrony danych nie mogą ignorować faktu, że dane mogą być przekazywane z naruszeniem prawa UE. Grupa Robocza przypomina zatem, że zgodnie z warunkami ustanowionymi unijnymi i krajowymi przepisami o ochronie danych organy ochrony danych mogą zawieszać przepływy danych przewidziane w instrumentach przekazywania danych, jeśli istnieje istotne prawdopodobieństwo, że naruszane są zasady ochrony danych, a dalsze przekazywanie danych powodowałoby bezpośrednie narażenie osób, których dane dotyczą, na poważną szkodę. Krajowe organy ochrony danych powinny decydować, zgodnie ze swoim zakresem kompetencji, czy w danej sytuacji należy nałożyć sankcje.

D. Poprawa ochrony na poziomie europejskim

1. Przyjęcie pakietu reform w obszarze ochrony danych

Finalizacja negocjacji dotyczących pakietu reform w obszarze ochrony danych ma fundamentalne znaczenie dla zapewnienia skutecznej ochrony danych w Europie. Nowe ogólne rozporządzenie o ochronie danych i dyrektywa o ochronie danych w przypadku policji i wymiaru sprawiedliwości mają na celu nie tylko lepszą ochronę danych osobowych osób fizycznych. Mają one również sprecyzować swój zakres zastosowania i przyznać większe uprawnienia egzekucyjne organom ochrony danych. Zwłaszcza możliwość nakładania – w ostateczności – kar (finansowych) powinna zapewnić im większy wpływ na administratorów danych. Grupa Robocza z zadowoleniem przyjmuje wniosek Parlamentu Europejskiego dotyczący obowiązkowego informowania osób fizycznych w przypadku, gdy w ciągu ostatnich 12 miesięcy organowi publicznemu udzielono dostępu do ich danych. Przejrzystość w odniesieniu do takich praktyk znacznie zwiększy zaufanie. Grupa Robocza

wzywa zatem Radę i Parlament Europejski do dotrzymania uzgodnionych terminów²² i zapewnienia, aby oba instrumenty zostały przyjęte w 2014 r.

2. Sprecyzowanie zakresu wyłączenia dotyczącego bezpieczeństwa narodowego

W chwili obecnej brakuje wspólnego porozumienia odnośnie do wykładni pojęcia bezpieczeństwa narodowego. Prawodawca europejski nie przyjął jasnej definicji, również orzecznictwo sądów europejskich nie jest pod tym względem rozstrzygające. Wyłączenie nie może jednak obejmować przetwarzania danych osobowych do celów, do których nie mogą być zgodnie z prawem wykorzystane.

Kolejne pytanie wymagające odpowiedzi dotyczy tego, w jakim stopniu wyłączenie uzasadnione względami bezpieczeństwa narodowego w dalszym ciągu odzwierciedla rzeczywistość dziś, kiedy wydaje się, że działalność służb wywiadowczych bardziej niż kiedykolwiek dotychczas zazębia się z działalnością organów ścigania i służy szeregowi różnych celów. Dane wymieniane są stale i w skali globalnej, przy czym nie ma znaczenia, do ochrony bezpieczeństwa którego kraju ma zostać wykorzystana analiza przekazywanych danych. Grupa Robocza wzywa zatem Radę, Komisję i Parlament do osiągnięcia porozumienia w zakresie definicji zasady bezpieczeństwa narodowego i jasnego określenia, co należy uznać za wyłączną domenę państw członkowskich. Definicja zasady bezpieczeństwa narodowego powinna w należyty sposób uwzględniać aspekty poruszone przez Grupę Roboczą, w tym w niniejszej opinii. Wzywa się również instytucje UE do sprecyzowania w pakiecie reform w zakresie ochrony danych, że sama ochrona bezpieczeństwa narodowego państw trzecich nie może uzasadniać wyłączenia zastosowania prawa UE.

E. Międzynarodowa ochrona mieszkańców UE

1. Nacisk na odpowiednie gwarancje w związku z wymianą danych wywiadowczych

Organy publiczne państw trzecich w ogóle, a ich służby wywiadowcze w szczególności, nie mogą mieć bezpośredniego dostępu do danych sektora prywatnego przetwarzanych w UE. Jeśli ubiegają się o dostęp do takich danych w określonej sprawie i na podstawie zasadnego podejrzenia, powinny – stosownie do sytuacji – złożyć wnioski zgodnie z umowami międzynarodowymi, zapewniając odpowiednie gwarancje ochrony danych. W odniesieniu do wymiany informacji wywiadowczych państwa członkowskie muszą zapewnić, aby przepisy krajowe przewidywały szczegółową podstawę prawną dla przekazywania takich danych oraz odpowiednie gwarancje ochrony danych osobowych. Zdaniem Grupy Roboczej tajne umowy o współpracy między państwami członkowskimi lub państwami trzecimi nie spełniają norm określonych przez Europejski Trybunał Praw Człowieka w zakresie jasnej i dostępnej podstawy prawnej.

²² <http://euobserver.com/justice/122853>

2. Wynegocjowanie międzynarodowych umów dotyczących udzielenia odpowiednich gwarancji ochrony danych

Krokiem we właściwym kierunku jest idea tzw. umowy ramowej, negocjowanej obecnie między USA i UE. Umowa taka będzie jednak prawdopodobnie cechować się dwoma niedociągnięciami: będzie wyłączać przypadki dotyczące bezpieczeństwa narodowego, przynajmniej z punktu widzenia UE, gdyż jest negocjowana jako umowa oparta tylko na prawie UE. Poza tym jej struktura sugeruje, że będzie mieć zastosowanie tylko do danych przekazywanych między organami publicznymi w USA i UE, i nie będzie uwzględniać danych gromadzonych przez podmioty prywatne. Wynika to również ze sprawozdania grupy kontaktowej wysokiego szczebla UE–USA ds. wymiany informacji oraz ochrony prywatności i danych osobowych²³, stanowiącego podstawę dla negocjacji dotyczących umowy ramowej. Grupa Robocza podkreśla, że zgodnie ze wspomnianą umową ramową cel przetwarzania przekazywanych danych powinien być taki sam zarówno w UE jak i w USA. Niedopuszczalne byłoby, aby dane pochodzące z organów ścigania w UE były następnie wykorzystywane do celów bezpieczeństwa narodowego przez wywiad amerykański, jeśli nie jest to możliwe również w UE.

Ponieważ umowa ramowa nie zapewni pełnej ochrony wszystkim obywatelom, potrzebna jest umowa międzynarodowa gwarantująca odpowiednią ochronę przed nieograniczoną inwigilacją. Gdyby taka umowa jasno określiła granice inwigilacji, złagodziłoby to również występująca obecnie kolizję jurysdykcji wpływająca na część ujawnionych działań w zakresie inwigilacji. Umowa taka byłaby jednak bezpośrednio powiązana z wyłączeniem dotyczącym bezpieczeństwa narodowego, a zatem wykraczałaby poza zakres prawa UE. Dlatego też do państw członkowskich należy rozpoczęcie negocjacji w skoordynowany sposób. Odpowiednią uwagę należy zwrócić na jasne określenie, które z opisanych działań w zakresie inwigilacji uznano by faktycznie za istotne dla bezpieczeństwa narodowego, a które za związane raczej z egzekwowaniem prawa i celami polityki zagranicznej, a zatem obszarami objętymi prawem unijnym. Umożliwiłoby to instytucjom UE większe zaangażowanie w przypadku podjęcia kroków w tym kierunku.

Taka nowa umowa nie może być tajna. Musi zostać opublikowana i powinna określać obowiązki umawiających się stron w odniesieniu do koniecznego nadzoru nad programami inwigilacji, w odniesieniu do przejrzystości, równego traktowania co najmniej obywateli wszystkich umawiających się stron umowy, mechanizmów dochodzenia roszczeń i innych praw związanych z ochroną danych. Należałoby ponadto zachęcić umawiające się strony do dopilnowania, aby ich parlamenty były regularnie informowane o stosowaniu zawartej umowy i płynących z niej korzyściach.

3. Opracowanie globalnego instrumentu ochrony prywatności i danych osobowych

Grupa Robocza popiera opracowanie globalnego instrumentu umożliwiającego stosowanie możliwych do wyegzekwowania ogólnych zasad ochrony prywatności i danych,

²³ Dokument Rady 15851/09, 23 listopada 2009 r.

uzgodnionych przez Międzynarodową Konferencję Rzeczników Ochrony Danych Osobowych i Prywatności w deklaracji madryckiej²⁴. Pod tym względem można rozważyć przyjęcie dodatkowego protokołu do art. 17 Międzynarodowego Paktu Praw Obywatelskich i Politycznych ONZ. W odniesieniu do takiego międzynarodowego instrumentu należy zapewnić, aby oferowane gwarancje dotyczyły wszystkich zainteresowanych osób fizycznych. Konieczne jest również wypracowanie ogólnej wykładni „przetwarzania danych”, ponieważ na całym świecie występują poważne różnice w rozumieniu tego terminu.

Grupa Robocza popiera inicjatywę podjętą przez rząd niemiecki i wezwanie Międzynarodowej Konferencji Rzeczników Ochrony Danych Osobowych i Prywatności^{25,26}. Ponadto Grupa nadal popiera przystąpienie państw trzecich do Konwencji Rady Europy nr 108.

²⁴ Międzynarodowe standardy ochrony danych osobowych i prywatności, przyjęte przez 31. Międzynarodową Konferencję Rzeczników Ochrony Danych Osobowych i Prywatności w Madrycie.

²⁵ <http://www.bundesregierung.de/Content/EN/Artikel/2013/07/2013-07-19-bkin-nsa-sommerpk.html>.

²⁶ Rezolucja dotycząca oparcia ochrony danych i ochrony prywatności na prawie międzynarodowym, przyjęta w trakcie 35. Międzynarodowej Konferencji Rzeczników Ochrony Danych Osobowych i Prywatności w Warszawie.