

Inwigilacja prowadzona przez służby wywiadowcze: środki zabezpieczające prawa podstawowe oraz środki prawne dostępne w Unii Europejskiej

Streszczenie

Artykuł 7 Karty praw podstawowych Unii Europejskiej gwarantuje wszystkim obywatelom Unii Europejskiej (UE) poszanowanie życia prywatnego i rodzinnego, podczas gdy art. 8 gwarantuje prawo do ochrony ich danych osobowych. Dane te muszą być przetwarzane rzetelnie w określonych celach, a każdej osobie zapewnia się prawo dostępu do danych osobowych, które jej dotyczą, oraz prawo do dokonania ich sprostowania. Przewiduje się w nim także, że przestrzeganie tego prawa podlega kontroli niezależnego organu. Artykuł 47 zapewnia prawo do skutecznego środka prawnego, w tym do sprawiedliwego i jawnego rozpatrzenia sprawy w rozsądnym terminie.

Kiedy w czerwcu 2013 r. światowe media obieły tzw. „dokumenty Snowdena”, światło dzienne ujrzały rozległe globalne programy inwigilacji realizowane przez służby wywiadowcze. Doniesienia Snowdena nie były pierwszym przykładem wskazującym na istnienie niezwykle rozbudowanego układu w zakresie inwigilacji komunikacyjnej, jaki powstał w następstwie ataków terrorystycznych z 11 września 2001 r. Niemniej sama skala tych doniesień jest bezprecedensowa, co potencjalnie wiąże się z naruszeniem prywatności osób na całym świecie. Inwigilacja nie jest już jedynie ukierunkowana na informacje stanowiące tajemnicę państwa lub tajemnicę przedsiębiorstwa, ale dopuszcza szeroko zakrojone przechwytywanie komunikacji jednostek. Działanie takie stoi w sprzeczności zarówno z zasadą poszanowania prawa do życia prywatnego, jak i prawa do ochrony danych – które na szczęblu UE zabezpieczone są na mocy Karty praw podstawowych

Unii Europejskiej (Karta). Do zadań UE i jej państw członkowskich należy ochrona wspomnianych praw, również w kontekście inwigilacji, a także zapewnienie dostępności środków odwoławczych umożliwiających zaskarżenie bezprawnej inwigilacji.

„Taka masowa i nieukierunkowana inwigilacja jest nieproporcjonalna ze swojej natury i stanowi nieuzasadnioną ingerencję w prawa zagwarantowane w art. 7 i 8 Karty”.

(TSUE, opinia rzecznika generalnego z dnia 23 września 2015 r. w sprawie Maximillian Schrems/Data Protection Commissioner, C-362/14)

Doniesienia wywołały szereg różnych reakcji. W środowisku wywiadowczym, w szczególności wśród wyspecjalizowanych organów odpowiedzialnych za nadzór nad służbami wywiadowczymi, przeprowadzono specjalne postępowania i sporządzono sprawozdania badające implikacje płynące z doniesień Snowdena. Instytucje UE zareagowały zdecydowanie. Zarówno Komisja Europejska, Rada Unii Europejskiej, jak i Parlament Europejski przedłożyły sprawozdania dotyczące tych doniesień, wyraziły obawy odnośnie do programów masowej inwigilacji, zwróciły się do władz Stanów Zjednoczonych o wyjaśnienie tej sprawy i prowadziły działania na rzecz odbudowania zaufania w stosunkach między USA a UE. Chociaż jest jeszcze zbyt wcześnie, aby ocenić pełny wpływ doniesień Snowdena, postępowania wyjaśniające prowadzone w następstwie tych doniesień w niektórych państwach członkowskich UE wykazały, że konieczne jest podjęcie reform obecnych krajowych ram prawnych. Konieczność taką podkreślił także Parlament Europejski w rezolucji

z marca 2014 r. w sprawie realizowanych przez NSA amerykańskich programów nadzoru, organów nadzoru w różnych państwach członkowskich oraz ich wpływu na prawa podstawowe obywateli UE oraz na współpracę transatlantycką w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych (2013/2188(INI), P7_TA(2014)0230), ustanawiającej akt pt. *Habeas corpus w europejskiej przestrzeni cyfrowej*.

„Wyznania Snowdena dały nam szansę na reakcję. Mam nadzieję, że będzie miała ona pozytywny skutek i że dalsze działania podjęte zostaną przez nowy Parlament, po wyborach, ponieważ możemy być dumni z pakietu dotyczącego ochrony danych osobowych”.

(Claude Moraes, poseł sprawozdawca w parlamentarnym śledztwie dotyczącym NSA, Komunikat prasowy z dnia 12 marca 2014 r.)

Analiza ram prawnych państw członkowskich UE dotyczących nadzoru

W kwietniu 2014 r. Parlament Europejski zwrócił się do Agencji Praw Podstawowych Unii Europejskiej (FRA) „o przeprowadzenie szczegółowego badania na temat ochrony praw podstawowych w kontekście inwigilacji”. Agencja Praw Podstawowych Unii Europejskiej przeprowadziła takie badanie, dokonując analizy ram prawnych dotyczących inwigilacji obowiązujących w 28 państwach członkowskich UE i przedstawiając opis istniejących norm w zakresie praw podstawowych. W badaniu szczególny nacisk położono na mechanizmy kontroli oraz środki odwoławcze przysługujące jednostkom podnoszącym zarzuty naruszenia ich prawa do prywatności.

Przedmiotem badania prawnego FRA nie są techniki inwigilacji jako takie. Agencja przeanalizowała, w jaki sposób obecne ramy prawne umożliwiają stosowanie tego rodzaju technik i zbadała kluczową rolę, jaką wyspecjalizowane organy odgrywają w kontroli pracy służb wywiadowczych. Ponadto w ramach badania dokonano skrupulatnej kontroli zakresu, w jakim odpowiednie środki

zabezpieczające gwarantują ochronę prywatności i danych w 28 państwach członkowskich UE.

„Służby wywiadowcze” są uprawnione do działania na arenie międzynarodowej i koncentrują się na zagrożeniach zewnętrznych, podczas gdy „służby bezpieczeństwa” posiadają mandat do działania na szczeblu krajowym i koncentrują się na zagrożeniach dla bezpieczeństwa wewnętrznego. W sprawozdaniu FRA określenia „służby wywiadowcze” użyto jako terminu rodzajowego obejmującego oba te pojęcia.

Niniejsze streszczenie zawiera główne ustalenia badania FRA, które w pełnej wersji opublikowano w sprawozdaniu zatytułowanym „Inwigilacja prowadzona przez służby wywiadowcze: środki zabezpieczające prawa podstawowe oraz środki prawne dostępne w Unii Europejskiej – analiza ram prawnych w państwach członkowskich” (*Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Mapping Member States’ legal frameworks*) (zob. Dalsze informacje).

Gromadzenie i zakres danych

W ramach tych badań FRA przyjrzała się systemom prawnym w zakresie inwigilacji w 28 państwach członkowskich UE, analizując ustawy i odpowiednie normy praw podstawowych w celu sporządzenia analizy porównawczej stanu prawnego w dziedzinie inwigilacji w całej UE.

Na podstawie odpowiedzi przekazanych za pośrednictwem multidyscyplinarnej sieci badawczej FRA, zwanej Franet, Agencja zgromadziła dane i informacje, przeprowadzając badanie źródeł we wszystkich 28 państwach członkowskich. Dodatkowe informacje zgromadzono w drodze konsultacji

z kluczowymi partnerami, w tym z szeregiem krajowych urzędników łącznikowych w państwach członkowskich, wyspecjalizowanymi organami oraz indywidualnymi ekspertami. Ustalenia opierają się także na istniejących sprawozdaniach i publikacjach, które mają na celu wspieranie ustawodawców krajowych w ustanawianiu ram prawnych dla służb wywiadowczych i demokratycznego nadzoru nad ich działaniami.

Drugie sprawozdanie społeczno-prawne zawierające opinie FRA, sporządzone na podstawie badań empirycznych, zostanie opublikowane w późniejszym terminie i zawierać będzie rozwinięcie ustaleń przedstawionych w niniejszym streszczeniu.

Środki zabezpieczające prawa podstawowe a prawo Unii

*„Smutna prawda jest taka, że wykorzystywanie technologii masowej inwigilacji skutecznie eliminuje prawo do prywatności w komunikacji przez internet”.
(specjalny sprawozdawca ONZ ds. propagowania i ochrony praw człowieka i wolności podstawowych w warunkach walki z terroryzmem (2014), czwarte sprawozdanie roczne przedłożone Zgromadzeniu Ogólnemu Organizacji Narodów Zjednoczonych, A/69/397, 23 września 2014)*

Państwa członkowskie UE zobowiązane są przestrzegać minimalnych międzynarodowych standardów w zakresie praw człowieka określonych przez Organizację Narodów Zjednoczonych, które mają powszechne zastosowanie, takich jak rezolucja Rady Praw Człowieka dotycząca prawa do prywatności w epoce cyfrowej (dok. A/HRC/28/L.27, 24 marca 2015 r.). W następstwie doniesień Snowdena różne organy eksperckie i traktatowe ONZ potępiły praktyki masowej inwigilacji. Normy Rady Europy, w tym orzecznictwo Europejskiego Trybunału Praw Człowieka (ETPC), także określają standardy minimalne. Ponadto istotne znaczenie ma prawo Unii zgodnie z wykładnią Trybunału Sprawiedliwości Unii Europejskiej (TSUE). Wreszcie w dziedzinie, w której bezpośrednio zastosowanie ma jedynie ograniczona liczba przepisów międzynarodowych – innych niż istniejące międzynarodowe prawa człowieka – ważne są także środki samoregulacji i instrumenty „miękkiego prawa”.

Główne kwestie poruszane w sprawozdaniu dotyczą prawa do prywatności i do ochrony danych, które zapisane są w art. 7 i 8 Karty. Uregulowania w zakresie prawa do ochrony danych wynikają także z pierwotnego i wtórnego prawa Unii, co gwarantuje, w odpowiednich granicach ich stosowania, że przetwarzanie danych osobowych odbywa się zgodnie z prawem i jedynie w zakresie koniecznym do osiągnięcia zamierzonego zasadnego celu. Wspomniane prawa obejmują wszystkie osoby, niezależnie od tego, czy mają one status obywateli UE czy obywateli państw trzecich. Zgodnie z art. 52 ust. 1 Karty wszelkie ograniczenia w korzystaniu z tych praw muszą być konieczne i proporcjonalne, a także rzeczywiście odpowiadać celom interesu ogólnego uznawanym przez Unię, muszą być przewidziane ustawą i szanować istotę tych praw.

Mimo że istnieją międzynarodowe wytyczne, w UE brak jest jednolitego zrozumienia określenia

„bezpieczeństwa narodowego”. Ani prawodawstwo Unii, ani orzecznictwo TSUE nie precyzują tego pojęcia, chociaż TSUE orzekł, że wyjątki od praw podstawowych należy poddawać wykładni zawężającej i uzasadniać.

Ta niejasność w definiowaniu „bezpieczeństwa narodowego” niesie ze sobą konsekwencje w obszarze stosowania prawa Unii. Artykuł 4 ust. 2 Traktatu o Unii Europejskiej stanowi, że „bezpieczeństwo narodowe pozostaje w zakresie wyłącznej odpowiedzialności każdego państwa członkowskiego”. Nie oznacza to, że wyłączenie dotyczące „bezpieczeństwa narodowego” czyni stosowanie prawa Unii całkowicie niemożliwym. Wykładnia pojęcia „bezpieczeństwo narodowe” na szczeblu państw członkowskich oraz sposób prowadzenia programów inwigilacji mogą podlegać ocenie instytucji UE, w szczególności TSUE.

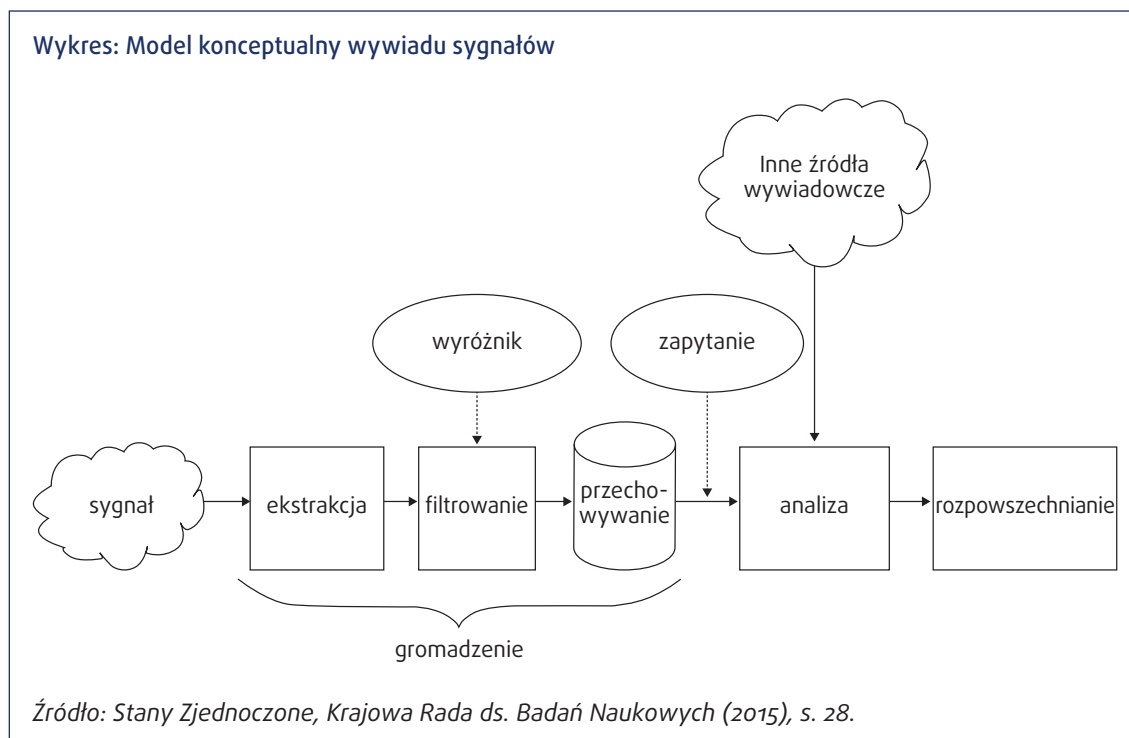
Rodzaje inwigilacji: ukierunkowana i nieukierunkowana

W badaniu FRA analizie poddano sposób, w jaki ramy prawne państw członkowskich UE regulują kwestię inwigilacji, zarówno ukierunkowanej, jak i nieukierunkowanej.

Niderlandzki komitet ds. kontroli służb wywiadowczych i służb bezpieczeństwa (CTIVD) proponuje następujące definicje inwigilacji ukierunkowanej i nieukierunkowanej:

- przechwytywanie ukierunkowane odnosi się do „przechwytywania w przypadku gdy osoba, organizacja lub właściwość techniczna, w stosunku do której gromadzenie danych ma zastosowanie, może być określona zawczasu”;
- przechwytywanie nieukierunkowane odnosi się do „przechwytywania w sytuacji, gdy nie można z góry określić, z jaką osobą, organizacją lub właściwością techniczną wiąże się gromadzenie danych”.

CTIVD, *Sprawozdanie roczne 2013-2014*, Haga, 31 marca 2014 r., s. 45-46



Już sama skala gromadzenia danych za pośrednictwem ujawnionych programów inwigilacji, takich jak PRISM, Xkeysoce i Upstream, wywołała burzę reakcji. „Masowa inwigilacja” (często rozumiana jako nieukierunkowana) oznacza gromadzenie zupełnie innych ilości danych niż w przypadku tradycyjnych metod tajnej inwigilacji (ukierunkowanej), takich jak podsłuch telefoniczny. Ten ostatni stosowany jest w wyniku istnienia wcześniejszego podejrzenia określonej osoby lub organizacji. Jest to najbardziej powszechny i najczęściej uznawany w przepisach prawa obowiązujących w państwach członkowskich UE typ inwigilacji. W przeważającej większości państw członkowskich UE ramy prawne nie regulują, a wręcz nie odnoszą się do „masowej inwigilacji” jako takiej. Jedynie kilka państw członkowskich UE dysponuje szczegółowym ustawodawstwem dotyczącym wywiadu sygnałów (SIGINT), który jest terminem rodzajowym opisującym przechwytywanie przez służby wywiadowcze sygnałów pochodzących z różnych źródeł. Terminu tego używa się w całej analizie przeprowadzonej w ramach badania FRA.

SIGINT ma swoje źródło w wywiadzie wojskowym. Odnosi się do automatycznego zbierania informacji poprzez przechwytywanie i gromadzenie danych cyfrowych związanych z działaniem wywiadowczym. Wykres pokazuje wyraźnie, że zgromadzone sygnały filtrowane są poprzez zastosowanie wyróżników lub selektorów – zbioru parametrów umiejscowionych w procesie filtrowania, *a priori* lub w sposób dynamiczny, w celu zdefiniowania kryteriów dla określenia, które dane należy przechowywać,

aby uzyskać odpowiednie informacje (na przykład „wszystkie adresy e-mail wykorzystane w komunikacji z Jemenem”).

Krajowa Rada ds. Badań Naukowych Krajowych Akademii Naukowych w Stanach Zjednoczonych określiła wywiad sygnałów jako pojęcie obejmujące wszelkie dane przechowywane na nośniku elektronicznym. Komisja Wenecka stosuje termin SIGINT jako pojęcie zbiorcze dla określenia środków i metod przechwytywania i analizowania komunikacji radiowej (w tym satelitarnej i komórkowej) oraz przewodowej.

Analiza FRA dotycząca ram prawnych regulujących metody inwigilacji stosowane przez służby wywiadowcze pokazuje, że przepisy obowiązujące w pięciu państwach członkowskich UE (we Francji, w Niemczech, w Niderlandach, w Szwecji i w Zjednoczonym Królestwie) szczegółowo określają warunki stosowania zarówno ukierunkowanej, jak i nieukierunkowanej inwigilacji, takiej jak wywiad sygnałów. W pozostałych państwach członkowskich przepisy w niewystarczającym stopniu określają te warunki, co utrudnia przeprowadzenie analizy prawnej procedur faktycznie stosowanych w odniesieniu do gromadzenia wywiadu sygnałów. Mimo że przepisy obowiązujące w tych krajach nie zawierają konkretnych odniesień do SIGINT, wywiad tego rodzaju może być prowadzony. Niemniej z uwagi na to, że w tych krajach praktyka ta jest określona jedynie w niepublikowanych środkach regulacyjnych, analiza obowiązujących ram prawnych nie rzuci światła na tę kwestię.

Kluczowe ustalenia

Służby wywiadowcze i przepisy prawa w zakresie nadzoru

Cel i struktura służb wywiadowczych

Głównym celem służb wywiadowczych w społeczeństwach demokratycznych jest ochrona bezpieczeństwa narodowego i podstawowych wartości otwartego społeczeństwa poprzez stosowanie narzędzi wywiadowczych. Organizacja struktur wywiadowczych w poszczególnych państwach członkowskich UE jest ściśle związana z uwarunkowaniami historycznymi poszczególnych państw i niekoniecznie jest zgodna ze standardami w zakresie praw podstawowych. W rezultacie w strukturach organizacyjnych służb wywiadowczych w całej UE występują znaczne różnice. W niektórych państwach członkowskich prace prowadzą dwie służby wywiadowcze, podczas gdy w innych zadanie to wykonuje pięć czy sześć organów.

- W przeważającej większości państw członkowskich UE ustanowiono co najmniej dwa różne organy służb wywiadowczych, jeden odpowiedzialny za sprawy cywilne, a drugi za kwestie wojskowe, przy czym te ostatnie nie są przedmiotem niniejszego sprawozdania. Cywilne służby wywiadowcze zasadniczo podlegają ministerstwu spraw wewnętrznych, a czasem także premierowi lub prezydentowi.
- W niektórych państwach członkowskich służby cywilne podlegają dalszemu podziałowi na jedną służbę z mandatem krajowym i jedną, której przyznano mandat zagraniczny. Ponadto niektóre państwa członkowskie powierzyły środki wywiadowcze jednostkom wyspecjalizowanym w działaniach dotyczących konkretnego zagrożenia, na przykład przestępczości zorganizowanej, korupcji czy walce z terroryzmem.

Ochrona bezpieczeństwa narodowego

W badaniu FRA przyjrano się pojęciu „bezpieczeństwa narodowego” w świetle mandatu przyznanego służbom bezpieczeństwa i środkom inwigilacji, które mogą one podejmować. Ustalenia będące wynikiem tego badania po raz kolejny wskazują na znaczną różnorodność pomiędzy państwami członkowskimi UE.

- Głównym celem służb wywiadowczych jest ochrona bezpieczeństwa narodowego, ale pojęcie to nie jest zharmonizowane w państwach członkowskich UE. Rzadko definiuje się zakres bezpieczeństwa narodowego, przy czym czasami stosuje się terminy bliskoznaczne. Niektóre państwa członkowskie w ogóle nie stosują terminu „bezpieczeństwo narodowe”, a zamiast tego posługują się określeniami „bezpieczeństwo wewnętrzne” lub „bezpieczeństwo zewnętrzne”, bądź też „bezpieczeństwo państwa”.
- Zakres rozmaitych zadań realizowanych przez służby wywiadowcze (tj. ich mandat) nie jest jednakowy we wszystkich państwach członkowskich UE. Oprócz bardziej tradycyjnych dziedzin, uprawnienia niektórych służb wywiadowczych obejmują przestępczość zorganizowaną i cyberprzestępczość. Definicje tych terminów nie są zharmonizowane.

Prawne uregulowanie inwigilacji

Granica pomiędzy zadaniami w zakresie egzekwowania prawa, a zadaniami służb wywiadowczych czasem się zaciera. Każde poszerzenie zakresu zadań musi być należycie uzasadnione jako konieczne dla zapewnienia ochrony państwa, co stanowi główny powód tworzenia służb wywiadowczych.

- Ramy prawne obowiązujące w większości państw członkowskich regulują jedynie inwigilację ukierunkowaną, obejmującą osoby fizyczne lub określone grupy/organizacje. Oprócz uregulowania inwigilacji ukierunkowanej, w pięciu państwach członkowskich wprowadzono w życie przepisy dotyczące warunków stosowania wywiadu sygnałowy.
- W świetle obowiązujących standardów w dziedzinie praw człowieka krajowe ramy prawne nie zawierają jasnych definicji określających kategorie osób i zakres działań, jakie mogą być przedmiotem gromadzenia wywiadu.
- Działalność służb wywiadowczych jest uregulowana prawnie w zdecydowanej większości państw członkowskich (w 26 z 28). Przepisy prawa określają sposób organizacji i funkcjonowania służb wywiadowczych danego kraju. Konstytucja jednego państwa członkowskiego zakazuje służbom wywiadowczym podejmowania działań w zakresie inwigilacji. W innym państwie członkowskim procedura przyjęcia aktu ustawodawczego regulującego praktyki służb

wywiadowczych tego państwa w dziedzinie inwigilacji jest w toku.

- Analiza FRA pokazuje, że podstawy prawne przyznawania mandatów i uprawnień krajowym służbom wywiadowczym w państwach członkowskich UE znacznie się różnią – może to być pojedynczy akt prawny regulujący strukturę organizacyjną służb krajowych i środki, jakimi dysponują, bądź też szereg powiązanych ustaw i rozporządzeń regulujących określone aspekty mandatu, organizacji, kompetencji tych służb, czy też środków, jakimi dysponują.
- Większość państw członkowskich organizuje pracę służb wywiadowczych w drodze dwóch ustaw: jednej dotyczącej mandatu i organizacji służb i drugiej mającej za przedmiot środków działania i warunki ich podejmowania.
- Większość państw członkowskich UE (23 z 28) oddzieliło służby wywiadowcze od organów ścigania. W dwóch państwach członkowskich zrezygnowano ostatnio z systemów, w ramach których służby wywiadowcze podlegały policji lub organom ścigania o podobnym charakterze.

Nadzór nad służbami wywiadowczymi

Analiza FRA podejmuje kwestie mechanizmów odpowiedzialności służb wywiadowczych stosujących inwigilację. Opisano w niej w szczególności sposób ustanowienia mechanizmów pociągania do odpowiedzialności w państwach członkowskich UE. Nadzór jest sposobem na zapewnienie odpowiedzialności publicznej za decyzje i działania służb wywiadowczych. Zdaniem ekspertów nadzór ma na celu zapobieganie nadużywaniu uprawnień, legitymizację wykonywania uprawnień o charakterze ingerencyjnym i uzyskanie lepszego rezultatu po dokonaniu oceny konkretnych działań. Sprawozdanie Komisji Weneckiej oraz inne badania naukowe wskazują na ogólny konsensus co do tego, że nadzór powinien łączyć w sobie:

- kontrolę wykonawczą;
- nadzór parlamentarny;
- organy eksperckie;
- kontrolę sądową.

Kontrola wykonawcza i koordynacja organów nadzoru

Władza wykonawcza może sprawować kontrolę nad służbami wywiadowczymi na wiele różnych sposobów: poprzez określanie ich polityki i priorytetów strategicznych lub ustanawianie wytycznych; mianowanie lub powoływanie kierownictwa wyższego szczebla w ramach tych służb; opracowywanie budżetu ostatecznie poddawanego pod głosowanie w parlamencie; lub poprzez zatwierdzanie współpracy z innymi służbami. W niektórych państwach członkowskich władza wykonawcza odgrywa także kluczową rolę w odniesieniu do udzielania zezwoleń na podejmowanie środków inwigilacji.

Skuteczny nadzór wymaga właściwej koordynacji działań różnych organów, w celu objęcia nadzorem każdego aspektu działalności służb wywiadowczych. Konsekwencją braku jasności i pełnej wiedzy organów nadzoru odnośnie do działalności całego krajowego środowiska wywiadowczego będą luki w sprawowanym nadzorze, a skuteczność systemu nadzoru jako takiego będzie ograniczona.

- Zróżnicowanie państw członkowskich UE pod względem systemów politycznych i prawnych przekłada się na ogromną różnorodność organów sprawujących nadzór nad służbami wywiadowczymi. W państwach członkowskich UE występują poważne różnice, jeżeli chodzi o systemy nadzoru. Chociaż istniejące systemy mogą posłużyć jako źródła dobrych praktyk, istnieją obszary, dla których korzystna byłaby reforma prawna, zwiększająca uprawnienia organów nadzoru.
- Poszczególnym organom nadzoru przyznaje się cały wachlarz uprawnień, przy czym różny jest zakres, w jakim organy mogą wykonywać te uprawnienia.
- W siedmiu państwach członkowskich funkcjonują systemy nadzoru łączące władzę wykonawczą, parlament i władzę sądowniczą (poprzez zatwierdzenie *ex ante*) oraz organy eksperckie. Niemniej do tych państw nie należą żadne z tych, w których ustanowiono ramy prawne dopuszczające gromadzenie wywiadu sygnałów.
- Skuteczny nadzór nie musi być równoznaczny z występowaniem wszystkich czterech mechanizmów nadzoru. Nadzór tego rodzaju może przynosić efekty pod warunkiem, że istniejące organy uzupełniają się i wspólnie tworzą silny system pozwalający na dokonanie oceny, czy sposób



wykonywania mandatu przez służby wywiadowcze jest właściwy. Realizacja tego celu będzie możliwa, jeżeli uprawnienia nadzoru obejmować będą wszystkie obszary działalności służb wywiadowczych. W przypadku gdy sam mandat jest źródłem niejasności lub nie został wystarczająco określony, organy nadzoru nie będą w stanie wywrzeć jakiegokolwiek wpływu.

- Niezbędny jest dostęp organów nadzoru do informacji i dokumentów. Chociaż informacje zebrane przez służby wywiadowcze mają charakter poufny, a środki ochronne muszą zagwarantować odpowiedni sposób postępowania z nimi, organy nadzoru nie mogą wykonywać swoich zadań, jeżeli nie uzyskały uprzednio dostępu do istotnych informacji. Normą wydaje się jednak przeciwna sytuacja.

Nadzór parlamentarny

Nadzór parlamentarny ma istotne znaczenie z uwagi na to, że do zadań parlamentu należy rozliczanie rządu. Parlament, jako ustawodawca, odpowiada za stanowienie zrozumiałych i przystępnych przepisów w zakresie tworzenia służb wywiadowczych i określania ich struktury organizacyjnej, szczególnych uprawnień i ograniczeń. Do jego zadań należy zatwierdzanie budżetu służb wywiadowczych, a w niektórych państwach członkowskich również kontrola, czy ich działania wpisują się w ustalone ramy prawne.

- Ustalenia FRA pokazują, że nadzór parlamentarny stosowany jest w 24 państwach członkowskich UE; w 21 z nich służby wywiadowcze podlegają nadzorowi ze strony specjalnych komisji parlamentarnych. W niektórych państwach członkowskich ustanowiono jedną komisję parlamentarną właściwą do nadzoru nad różnymi służbami bezpieczeństwa i służbami wywiadowczymi, podczas gdy w innych utworzono szereg komisji nadzorujących każdą ze służb osobno.
- W żadnym państwie członkowskim komisje parlamentarne nie mają nieograniczonego dostępu do informacji wywiadowczych.
- Poszczególnym komisjom parlamentarnym w państwach członkowskich przyznaje się mandat o różnym zakresie: w większości z nich uprawnienia do nadzoru tradycyjnie odnoszą się do ustawodawstwa, budżetu i otrzymywania informacji dotyczących funkcjonowania służb, podczas gdy bardzo niewiele z nich posiada uprawnienia do rozpatrywania skarg, wydawania wiążących decyzji czy pomocy w zatwierdzeniu środków wywiadowczych.

- Co się tyczy uprawnień komisji parlamentarnych w zakresie wszczynania śledztw, przepisy prawa obowiązujące w większości państw upoważniają te komisje do występowania z wnioskiem o przekazanie informacji przez służby wywiadowcze lub organy władzy wykonawczej, ale nie do żądania przekazania takich informacji.

Nadzór ekspercki

Nadzór ekspercki jest szczególnie wartościowy, ponieważ umożliwia kontrolowanie działalności służb wywiadowczych przez osoby zorientowane w temacie, dysponujące czasem, aby poświęcić się tej kwestii, i niezwiązane politycznymi sojuszami. Zdaniem Komisarza Praw Człowieka Rady Europy są to często osoby najbardziej odpowiednie do sprawowania bieżącego nadzoru nad działalnością służb bezpieczeństwa i służb wywiadowczych.

- Chociaż nadzór parlamentarny jest kluczowy, musi on być uzupełniany przez nadzór prowadzony przez inne organy, w szczególności silne organy eksperckie, które mogą obejmować nadzorem działalność operacyjną, w tym w zakresie gromadzenia, wymiany i wykorzystywania danych osobowych, jak również kwestię ochrony prawa do życia prywatnego.
- W 15 państwach członkowskich UE ustanowiono przynajmniej jeden organ ekspercki, którego działalność skupia się wyłącznie na sprawowaniu nadzoru nad służbami wywiadowczymi. Kompetencje tych organów obejmują zatwierdzanie środków inwigilacji, badanie skarg, kierowanie do służb wywiadowczych wniosków o dostarczenie dokumentów lub informacji, a także doradztwo na rzecz organów władzy wykonawczej lub parlamentu. W celu maksymalnego wykorzystania ich potencjału, organom eksperckim należy zapewnić odpowiedni poziom niezależności, zasobów i uprawnień.
- W niektórych państwach członkowskich zatwierdzanie środków inwigilacji nie odbywa się z udziałem jakichkolwiek instytucji niezależnych od służb wywiadowczych i organów władzy wykonawczej.
- W tych państwach członkowskich, w których funkcjonuje niezależny organ zajmujący się zatwierdzaniem środków inwigilacji, inwigilacja ukierunkowana zwykle wymaga zgody organu sądowego, a alternatywnym preferowanym rozwiązaniem jest zgoda wydana przez organ ekspercki. Brak jest powszechnie przyjętego podejścia do nadzoru nad gromadzeniem wywiadu sygnałów.

- Chociaż niezbędna jest znajomość aspektów prawnych inwigilacji, organy eksperckie muszą także posiadać kompetencje techniczne. Niektóre państwa członkowskie zapewniają spełnienie tego warunku poprzez włączanie do tych organów ekspertów specjalizujących się w szeregu różnych dziedzin, w tym w technologiach informacyjnych i komunikacyjnych (ICT). Inne, z kolei, kładą duży nacisk na połączenie w składzie obecnych lub byłych sędziów i parlamentarzystów.

W państwach członkowskich UE kluczową rolę w dziedzinie ochrony danych osobowych powierzono organom ochrony danych – wyspecjalizowanym organom powołanym w celu zapewnienia ochrony prywatności i ochrony danych. – Rola ta wynika z prawa pierwotnego i wtórnego UE. Jednakże organy eksperckie wyspecjalizowane w dziedzinie nadzoru nad służbami wywiadowczymi bez wątpienia posiadają potwierdzoną wiedzę fachową w zakresie ochrony prywatności i danych w obszarze wywiadu.

- Ustalenia FRA pozwalają stwierdzić, że w porównaniu z innymi działaniami w zakresie przetwarzania danych i administratorami danych w sektorze publicznym i prywatnym, organy ochrony prywatności i danych w siedmiu państwach członkowskich posiadają takie same uprawnienia względem służb wywiadowczych, jak względem wszelkich innych administratorów danych. W 12 państwach członkowskich organy ochrony prywatności i danych nie posiadają kompetencji względem służb wywiadowczych, a w dziewięciu uprawnienia te są ograniczone.
- W państwach członkowskich, w których zastosowanie mają dzielone kompetencje organów ochrony prywatności i danych i innych organów nadzoru eksperckiego, brak współpracy pomiędzy tymi organami może skutkować powstawaniem luk z uwagi na fragmentaryczny charakter odpowiedzialności. W państwach członkowskich, w których organy ochrony prywatności i danych nie posiadają uprawnień w stosunku do służb wywiadowczych, organ nadzoru odpowiada za właściwe zastosowanie środków służących ochronie prywatności i danych.
- Poprzednie badania FRA w dziedzinie dostępu do środków prawnych w zakresie ochrony prywatności i danych wskazują na konieczność zwiększenia kompetencji organów ochrony prywatności i danych; jest to istotne z uwagi na rolę, jaką organy ochrony danych mogłyby odegrać w kontekście nadzoru nad służbami wywiadowczymi.

Środki odwoławcze

Zgodnie z obowiązującymi standardami międzynarodowymi każdy, kto podejrzewa, że padł ofiarą naruszenia prawa do ochrony prywatności lub danych musi mieć możliwość dochodzenia swoich roszczeń. Prawo do skutecznego środka odwoławczego, umożliwiające jednostkom uzyskanie zadośćuczynienia z tytułu naruszenia ich praw, jest istotnym elementem dostępu do wymiaru sprawiedliwości. Środek odwoławczy musi być „skuteczny” zarówno w praktyce, jak i według prawa.

Jak wykazano w poprzednich sprawozdaniach FRA dotyczących dostępu do środków prawnych w zakresie ochrony danych osobowych oraz dostępu do wymiaru sprawiedliwości, ofiary naruszeń praw do ochrony prywatności i danych mają do dyspozycji szereg środków prawnych. Zważywszy na praktyczne trudności w dostępie do sądów powszechnych, organy pozasądowe odgrywają istotną rolę naprawczą w dziedzinie inwigilacji. W 28 państwach członkowskich UE, organy pozasądowe obejmują organy eksperckie (w tym organy ochrony danych), wykonawcze i parlamentarne, a także instytucje rzecznika praw obywatelskich. W niektórych państwach członkowskich liczba organów pozasądowych, którym powierzono role organów odwoławczych w obszarze inwigilacji, może budzić entuzjazm, jednak należy wziąć pod uwagę następujące ustalenia.

Złożony charakter różnych środków prawnych nie ułatwia stosowania skutecznych środków odwoławczych, tak samo, jak nie ułatwia tego zadania ilość danych gromadzonych przez służby wywiadowcze prowadzące SIGINT. Fragmentaryczny charakter i rozwarstwienie różnych ścieżek odwoławczych sprawia, że dochodzenie roszczeń jest utrudnione. W rzeczywistości, zgromadzone dane wskazują, że od czasu doniesień Snowdena jedynie ograniczona liczba spraw mających za przedmiot zaskarżenie praktyk inwigilacji była rozstrzygana na szczeblu krajowym.

Obowiązek informowania i prawo dostępu

Prawo do otrzymania zawiadomienia i dostępu do informacji jest kluczowe w celu ostrzeżenia jednostek o stosowaniu środków inwigilacji i wszczęcia postępowania naprawczego. Europejski Trybunał Praw Człowieka (ETPC) przyjął jednak, że wspomniane prawa mogą zostać zasadnie ograniczone (zob. wyrok ETPC, *Klass i in. p. Niemcom*, nr 5029/71,

6 września 1978 r.). Zgodnie z ustaleniami FRA poufność związana z pracą służb wywiadowczych w rzeczy samej ogranicza te prawa. Innym czynnikiem jest już sama ilość danych zgromadzonych za pośrednictwem SIGINT w porównaniu z bardziej tradycyjnymi formami inwigilacji.

- W ośmiu państwach członkowskich przepisy prawa w ogóle nie regulują obowiązku informowania i prawa dostępu, a zastosowanie mają zasady dotyczące dokumentów niejawnych lub tajemnic państwowych. W pozostałych 20 państwach członkowskich ustawodawstwo przewiduje obowiązek informowania i prawo dostępu, w niektórych przypadkach w określonych ramach czasowych, z kilkoma jednak ograniczeniami. Wspomniane ograniczenia opierają się na rozmaitych przesłankach, takich jak względy bezpieczeństwa narodowego, interesy narodowe lub cel samego środka nadzoru.
- Jedynie w dwóch państwach członkowskich ustanowiono konkretne przepisy dotyczące obowiązku informowania w kontekście wywiadu sygnałowy: w jednym z nich jednostki nie są informowane, jeżeli zastosowane selektory nie odnoszą się bezpośrednio do nich; w drugim państwie jednostki nie informuje się, jeżeli pozyskane dane osobowe są usuwane natychmiast po ich zebraniu i nie podlegają dalszemu przetwarzaniu.
- Organy nadzoru w 10 państwach członkowskich, w tym sześć organów ochrony prywatności i danych, dokonują oceny ograniczeń w zakresie prawa do otrzymania zawiadomienia i prawa dostępu do informacji weryfikując, czy powołane zagrożenie dla bezpieczeństwa narodowego jest uzasadnione lub pośrednio wykonując prawo dostępu przysługujące jednostce. W ostatnim z wymienionych przypadków organy dokonują oceny, czy możliwe jest uzyskanie dostępu do danych lub czy odmowa dostępu jest zasadna, kontrolując także zgodność z prawem przetwarzania danych. W jednym państwie członkowskim wymagane jest orzeczenie sądu poświadczające, że zawiadomienie utrudniłoby śledztwo lub że istnieją inne argumenty przeciwko takiemu rozwiązaniu.
- W dwóch innych państwach członkowskich nie przyznaje się prawa dostępu do informacji jako takiego. Ustawodawca przewidział jednak prawo, które rodzi taki sam skutek: każdy może zwrócić się do organu nadzoru o sprawdzenie, czy jego dane są przedmiotem nieprawidłowej inwigilacji.

- W niektórych państwach członkowskich organ nadzoru zaangażowany w pośrednie wykonywanie przysługującego jednostce prawa do żądania dostępu do danych nie potwierdza, ani nie zaprzecza, że doszło do przetwarzania danych. Odpowiedzi ograniczają się zwykle do stwierdzenia, że skarga została rozpatrzona lub sprawdzona.

Sądowe środki odwoławcze

Każde państwo członkowskie zapewnia możliwość złożenia skargi do sądu na naruszenie prywatności, niezależnie od tego, czy rzezone naruszenia zaistniały w wyniku wywiadu ukierunkowanego lub wywiadu sygnałowy. Sądowej kontroli podlegają także decyzje organu nadzoru w sprawie skarg na naruszenie prywatności. W sądach ponadto można dochodzić roszczeń, także wynikających ze stosowania inwigilacji.

- Wcześniejsze badania FRA wykazały jednak, że brak sędziów wyspecjalizowanych w dziedzinie ochrony danych stanowi poważną przeszkodę dla skutecznego dochodzenia roszczeń z tytułu naruszeń prawa do ochrony danych. Wniosek ten ma istotne znaczenie w kontekście inwigilacji, gdzie oprócz koniecznej poufności związanej z działalnością wywiadowczą niezbędne jest posiadanie odpowiedniej wiedzy fachowej na przykład w dziedzinie ICT lub wywiadu.
- Jedynie w dwóch państwach członkowskich ograniczono ryzyko związane z brakiem specjalizacji poprzez zaangażowanie sędziów dysponujących zarówno wiedzą niezbędną do orzekania w kwestiach (często) natury technicznej i upoważnionych do uzyskania dostępu do materiałów poufnych.

Pozasądowe środki odwoławcze

Możliwości pozasądowe charakteryzują się zwykle większą dostępnością niż mechanizmy sądowe, z uwagi na mniej restrykcyjne przepisy proceduralne, niższe koszty i szybszy bieg postępowania. Wynika to między innymi z wcześniejszych ustaleń FRA, szczególnie w kontekście ochrony danych, gdyż zasadniczo więcej skarg kierowanych jest do krajowych organów ochrony prywatności i danych, a niewielu skarżących wybiera drogę postępowania sądowego. Liczba organów pozasądowych, innych niż organy ochrony prywatności i danych, mających działać w obszarze ochrony danych jest jednak niewielka, a wiele organów pozasądowych dysponuje jedynie ograniczonymi uprawnieniami w zakresie środków odwoławczych.

- Organy nadzoru (w tym organy ochrony prywatności i danych) odpowiedzialne za rozpatrywanie skarg w znacznej większości państw członkowskich mają status niezależnych instytucji.
- W przypadku gdy wykonawczy organ nadzoru posiada uprawnienia naprawcze, kwestia niezależności pojawia się w sytuacji, gdy oprócz tego ma on także prawo do zatwierdzenia inwigilacji. Parlamentarne i eksperckie organy nadzoru charakteryzuje większa autonomia pod względem struktury administracyjnej, jednak autonomia nie stanowi gwarancji skutecznego środka odwoławczego, chyba że poparta jest wystarczającą wiedzą. Przy ocenie niezależności organu istotnym aspektem, który należy rozważyć, jest także sposób powoływania członków tych organów oraz ich umiejscowienie w hierarchii administracyjnej.
- Organy ochrony prywatności i danych w 13 państwach członkowskich UE posiadają uprawnienia do badania indywidualnych skarg i wydawania wiążących decyzji. Jednak w trzech spośród tych państw uprawnienie do dostępu do akt i do prowadzenia przeszukań jest ograniczone. Dodatkowo, w pięciu państwach członkowskich, podczas prowadzenia kontroli w siedzibie służb wywiadowczych wymagana jest obecność szefa lub członka organu ochrony.
- Pięć z siedmiu państw członkowskich, które przyznają swoim eksperckim organom nadzoru (innym niż organy ochrony prywatności i danych) szczególne uprawnienia naprawcze, czyni to poprzez zezwolenie na wydawanie wiążących decyzji przez te organy. W dwóch państwach członkowskich organ nadzoru wykonawczego dysponuje także uprawnieniami naprawczymi. Komisje parlamentarne w czterech państwach członkowskich są upoważnione do rozpatrywania indywidualnych skarg, ale tylko jedna może je rozstrzygać w drodze wiążących decyzji.
- Instytucje rzecznika praw obywatelskich istniejące we wszystkich 28 państwach członkowskich UE zajmują się głównie nieprawidłowościami natury administracyjnej, a nie samym meritem inwigilacji. Przepisy dotyczące działalności wywiadowczej obowiązujące tylko w jednym państwie członkowskim przyznają rzecznikowi praw obywatelskich uprawnienia naprawcze.. Ponadto uprawnienia instytucji rzecznika praw obywatelskich mogą być dość ograniczone, a postępowanie zwykle kończy się wydaniem niewiążących zaleceń, mających na celu uregulowanie podniesionych kwestii oraz określających przyszłe działania, a nie wydaniem wiążącego i wykonalnego wyroku. To przekłada się oczywiście na skuteczność środków odwoławczych, jakie są one w stanie zapewnić.
- Inne elementy, które mogą ułatwiać dostęp do środków odwoławczych, to między innymi mniej restrykcyjne przepisy dotyczące ciężaru dowodu i powództw zbiorowych, a także skuteczna ochrona osób zgłaszających przypadki naruszeń (ang. whistleblowers). Zgromadzenie Parlamentarne Rady Europy uważa, że sygnalizowanie nieprawidłowości stanowi najskuteczniejsze narzędzie służące egzekwowaniu ograniczeń w zakresie inwigilacji.



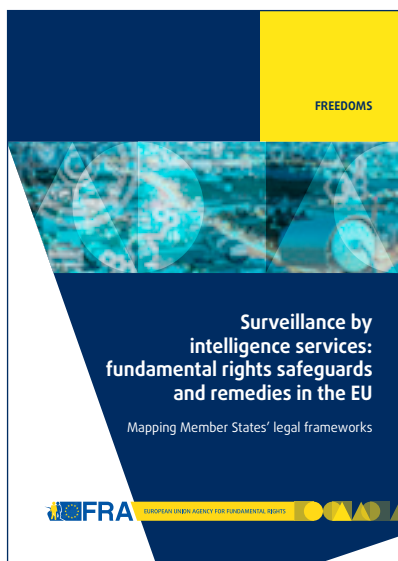
Wnioski

Podjmując kwestie związane z obszarem ograniczonych kompetencji UE, w sprawozdaniu zwrócono uwagę na różnice występujące pomiędzy państwami członkowskimi dotyczące struktury organizacyjnej służb wywiadowczych i wykonywania przez te służby swoich podstawowych obowiązków.

Środki inwigilacji w ogromnym stopniu naruszają prawa jednostek. Z uwagi na poufny charakter tych środków, od jednostek oczekuje się określonego poziomu zaufania do organów publicznych, których zadaniem z kolei, jest ochrona praw podstawowych. Osiągnięcie poziomu zaufania społecznego do służb wywiadowczych wymaga ustalenia jasnych reguł ich odpowiedzialności za pewne działania. Zrozumiałe i przystępne przepisy, silne mechanizmy nadzoru, odpowiednie mechanizmy kontroli i skuteczne środki odwoławcze to jedynie niektóre elementy niezbędne do osiągnięcia tego rodzaju rozliczalności, co niewątpliwie jest rzeczą trudną, biorąc pod uwagę poufność, jaka charakteryzuje środowisko pracy służb wywiadowczych. Wprowadzenie i utrzymanie zrozumiałych i przystępnych mechanizmów nadzoru na szczeblu państwa członkowskiego to jedynie pierwszy krok na drodze ku

przejrzystemu i zgodnemu z prawami podstawowymi systemu – trudności w tym zakresie wskazują na przeszkody, które jeszcze należy pokonać.

Reakcje na doniesienia Snowdena zwróciły uwagę na konieczność dostosowania i wzmocnienia odpowiednich ram prawnych w UE i we wszystkich państwach członkowskich. Badanie FRA pokazuje, że szereg reform prawnych już przeprowadzono. Okresowe kontrole funkcjonowania i zasadność przepisów regulujących działalność służb wywiadowczych muszą stać się integralną częścią systemów nadzoru. Kluczowe jest także pytanie o to, w jaki sposób przeprowadzać dalsze reformy ram prawnych, aby zaradzić sytuacji braku odpowiedniego nadzoru. Ponadto reformy w państwach członkowskich UE muszą uwzględniać najnowsze osiągnięcia technologiczne, w celu zapewnienia, że mechanizmy nadzoru są wyposażone w niezbędne narzędzia i podparte wiedzą fachową. Realizacja wszystkich tych założeń jest niewątpliwie przedsięwzięciem trudnym, ale niezbędnym dla wykonania zadania, jakim jest ochrona bezpieczeństwa przy jednoczesnej gwarancji przestrzegania praw podstawowych.



Ochrona społeczeństwa przed zagrożeniami bezpieczeństwa i zagwarantowanie przestrzegania praw podstawowych to działanie wymagające zachowania delikatnej równowagi. Sprawę jeszcze bardziej komplikują brutalne ataki terrorystyczne i innowacje w dziedzinie technologii umożliwiające zakrojone na szeroką skalę monitorowanie danych komunikacyjnych, wzbudzające obawy o naruszenia praw do prywatności i ochrony danych popełniane w imię ochrony bezpieczeństwa narodowego. W wyniku doniesień Snowdena, które ujawniły rozległe i prowadzone na całym świecie masowe działania inwigilacyjne, stało się jasne, że niezbędne jest wprowadzenie wzmocnionych środków na rzecz ochrony tych praw.

Niniejsze sprawozdanie, sporządzone w odpowiedzi na wezwanie ze strony Parlamentu Europejskiego do przeprowadzenia szczegółowego badania kwestii ochrony praw podstawowych w kontekście inwigilacji, wskazuje i analizuje ramy prawne regulujące kwestie inwigilacji w państwach członkowskich UE. Koncentrując się na problemie tzw. „masowej inwigilacji”, szczegółowo opisuje ono mechanizmy nadzoru wprowadzone w całej UE, przedstawiając działalność podmiotów, których zadaniem jest kontrola działań w zakresie inwigilacji. W sprawozdaniu zaprezentowano także wachlarz środków odwoławczych dostępnych w celu zaskarżenia tego rodzaju działalności wywiadowczej. Poprzez ukazanie skomplikowanych kwestii, jakie składają się na ten problem, w niniejszym sprawozdaniu podkreślono potencjalną trudność rozwiązania problemów postrzeganych często jako sprzeczne priorytety, oferując tym samym ważny głos w debacie na temat najlepszych sposobów na pogodzenie tych interesów.

Dalsze informacje:

Pełna wersja sprawozdania FRA *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Mapping Member States’ legal frameworks* (Inwigilacja prowadzona przez służby wywiadowcze: środki zabezpieczające prawa podstawowe oraz środki prawne dostępne w Unii Europejskiej – analiza ram prawnych w państwach członkowskich) znajduje się na stronie internetowej <http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services>

Zobacz także publikacje FRA w tej dziedzinie:

- FRA-Rada Europy (2014), *Podręcznik europejskiego prawa o ochronie danych*, Luksemburg, Urząd Publikacji, <http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-pl.pdf> (dostępny w różnych językach)
- FRA (2014), *Access to data protection remedies in EU Member States* (Dostęp do środków prawnych w zakresie ochrony danych w państwach członkowskich UE), Luksemburg, Urząd Publikacji, <http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states> oraz streszczenie sprawozdania http://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies-summary_pl.pdf (dostępne w różnych językach)

Przegląd działalności FRA w dziedzinie ochrony danych znajduje się na stronach internetowych: <http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection>



© Agencja Praw Podstawowych Unii Europejskiej, 2015
Zdjęcia: © Shutterstock

FRA – AGENCJA PRAW PODSTAWOWYCH UNII EUROPEJSKIEJ

Schwarzenbergplatz 11 – 1040 Wiedeń – Austria
Tel.: +43 158030-0 – Faks: +43 158030-699
fra.europa.eu – info@fra.europa.eu
[facebook.com/fundamentalrights](https://www.facebook.com/fundamentalrights)
[linkedin.com/company/eu-fundamental-rights-agency](https://www.linkedin.com/company/eu-fundamental-rights-agency)
twitter.com/EURightsAgency



Print: ISBN 978-92-9491-008-0, doi:10.2811/983297
PDF: ISBN 978-92-9491-009-7, doi:10.2811/10719