**RADA UNII EUROPEJSKIEJ**

**Bruksela, 19 kwietnia 2011 r. (02.05)**
**(OR. en)**

**9324/11**

**DAPIX 38**
**TELECOM 47**
**COPEN 85**

**PISMO PRZEWODNIE**

| | |
|---|---|
| Od: | Sekretarz Generalny Komisji Europejskiej, podpisał dyrektor Jordi AYET PUIGARNAU |
| Data otrzymania: | 18 kwietnia 2011 r. |
| Do: | Pierre de BOISSIEU, Sekretarz Generalny Rady Unii Europejskiej |
| Nr dok. Kom.: | COM(2011) 225 wersja ostateczna |
| Dotyczy: | Sprawozdanie Komisji dla Rady i Parlamentu Europejskiego. Sprawozdanie z oceny dyrektywy w sprawie zatrzymywania danych (dyrektywa 2006/24/WE) |

Delegacje otrzymują w załączeniu dokument Komisji COM(2011) 225 wersja ostateczna.

Zał.: COM(2011) 225 wersja ostateczna

KOMISJA EUROPEJSKA

Bruksela, dnia 18.4.2011
KOM(2011) 225 wersja ostateczna

# SPRAWOZDANIE KOMISJI DLA RADY I PARLAMENTU EUROPEJSKIEGO

## Sprawozdanie z oceny dyrektywy w sprawie zatrzymywania danych (dyrektywa 2006/24/WE)

**SPRAWOZDANIE KOMISJI DLA RADY I PARLAMENTU EUROPEJSKIEGO**

**Sprawozdanie z oceny dyrektywy w sprawie zatrzymywania danych (dyrektywa 2006/24/WE)**

## 1. WPROWADZENIE

Na podstawie dyrektywy w sprawie zatrzymywania danych[1] (dalej zwanej „dyrektywą") państwa członkowskie zobowiązane są do nałożenia na dostawców ogólnie dostępnych usług łączności elektronicznej lub publicznych sieci łączności (dalej zwanych „operatorami") obowiązku zatrzymywania danych o ruchu i lokalizacji przez okres od sześciu miesięcy do dwóch lat w celu prowadzenia dochodzeń w sprawie poważnych przestępstw, ich wykrywania i ścigania .

Niniejsze sprawozdanie Komisji zawiera, dokonaną na podstawie art. 14 dyrektywy, ocenę stosowania dyrektywy przez państwa członkowskie oraz jej wpływu na podmioty gospodarcze i konsumentów, z uwzględnieniem rozwoju technologii łączności elektronicznej oraz udostępnionych Komisji danych statystycznych. Celem sprawozdania jest określenie ewentualnej potrzeby zmodyfikowania przepisów dyrektywy, zwłaszcza w odniesieniu do zakresu danych oraz okresów zatrzymywania. W niniejszym sprawozdaniu dodatkowo oceniono wpływ dyrektywy na prawa podstawowe ze względu na krytykę zatrzymywania danych w ogóle, a także rozważono, czy ze względu na obawy związane ze stosowaniem anonimowych kart SIM w celach przestępczych istnieje konieczność wprowadzenia odpowiednich środków[2].

Ogólnie rzecz biorąc przeprowadzona ocena dowodzi, że zatrzymywanie danych jest cennym narzędziem dla systemów wymiaru sprawiedliwości w sprawach karnych oraz organów ścigania w UE. Wpływ dyrektywy na harmonizację zatrzymywania danych był w niektórych dziedzinach ograniczony, np. w zakresie zasady celowości i okresów zatrzymywania, a także w dziedzinie zwrotu wydatków poniesionych przez operatorów, która to kwestia pozostaje poza zakresem dyrektywy. Biorąc pod uwagę oddziaływanie na rynek wewnętrzny oraz ewentualne zagrożenia dla tego rynku oraz dla poszanowania prawa do prywatności i ochrony danych osobowych, UE powinna w dalszym ciągu zapewniać – za pośrednictwem wspólnych przepisów – utrzymywanie wysokich standardów w zakresie przechowywania, pobierania i wykorzystania danych o ruchu i lokalizacji. W świetle powyższych konkluzji i w oparciu o ocenę skutków Komisja zamierza zaproponować wprowadzenie zmian do dyrektywy.

---

[1] Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE, Dz.U. L 105 z 13.4.2006, s. 54-63.

[2] Konkluzje Rady w sprawie walki z wykorzystywaniem do celów przestępczych łączności elektronicznej i jej anonimowości, 2908. posiedzenie Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych, Bruksela, 27-28 listopada 2008 r.

## 2. KONTEKST NINIEJSZEJ OCENY

Niniejsze sprawozdanie z oceny zostało poprzedzone obszernymi dyskusjami z przedstawicielami państw członkowskich, ekspertami i zainteresowanymi stronami i sporządzono je w oparciu o uzyskane od nich informacje.

W maju 2009 r. Komisja zorganizowała konferencję zatytułowaną „W kierunku oceny dyrektywy o zatrzymywaniu danych", w której uczestniczyli przedstawiciele organów ds. ochrony danych, przedstawiciele sektora prywatnego, środowiska akademickiego oraz społeczeństwa obywatelskiego. We wrześniu 2009 r. Komisja przesłała do zainteresowanych stron reprezentujących powyższe grupy kwestionariusz, na który otrzymała około 70 odpowiedzi[3]. W grudniu 2010 r. Komisja zorganizowała drugą konferencję dotyczącą dyrektywy w sprawie zatrzymywania danych, w której wzięła udział podobna grupa zainteresowanych stron i podczas której wymieniono się wstępnymi ocenami dyrektywy oraz przedyskutowano przyszłe wyzwania w tym obszarze.

W okresie od października 2009 do marca 2010 r. Komisja spotkała się z przedstawicielami wszystkich państw członkowskich oraz stowarzyszonych państw EOG w celu bardziej szczegółowego omówienia kwestii dotyczących stosowania dyrektywy. Państwa członkowskie rozpoczęły stosowanie dyrektywy później niż przewidywano, szczególnie w odniesieniu do danych związanych z Internetem. Opóźnienia w transpozycji oznaczały, że dziewięć państw członkowskich zdołało dostarczyć Komisji pełne statystyki wymagane na podstawie art. 10 dyrektywy (za lata 2008 lub 2009), zaś 19 państw członkowskich dostarczyło jakieś statystyki (zob. pkt. 4.7). W lipcu 2010 r. Komisja zwróciła się do państw członkowskich z prośbą o przekazanie dalszych ilościowych i jakościowych informacji dotyczących konieczności zatrzymywania danych w celu uzyskiwania rezultatów w egzekwowania prawa. W odpowiedzi dziesięć państw członkowskich podało szczegółowe informacje o konkretnych przypadkach, w których dane okazały się konieczne[4].

Niniejsze sprawozdanie opiera się na dokumentach prezentujących stanowiska, przyjętych od jej ustanowienia w 2008 r. przez „Platformę ds. zatrzymywania danych elektronicznych w celu dochodzenia, wykrywania i ścigania poważnych przestępstw"[5]. Komisja uwzględniła sprawozdania Grupy Roboczej ds. Ochrony Osób Fizycznych powołanej na mocy art. 29[6], w szczególności sprawozdanie na temat drugiego etapu egzekwowania, tzn. oceny

---

3 Odpowiedzi zostały opublikowane na stronach internetowych Komisji (http://ec.europa.eu/home-affairs/news/consulting_public/consulting_0008_en.htm_

4 Belgia, Cypr, Litwa, Niderlandy, Polska, Republika Czeska, Słowenia, Węgry, Zjednoczone Królestwo. Szwecja zgłosiła także szereg przypadków szczególnie poważnych przestępstw, w których historyczne dane o ruchu, dostępne mimo braku obowiązku zatrzymywania danych, miały kluczowe znaczenie dla uzyskania wyroków skazujących.

5 Ta grupa ekspertów została utworzona na podstawie decyzji Komisji nr 2008/324/WE, Dz.U. L 111 z 23.4.2008, s. 11-14. Komisja odbywała regularne spotkania z grupą. Dokumenty określające jej stanowisko publikowane są na stronie: http://ec.europa.eu/justice_home/doc_centre/police/doc_police_intro_en.htm

6 Grupa robocza ds. ochrony osób fizycznych w odniesieniu do przetwarzania danych osobowych została ustanowiona na mocy art. 29 dyrektywy o ochronie danych (dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz.U. L 281 z 23.11.1995, s. 31).

przestrzegania przez państwa członkowskie zawartych w dyrektywie wymogów dotyczących ochrony oraz bezpieczeństwa danych[7].

## 3. ZATRZYMYWANIE DANYCH W UNII EUROPEJSKIEJ

### 3.1. Zatrzymywanie danych do celów wymiaru sprawiedliwości w sprawach karnych oraz egzekwowania prawa

Dostawcy usług i sieci (zwani dalej „operatorami") przetwarzają w ramach swojej działalności dane osobowe w celu przekazywania połączeń, naliczania opłat i rozliczeń międzyoperatorskich, w celach marketingowych oraz w związku z wykonywaniem niektórych innych usług o wartości dodanej. Takie przetwarzanie dotyczy danych wskazujących na źródło, odbiorcę, datę, godzinę, czas trwania i rodzaj połączenia, a także na urządzenie komunikacji użytkownika oraz – w przypadku telefonii komórkowej – na lokalizację urządzenia. Na mocy dyrektywy 2002/58/WE dotyczącej prywatności w sektorze łączności elektronicznej (zwanej dalej dyrektywą w sprawie e-prywatności)[8] takie dane o ruchu wygenerowane przy korzystaniu z usług łączności elektronicznej muszą zasadniczo zostać usunięte lub uczynione anonimowymi, gdy nie są już potrzebne do celów przekazywania połączenia, z wyjątkiem sytuacji gdy są niezbędne (i tylko tak długo jak są niezbędne) do celów naliczania opłat abonenta lub gdy uzyskano zgodę abonenta lub użytkownika. Dane o lokalizacji mogą być przetwarzane wyłącznie wtedy, gdy zostały zanonimizowane lub za zgodą danego użytkownika, w zakresie i przez okres niezbędny do świadczenia usług stanowiących wartość dodaną.

Przed wejściem w życie dyrektywy i przy spełnieniu szczególnych warunków krajowe organy zwracały się z wnioskiem do operatorów o dostęp do tych danych w celu na przykład zidentyfikowania abonentów korzystających z adresu protokołu komunikacyjnego (IP), w celu zbadania wcześniejszych połączeń oraz ustalenia lokalizacji telefonu komórkowego.

Pierwszą próbę uregulowania na szczeblu UE kwestii zatrzymywania i wykorzystywania danych w celu egzekwowania prawa stanowiła dyrektywa 97/66/WE dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze telekomunikacyjnym. Dyrektywa ta po raz pierwszy wprowadziła możliwość przyjęcia przez państwa członkowskie stosownych środków legislacyjnych, jeżeli jest to konieczne z punktu widzenia ochrony bezpieczeństwa publicznego, obronności lub porządku publicznego, w tym dobrej kondycji gospodarczej

---

[7] Sprawozdanie 01/2010 w sprawie drugiego wspólnego działania w zakresie egzekwowania prawa: stopień zachowania zgodności przez dostawców usług telekomunikacyjnych i internetowych z wymogami wypływającymi z krajowych przepisów dotyczących zatrzymywania danych o ruchu w oparciu o podstawę prawną zawartą w art. 6 i 9 dyrektywy o prywatności i łączności elektronicznej 2002/58/WE i dyrektywy w sprawie zatrzymywania danych 2006/24/WE zmieniającą dyrektywę o prywatności i łączności elektronicznej (WP 172) z 13.7.2010 r., dostępne pod adresem: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm.

[8] Dyrektywa Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), (Dz.U. L 201 z 31.7.2002, s. 37-47).

państwa, gdy dana działalność wiązała się z kwestiami dotyczącymi bezpieczeństwa państwa oraz egzekwowaniem prawa karnego[9].

Przepis ten został dalej rozwinięty w dyrektywie w sprawie e-prywatności, która przewiduje możliwość przyjęcia przez państwa członkowskie środków legislacyjnych wprowadzających odstępstwa od zasady poufności komunikacji, obejmujących, pod pewnymi warunkami, zatrzymywanie danych, dostęp i korzystanie z danych do celów egzekwowania prawa. Na podstawie art. 15 ust. 1 państwa członkowskie mogą ograniczać prawo do prywatności oraz związane z nią obowiązki, w tym poprzez zatrzymywanie danych przez określony czas, jeżeli jest to „niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego (tzn. bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej".

Znaczenie zatrzymywanych danych dla wymiaru sprawiedliwości w sprawach karnych oraz dla egzekwowania prawa zostało bliżej omówione w sekcji 5.

### 3.2. Cel i podstawa prawna dyrektywy w sprawie zatrzymywania danych

W wyniku wejścia w życie dyrektywy 97/66/WE i dyrektywy w sprawie e-prywatności, które umożliwiają państwom członkowskim przyjęcie przepisów o zatrzymywaniu danych, operatorzy w niektórych państwach członkowskich zostali zobowiązani do nabywania urządzeń do zatrzymywania danych oraz zatrudniania pracowników zajmujących się pobieraniem danych w imieniu organów ścigania, podczas gdy operatorzy w innych państwach członkowskich nie mieli takiego obowiązku, co doprowadziło do zakłóceń na rynku wewnętrznym. Ponadto tendencje w modelach biznesowych i ofertach usług, takie jak rozwój taryf zryczałtowanych, usług typu *pre-paid* oraz darmowych usług łączności elektronicznej oznaczały, że operatorzy stopniowo przestali przechowywać dane o ruchu oraz dane o lokalizacji dla potrzeb naliczania opłat, ograniczając tym samym dostępność takich danych dla potrzeb wymiaru sprawiedliwości w sprawach karnych i egzekwowania prawa. Ataki terrorystyczne w Madrycie w 2004 r. oraz w Londynie w 2005 r. na nowo ożywiły dyskusje na szczeblu UE w sprawie sposobu rozwiązania tych kwestii.

W odpowiedzi na te problemy w dyrektywie o zatrzymywaniu danych nałożono na państwa członkowskie obowiązek dopilnowania, by dostawcy ogólnie dostępnych usług łączności elektronicznej oraz publicznych sieci łączności zatrzymywali dane o łączności na potrzeby wykrywania poważnych przestępstw, prowadzenia dochodzeń w ich sprawie i ich ścigania, zgodnie z definicjami przyjętymi przez każde państwo członkowskie w prawie krajowym. Jej celem była harmonizacja pewnych powiązanych aspektów w całej UE.

Dyrektywa zmieniła art.15 ust.1 dyrektywy o prywatności i łączności elektronicznej, wprowadzając ustęp stanowiący, że art. 15 ust. 1 nie ma zastosowania do danych

---

[9] Artykuł 14 ust. 1 dyrektywy 97/66/WE Parlamentu Europejskiego i Rady z dnia 15 grudnia 1997 r. w sprawie przetwarzania danych osobowych oraz ochrony prywatnych danych w sektorze telekomunikacyjnym (Dz.U. L 24 z 30.1.1998, s. 1-8).

zatrzymanych na podstawie dyrektywy w sprawie zatrzymywania danych[10]. Dlatego państwa członkowskie (zgodnie z treścią motywu 12 dyrektywy) mają nadal możliwość dokonywania odstępstw od przestrzegania zasady poufności komunikacji. Dyrektywa (w sprawie zatrzymywania danych) reguluje jedynie zatrzymywanie danych w bardziej ograniczonym celu: prowadzenia dochodzeń w sprawie poważnych przestępstw, wykrywania ich i ścigania.

Ten złożony stosunek prawny między dyrektywą a dyrektywą o prywatności i łączności elektronicznej, a także fakt, że w żadnej z dyrektyw nie zdefiniowano pojęcia „poważnego przestępstwa", utrudnia rozróżnienie między środkami podejmowanymi przez państwa członkowskie w celu transponowania określonych w dyrektywie wymogów związanych z zatrzymywaniem danych z jednej strony, a bardziej ogólnymi praktykami zatrzymywania danych, stosowanymi w państwach członkowskich, na które zezwala art. 15 ust. 1 dyrektywy o prywatności i łączności elektronicznej[11]. Kwestie te przedstawiono dokładniej w rozdziale 4.

Dyrektywa opiera się na art. 95 Traktatu ustanawiającego Wspólnotę Europejską (zastąpionym art. 114 Traktatu o funkcjonowaniu Unii Europejskiej), dotyczącym ustanowienia i funkcjonowania rynku wewnętrznego. Po przyjęciu dyrektywy zakwestionowano jej podstawę prawną przed Trybunałem Sprawiedliwości Unii Europejskiej ze względu na to, że jej celem nadrzędnym jest prowadzenie dochodzeń w sprawie poważnych przestępstw. Zdaniem Trybunału dyrektywa reguluje działania, które są niezależne od realizacji jakiejkolwiek policyjnej lub sądowej współpracy w sprawach karnych, i nie prowadzi do harmonizacji dostępu właściwych krajowych organów ścigania do danych, ani do ich wykorzystywania i wymiany przez te organy. Trybunał doszedł zatem do wniosku, że dyrektywa obejmuje przede wszystkim działania operatorów w danym sektorze rynku wewnętrznego. W oparciu o to uznał on podstawę prawną za prawidłową[12].

### 3.3. Zachowywanie danych

Zatrzymywanie danych różni się od zachowywania danych (zwanego również „szybkim zamrożeniem"); w przypadku tego ostatniego na mocy nakazu sądowego operatorzy mają obowiązek, począwszy od dnia wystawienia nakazu, zachowywania danych dotyczących jedynie konkretnych osób fizycznych, które podejrzewane są o działalność przestępczą. Zachowywanie danych to jedno z narzędzi dochodzeniowych, które przewidziano w Konwencji Rady Europy z 2001 r. o cyberprzestępczości[13], i które wykorzystywane jest przez

---

10 Artykuł 11 dyrektywy stanowi: „W art. 15 dyrektywy 2002/58/WE dodaje się ustęp w następującym brzmieniu: „1a. Ustępu 1 nie stosuje się do danych, których zatrzymywanie jest wyraźnie wymagane na mocy dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania danych wygenerowanych lub przetworzonych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności zatrzymywanych dla celów określonych w art. 1 ust. 1 tej dyrektywy".

11 Grupa Robocza powołana na podstawie art. 29 podała w wątpliwość, czy celem dyrektywy w sprawie ochrony danych było odstępowanie od ogólnego wymogu usuwania danych o ruchu w momencie zakończenia komunikacji elektronicznej, czy też raczej uprawnienie do zatrzymywania wszystkich danych, do przetrzymywania których usługodawcy zostali uprawnieni w celu realizowania swoich celów handlowych."

12 TS, C-301/6 Irlandia przeciwko Parlamentowi i Radzie, Zb.Orz. [2009] I-00593.

13 Artykuł 16 Konwencji o cyberprzestępczości (http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm) .

uczestniczące w niej państwa. Niemal wszystkie uczestniczące w niej państwa stworzyły punkty kontaktowe, których zadaniem jest zapewnienie natychmiastowej pomocy w dochodzeniach lub postępowaniach dotyczących cyberprzestępczości. Jednak wydaje się, że jeszcze nie wszystkie strony Konwencji zapewniły zachowywanie danych i nie dokonano jeszcze oceny, na ile powyższy model jest skuteczny w zwalczaniu cyberprzestępczości[14]. Niedawno opracowano nowy rodzaj zachowywania danych, znany jako „szybkie zamrożenie plus": wykracza on poza zachowywanie danych w tym sensie, że sędzia może przyznać także dostęp do danych, które nie zostały jeszcze usunięte przez operatorów. Podobnie istniałby bardzo ograniczony prawny wyjątek od obowiązku usuwania, przez krótki okres czasu, określonych danych komunikacyjnych, które normalnie nie są przechowywane, takich jak dane o lokalizacji i połączeniu internetowym oraz dynamicznych adresach IP użytkowników posiadających abonament ryczałtowy, w przypadku których nie ma potrzeby przechowywania danych do celów rozliczeniowych.

Zwolennicy zachowywania danych uważają, że stanowi ono mniejszą ingerencję w prawo do prywatności niż zatrzymywanie danych. Jednak większość państw członkowskich jest zdania, że różne rodzaje zachowywania danych nie mogą odpowiednio zastąpić zatrzymywania danych, argumentując, że podczas gdy zatrzymywanie danych prowadzi do uzyskania danych historycznych, zachowywanie danych nie gwarantuje możliwości ustalenia tropów dowodowych przed wydaniem nakazu zachowywania, nie umożliwia prowadzenia dochodzeń w przypadku gdy cel nie jest znany oraz nie umożliwia zebrania materiałów dowodowych dotyczących przemieszczania, np. pokrzywdzonych lub świadków przestępstwa[15].

## 4. TRANSPOZYCJA DYREKTYWY W SPRAWIE ZATRZYMYWANIA DANYCH

Państwa członkowskie zostały zobowiązane do transponowania dyrektywy przed dniem 15 września 2007 r., przy czym istniała możliwość przedłużenia do dnia 15 marca 2009 r. wdrożenia obowiązków związanych z zatrzymywaniem danych w odniesieniu do dostępu do Internetu, poczty elektronicznej oraz telefonii internetowej.

Poniższa analiza opiera się na zgłoszeniach dotyczących transpozycji otrzymanych przez Komisję od 25 państw członkowskich, w tym Belgii, która dokonała jedynie częściowej transpozycji[16]. W Austrii i Szwecji projekt przepisów jest nadal przedmiotem debaty. W tych dwóch państwach członkowskich nie istnieje wymóg zatrzymywania danych, jednak organy ścigania mogą złożyć wniosek do operatora o dostęp do danych o ruchu w zakresie, w jakim dane te są do dyspozycji, i z takiej możliwości korzystają. Po wstępnym zgłoszeniu transpozycji przez Republikę Czeską, Niemcy i Rumunię, sądy konstytucyjne tych państw

---

14 Źródło: Rada Europy.

15 Zostało to również uznane przez niemiecki Trybunał Konstytucyjny w wyroku uchylającym niemiecką ustawę transponującą dyrektywę (zob. pkt. 4.9 wyroku) (Bundesverfassungsgericht, 1 BvR 256/08 z 2 marca 2010 r., pkt 208).

16 Dwadzieścia pięć państw członkowskich, które zgłosiły Komisji transpozycję dyrektywy to Belgia, Bułgaria, Republika Czeska, Dania, Niemcy, Grecja, Estonia, Irlandia, Hiszpania, Francja, Włochy, Cypr, Łotwa, Litwa, Luksemburg, Węgry, Malta, Niderlandy, Polska, Portugalia, Rumunia, Słowenia, Słowacja, Finlandia, Zjednoczone Królestwo. Belgia poinformowała Komisję, że projekt przepisów, które zakończą proces transpozycji, jest nadal rozpatrywany w Parlamencie.

uchyliły krajowe przepisy transponujące dyrektywę[17]; obecnie państwa te rozważają zatem metody ponownej jej transpozycji.

W poniższej sekcji przeanalizowano, w jaki sposób państwa członkowskie dokonały transpozycji właściwych przepisów dyrektywy. Zbadano w nim również kwestię, czy państwa członkowskie zdecydowały o zwrocie operatorom kosztów powstałych w związku z zatrzymywaniem i umożliwianiem pobierania danych, czego nie reguluje dyrektywa, a także poruszono kwestię znaczenia wyroków trybunałów konstytucyjnych w Niemczech, Rumunii i Republice Czeskiej w kontekście dyrektywy.

### 4.1. Cel zatrzymywania danych (artykuł 1)

Dyrektywa zobowiązuje państwa członkowskie do przyjęcia środków mających zapewnić zatrzymywanie danych w celu prowadzenia dochodzenia w sprawie poważnych przestępstw oraz ich wykrywania i ścigania , zgodnie z definicjami przyjętymi przez każde państwo członkowskie w swoim prawie krajowym. Jednak cele zatrzymywania lub uzyskiwania dostępu do danych, określone w przepisach krajowych, są w UE w dalszym ciągu różne. Dziesięć państw członkowskich (Bułgaria, Estonia, Irlandia, Grecja, Hiszpania, Litwa, Luksemburg, Węgry, Niderlandy, Finlandia) zdefiniowało „poważne przestępstwo", odnosząc się do minimalnej kary pozbawienia wolności, możliwości nałożenia kary polegającej na pozbawieniu wolności lub wykazu przestępstw określonych w innych przepisach krajowych. Osiem państw członkowskich (Belgia, Dania, Francja, Włochy, Łotwa, Polska, Słowacja, Słowenia) wymaga, aby dane były zatrzymywane nie tylko w celu prowadzenia dochodzeń w sprawach poważnych przestępstw oraz ich wykrywania i karania, ale również odniesieniu do wszystkich przestępstw kryminalnych oraz w celu zapobiegania przestępstwom, lub – z ogólnych przyczyn bezpieczeństwa narodowego lub państwowego albo publicznego. Ustawodawstwo czterech państw członkowskich (Cypr, Malta, Portugalia, Zjednoczone Królestwo) odwołuje się do „poważnego czynu karalnego" lub „poważnego przestępstwa", nie definiując ich. Szczegóły zamieszczono w tabeli 1.

| **Tabela 1: Ograniczanie celu zatrzymywania danych określone w przepisach krajowych** | |
|---|---|
| Belgia | W celu prowadzenia dochodzeń w sprawie przestępstw i ich ścigania, ścigania nadużywania alarmowego numeru telefonicznego, prowadzenia dochodzeń w sprawie złośliwego nadużywania sieci lub usług łączności elektronicznej, do celów misji wywiadowczych podjętych przez organy wywiadu i bezpieczeństwa wewnętrznego[18]. |
| Bułgaria | Do celów „wykrywania poważnych przestępstw i innych przestępstw i prowadzenia dochodzeń w ich sprawie, na mocy art. 319a-319f kodeksu karnego, jak również w celu poszukiwania osób[19]. |
| Republika Czeska | Brak transpozycji. |

[17] Orzeczenie nr 1258 rumuńskiego Trybunału Konstytucyjnego z dnia 8 października 2009 r., rumuński dziennik urzędowy nr 789 z dnia 23 listopada 2009 r.; wyrok Bundesverfassungsgericht 1 BvR 256/08, z dnia 2 marca 2010 r.; dziennik urzędowy z dnia 1 kwietnia 2011 r., wyrok Trybunału Konstytucyjnego z dnia 22 marca w sprawie przepisów art. 97 ust. 3 i 4 ustawy nr 127/2005 Coll. w sprawie łączności elektronicznej, zmieniającej niektóre powiązane ustawy, oraz dekret nr 485/2005 w sprawie zatrzymywania danych i ich przekazywania właściwym organom.

[18] Artykuł 126 ust. 1 ustawy z dnia 2005 r. o łączności elektronicznej .

[19] Artykuł 250a ust. 2 ustawy o łączności elektronicznej (z późn. zm.) z 2010 r.

| Tabela 1: Ograniczanie celu zatrzymywania danych określone w przepisach krajowych | |
|---|---|
| Dania | Dla potrzeb prowadzenia dochodzeń w sprawie czynów przestępczych i ich ścigania [20]. |
| Niemcy | Brak transpozycji. |
| Estonia | Może być wykorzystane, jeżeli gromadzenie dowodów w ramach innych działań proceduralnych jest wyłączone lub szczególnie skomplikowane, zaś przedmiotem postępowania karnego jest przestępstwo kryminalne [pierwszego lub drugiego stopnia, za które grozi kara pozbawienia wolności na okres co najmniej trzech lat]"[21]. |
| Irlandia | Dla zapobiegania poważnym przestępstwom [tzn. przestępstwom, za które grozi kara pozbawienia wolności na okres co najmniej pięciu lat, lub przestępstwom wyszczególnionym w załączniku do ustawy transponującej], w celu zapewnienia bezpieczeństwa państwa oraz dla ochrony ludzkiego życia[22]. |
| Grecja | Do celów wykrywania szczególnie poważnych przestępstw[23]. |
| Hiszpania | Na potrzeby wykrywania, poważnych przestępstw, przewidzianych w kodeksie karnym lub w szczególnych ustawach karnych, prowadzenia dochodzeń w ich sprawie i ich ścigania "[24]. |
| Francja | Na potrzeby wykrywania, dochodzenia i ścigania przestępstw, a także dla realizacji wyłącznego celu w postaci udostępniania organom sądowym potrzebnych im informacji oraz zapobiegania aktom terrorystycznym i ochrony własności intelektualnej[25]. |
| Włochy | Na potrzeby wykrywania i zwalczania przestępstw[26]. |
| Cypr | Na potrzeby prowadzenia dochodzeń w sprawie poważnych przestępstw[27]. |
| Łotwa | W celu ochrony bezpieczeństwa państwa i bezpieczeństwa publicznego lub dla zapewnienia prowadzenia dochodzeń w sprawie przestępstw, postępowań przygotowawczych i postępowań przed sądem karnym[28]. |
| Litwa | Na potrzeby prowadzenia dochodzeń w sprawie poważnych i bardzo poważnych przestępstw, ich wykrywania i ścigania, zgodnie z definicją litewskiego kodeksu karnego[29]. |
| Luksemburg | Na potrzeby wykrywani przestępstw, za które grozi kara pozbawienia wolności na okres maksymalnie jednego roku lub dłuższy, prowadzenia dochodzeń w ich sprawie oraz ich ścigania[30]. |

20 Artykuł 1 rozporządzenia o zatrzymywaniu danych.
21 Artykuł 110 ust. 1 kodeksu postępowania karnego.
22 Artykuł 6 ustawy o łączności (zatrzymywanie danych) z 2011 r.
23 Przestępstwa te zdefiniowano w art. 4 ustawy 2225/1994; Artykuł 1 ustawy 3917/2011.
24 Artykuł 1 ust. 1 ustawy 25/2007.
25 Ustawy regulujące wykorzystanie zatrzymanych danych, odpowiednio, w przypadku przestępstw, zapobiegania aktom terrorystycznym oraz ochrony własności intelektualnej są następujące: art. L.34-1(II), CPCE, ustawa nr 2006-64 z dnia 23 stycznia 2006 r. oraz ustawa nr 2009-669 z dnia 12 czerwca 2009 r.
26 Artykuł 132 ust. 1, kodeks ochrony danych.
27 Artykuł 4 ust. 1 ustawy 183/2007.
28 Artykuł 71 ust. 1 ustawy o łączności elektronicznej.
29 Artykuł 65 ustawy X-1835.
30 Artykuł 1 ust. 1 ustawy z dnia 24 lipca 2010 r.

| Tabela 1: Ograniczanie celu zatrzymywania danych określone w przepisach krajowych | |
|---|---|
| Węgry | W celu umożliwienia organom dochodzeniowym, prokuratorom, sądom oraz krajowym agencjom bezpieczeństwa realizację ich obowiązków, umożliwienia policji oraz urzędowi ds. celnych i podatkowych dochodzenia międzynarodowych przestępstw, za które grozi kara pozbawienia wolności na okres dwóch lat lub więcej[31]. |
| Malta | Na potrzeby prowadzenia dochodzeń w sprawie poważnych przestępstw, ich wykrywania lub ścigania[32]. |
| Niderlandy | Na potrzeby prowadzenia dochodzenia w sprawie poważnych przestępstw , za które grozi kara pozbawienia wolności[33] i ścigania tych przestępstw. |
| Austria | Brak transpozycji. |
| Polska | W celu zapobiegania przestępstwom lub ich wykrywania, w celu zapobiegania przestępstwom skarbowym lub ich wykrywania, w celu wykorzystania przez prokuratorów i sądy, jeżeli są istotne dla trwającego postępowania sądowego, na potrzeby Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Centralnego Biura Antykorupcyjnego, Służby Kontrwywiadu Wojskowego oraz Wywiadu Wojskowego w realizacji ich zadań[34]. |
| Portugalia | Na potrzeby prowadzenia dochodzeń w sprawie poważnych przestępstw[35] oraz ich wykrywania i ścigania. |
| Rumunia | Brak transpozycji. |
| Słowenia | Dla „zapewnienia bezpieczeństwa narodowego, postanowień konstytucyjnych i bezpieczeństwa, a także politycznych i gospodarczych interesów państwa […] jak również w celu obrony narodowej”[36]. |
| Słowacja | W celu zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, ich wykrywania i ścigania[37]. |
| Finlandia | W celu prowadzenia dochodzeń w sprawie poważnych przestępstw, ich wykrywania i ścigania, zgodnie z rozdziałem 5a, art. 3 ust. 1 ustawy o środkach przymusu[38]. |
| Szwecja | Brak transpozycji. |
| Zjednoczone Królestwo | Na potrzeby prowadzenia dochodzeń w sprawie poważnych przestępstw[39] oraz ich wykrywania i ścigania. |

Większość transponujących państw członkowskich pozwala na podstawie swoich przepisów na dostęp do zatrzymanych danych i korzystanie z nich do celów wykraczających poza cele objęte dyrektywą, w tym do zapobiegania i zwalczania przestępczości, a także zapobiegania

31 Ogólny cel zatrzymywania danych - art. 159 lit. A) ustawy C/2003, zmienionej ustawą CLXXIV/2007; cel uzyskiwania dostępu przez policję - art. 68 ustawy XXXIV/1994; cel uzyskiwania dostępu przez urząd ds. celnych i podatkowych, art. 59 ustawy CXXII/2010.

32 Art. 20 ust. 1, Legal Notice 198/2008.

33 Artykuł 126 kodeksu postępowania karnego.

34 Artykuł 180a, ustawy – Prawo telekomunikacyjne z dnia 16 lipca 2004 r. zmienionej art. 1 ustawy z dnia 24 kwietnia 2009 r.

35 Artykuł 1 ust. 3 pkt 1 ustawy 32/2008.

36 Artykuł 170a ust. 1 ustawy o łączności elektronicznej.

37 Artykuł 59a ust. 6 ustawy o łączności elektronicznej.

38 Artykuł 14a ust. 1 ustawy o łączności elektronicznej.

39 Regulacje w sprawie zatrzymywania danych (dyrektywa WE) z 2009 r. (2009 nr 859).

zagrożeniom dla zdrowia i życia. Dyrektywa o e-prywatności dopuszcza takie rozwiązanie, jednak stopień harmonizacji osiągnięty w prawodawstwie UE jest nadal ograniczony. Różnice pod względem celów zatrzymywania danych przypuszczalnie wpływają na ilość i częstotliwość wniosków, a tym samym na koszty ponoszone przy wypełnianiu obowiązków ustanowionych w dyrektywie. Ponadto w tej sytuacji może brakować wystarczającej przewidywalności, która jest wymagana przy każdym środku legislacyjnym ograniczającym prawo do prywatności[40]. Komisja zbada potrzebę osiągnięcia większego stopnia harmonizacji w tym obszarze oraz warianty, które na to pozwalają[41].

### 4.2. Operatorzy, od których wymaga się zatrzymywania danych (art. 1)

Dyrektywa ma zastosowanie do „dostawców ogólnie dostępnych usług łączności elektronicznej lub publicznych sieci łączności" (art. 1 ust. 1). Dwa państwa członkowskie (Finlandia i Zjednoczone Królestwo) nie wymagają zatrzymywania danych od małych operatorów ponieważ, jak argumentują, koszty realizacji tego obowiązku zarówno dla dostawców, jak i państwa przewyższałyby korzyści dla wymiaru sprawiedliwości w sprawach karnych oraz egzekwowania prawa. Cztery państwa członkowskie (Łotwa, Luksemburg, Niderlandy i Polska) zgłosiły, że wprowadziły alternatywne rozwiązania administracyjne. Podczas gdy duzi operatorzy w szeregu państw członkowskich korzystają z efektu skali w zakresie kosztów, mniejsi operatorzy w niektórych państwach członkowskich ustanawiają zazwyczaj wspólne przedsięwzięcia lub zlecają to zadanie spółkom zewnętrznym wyspecjalizowanym w zatrzymywaniu i pobieraniu danych, w celu ograniczenia kosztów. Zlecenie realizacji funkcji technicznych w ten sposób nie wpływa na obowiązek odpowiedniego nadzorowania przez dostawców operacji przetwarzania oraz zagwarantowania niezbędnych środków bezpieczeństwa, co może być problematyczne dla mniejszych operatorów. Komisja zbada kwestie bezpieczeństwa danych oraz wpływu na małe i średnie przedsiębiorstwa w kontekście wariantów zmiany ram zatrzymywania danych.

### 4.3. Dostęp do danych: organy, procedury i warunki (art. 4)

Od państw członkowskich wymaga się zapewnienia, że zatrzymane dane „są udostępniane jedynie właściwym organom krajowym, w szczególnych przypadkach i zgodnie z krajowym ustawodawstwem". Pozostawia się państwom członkowskim, aby określiły w swoich przepisach krajowych „proces oraz warunki uzyskiwania dostępu do zatrzymanych danych, w przypadkach gdy został spełniony wymóg konieczności oraz proporcjonalności […] podlegając odpowiednim przepisom prawa Unii Europejskiej lub międzynarodowego prawa publicznego, w szczególności EKOPC, zgodnie z interpretacją Europejskiego Trybunału Praw Człowieka".

---

40 Wyrok Europejskiego Trybunał Sprawiedliwości z dnia 20 maja 2003 r. w sprawach połączonych C-465/00, C-138/01 i C-139/01 (wniosek o wydanie orzeczenia w trybie prejudycjalnym złożony przez Verfassungsgerichtshof i Oberster Gerichtshof): Rechnungshof (C-465/00) przeciwko Österreichischer Rundfunk i in. oraz między Christą Neukomm (C-138/01), Josephem Lauermannem (C-139/01) i Österreichischer Rundfunk (Ochrona osób fizycznych w odniesieniu do przetwarzania danych osobowych – Dyrektywa 95/46/WE – Ochrona życia prywatnego – Ujawnianie danych na temat dochodów pracowników podmiotów podlegających kontroli Rechnungshof).).

41 W momencie przyjmowania dyrektywy Komisja wydała oświadczenie, w którym zasugerowała przeanalizowanie wykazu przestępstw w europejskim nakazie aresztowania. (Decyzja ramowa Rady 2002/584/WSiSW z dnia 13 czerwca 2002 r. w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między państwami członkowskimi)

We wszystkich państwach członkowskich dostęp do zatrzymywanych danych mają krajowe służby policyjne oraz – z wyjątkiem jurysdykcji *common law* (Irlandia i Zjednoczone Królestwo) – prokuratorzy. Czternaście państw członkowskich wśród właściwych organów wymieniło służby bezpieczeństwa, agencje wywiadu lub wojsko. Sześć państw członkowskich wyszczególniło organy podatkowe lub celne, trzy zaś – organy straży granicznej. Jedno państwo członkowskie zezwala na dostęp do danych organom publicznym, jeżeli organy te są uprawnione do realizacji zadań specjalnych na mocy prawodawstwa wtórnego. Jedenaście państw członkowskich wymaga zezwolenia sądu w przypadku każdego wniosku o dostęp do zatrzymanych danych. W trzech państwach członkowskich zezwolenie sądu jest wymagane w większości przypadków. Cztery inne państwa członkowskie wymagają zezwolenia od wyższego urzędu, jednak nie sędziowskiego. W dwóch państwach członkowskich jedynym wymogiem jest złożenie wniosku w formie pisemnej.

| **Tabela 2: Dostęp do zatrzymanych danych telekomunikacyjnych** | | |
|---|---|---|
| | *Właściwe organy krajowe* | *Proces i warunki* |
| Belgia | Sądowa jednostka koordynacyjna, sędziowie śledczy, prokurator, policja kryminalna | Sędzia lub prokurator musi wydać zezwolenie na dostęp. W odpowiedzi na wniosek operator musi udostępnić w „czasie rzeczywistym" dane abonenta, dane o ruchu i lokalizacji dotyczące połączeń wykonanych w przeciągu minionego miesiąca.<br>Dane dotyczące starszych połączeń muszą zostać udostępnione jak najszybciej. |
| Bułgaria[42] | Specjalne oddziały i departamenty Państwowej Agencji Bezpieczeństwa Narodowego, Ministerstwo Spraw Wewnętrznych, Agencja Informacji Wojskowej, Agencja Policji Wojskowej, Ministerstwo Obrony, Krajowa Agencja Dochodzeniowa; sąd i organy prowadzące postępowanie przygotowawcze na określonych warunkach. | Dostęp możliwy jedynie w oparciu o nakaz prezesa sądu regionalnego |
| Republika Czeska | Brak transpozycji. | |
| Dania[43] | Policja | Dostęp wymaga zezwolenia sądu; nakazy sądowe są wydawane wtedy, gdy wniosek spełnia ścisłe kryteria dotyczące podejrzenia, konieczności oraz proporcjonalności. |
| Niemcy | Brak transpozycji | |
| Estonia[44] | Policja i straż graniczna, Urząd Policji Bezpieczeństwa oraz, w odniesieniu do przedmiotów i łączności elektronicznej – Urząd ds. Podatków i Ceł. | Dostęp wymaga zezwolenia sędziego śledczego.<br>Operatorzy muszą „udostępnić zatrzymane dane w pilnych przypadkach w ciągu dziesięciu godzin, zaś w innych przypadkach w ciągu dziesięciu dni roboczych [od momentu otrzymania wniosku]". |
| Irlandia[45] | Członkowie Garda Síochána (policja) w randze Chief Superintendant lub wyższej; Oficerowie Permanent Defence Force w | Wniosek musi być złożony w formie pisemnej |

[42] Artykuł 250b ust. 1 ustawy o łączności elektronicznej (wersja zmieniona) z 2010 r. (organy); Artykuł 250b ust. 2, art. 250c ust. 1 ustawy o łączności elektronicznej (wersja zmieniona) z 2010 r. (dostęp);

[43] Rozdział 71 ustawy o organizacji wymiaru sprawiedliwości.

[44] Artykuł 112 ust. 2 i 3 kodeksu postępowania karnego (w odniesieniu do organów i procesu); Artykuł 111 ust. 9 ustawy o łączności elektronicznej (warunki);

| Tabela 2: Dostęp do zatrzymanych danych telekomunikacyjnych | | |
|---|---|---|
| | *Właściwe organy krajowe* | *Proces i warunki* |
| | randze pułkownika lub wyższej; Urzędnicy komisarza ds. dochodów w randze głównego urzędnika lub wyższej | |
| Grecja[46] | Organy sądowe, wojskowe lub policyjne. | Dostęp wymaga orzeczenia sądowego stwierdzającego, że prowadzenie dochodzenia innymi metodami jest niemożliwie lub niezwykle trudne. |
| Hiszpania[47] | Służby policyjne odpowiedzialne za wykrywanie poważnych przestępstw, prowadzenie dochodzeń w ich sprawie oraz ich ściganie, Krajowy Ośrodek Wywiadowczy oraz Agencja Celna. | Dostęp właściwych organów krajowych do tych danych wymaga wcześniejszego uzyskania zezwolenia sądu. |
| Francja[48] | Prokurator, wyznaczeni oficerowie policji i żandarmerii | Policja musi przedstawić uzasadnienie dla każdego wniosku o dostęp do zatrzymanych danych i musi uzyskać zezwolenie od osoby z Ministerstwa Spraw Wewnętrznych wyznaczonej przez Commission nationale de contrôle des interceptions de sécurité.<br>Za wnioski o dostęp odpowiada wyznaczony urzędnik zatrudniony przez operatora. |
| Włochy[49] | Prokurator; policja; obrońca – czy to w imieniu oskarżonego, czy to w imieniu osoby objętej dochodzeniem | Dostęp wymaga złożenia „uzasadnionego nakazu" wystawionego przez prokuratora |
| Cypr[50] | Sądy, prokuratura, policja | Zezwolenie na dostęp musi zatwierdzić prokurator, który czyni to jeżeli uważa, że może dzięki temu zyskać dowody popełnienia poważnego przestępstwa.<br>Taki nakaz może wystawić sędzia, jeżeli istnieje uzasadnione podejrzenie, że popełniono poważne przestępstwo, i jeżeli jest prawdopodobne, że dane się z nim wiążą. |
| Łotwa[51] | Upoważnieni urzędnicy w instytucjach dochodzeniowych prowadzących postępowanie przygotowawcze; osoby wykonujące pracę dochodzeniową; upoważnieni urzędnicy w instytucjach bezpieczeństwa państwa; prokuratura; sądy. | Upoważnieni urzędnicy, urząd prokuratora i sądy mają obowiązek oceny „stosowalności i znaczenia" wniosku, zarejestrowania wniosku oraz zapewnienia bezpieczeństwa uzyskanych danych. Upoważnione organy mogą podpisać porozumienie z operatorem, np. dotyczące zakodowania udostępnionych danych. |
| Litwa[52] | Organy prowadzące dochodzenie (przygotowawcze), prokurator, sąd (sędziowie) oraz oficerowie wywiadu. | Upoważnione organy publiczne muszą złożyć wniosek o zatrzymane dane w formie pisemnej.<br>Dla dostępu na potrzeby dochodzenia przygotowawczego niezbędny jest nakaz sądowy. |
| Luksemburg[53] | Organy sądowe (sędziowie śledczy, | Dostęp wymaga zezwolenia sądu. |

45 Artykuł 6 ustawy o łączności (zatrzymywanie danych) z 2009 r.

46 Art. 3 i 4 ustawy 2225/94.

47 Artykuły 6-7 ustawy 25/2007.

48 Artykuł 60 ust. 1 i art. 60 ust. 2 kodeksu postępowania karnego (organy); Artykuł L.31 ust.1 pkt 1 (warunki).

49 Artykuł 132 ust. 3, kodeks ochrony danych.

50 Artykuł 4 ust. 2 i art. 4 ust. 4 ustawy 183(I)/2007.

51 Artykuł 71 ust. 1 ustawy o łączności elektronicznej (organy); Rozporządzenie gabinetu nr 820 (procedury).

52 Artykuł 77 ust. 1, 2 ustawy X-1835; ustne sprawozdanie złożone w Komisji.

| Tabela 2: Dostęp do zatrzymanych danych telekomunikacyjnych | | |
|---|---|---|
| | *Właściwe organy krajowe* | *Proces i warunki* |
| | prokurator), organy odpowiedzialne za zapewnienie bezpieczeństwa państwa, obrony, bezpieczeństwa publicznego, zapobieganie przestępstw, prowadzenie dochodzeń w ich sprawie oraz ich wykrywanie i ściganie. | |
| Węgry[54] | Policja, Urząd ds. Podatków i Ceł, krajowe agencje bezpieczeństwa, prokuratura, sądy. | Policja oraz Urząd ds. Podatków i Ceł, wymóg uzyskania zezwolenia prokuratora. Prokurator i agencje bezpieczeństwa krajowego mogą mieć dostęp do takich danych bez konieczności nakazu sądowego. |
| Malta[55] | maltańska policja; służby bezpieczeństwa | Wniosek musi być w formie pisemnej. |
| Niderlandy[56] | Oficer policji dochodzeniowej | Dostęp musi zostać uzyskany na podstawie nakazu prokuratora lub sędziego śledczego. |
| Austria | Brak transpozycji | |
| Polska[57] | Policja, straż graniczna, inspektorzy podatkowi, Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu Zagranicznego, Centralne Biuro Antykorupcyjne, Służby Kontrwywiadu Wojskowego oraz Wywiadu Wojskowego, sądy i prokurator. | Wniosek musi być sporządzony w formie pisemnej, a w przypadku policji, straży granicznej, inspektorów podatkowych - autoryzowany przez urzędnika wyższego szczebla w danej jednostce. |
| Portugalia[58] | Policja kryminalna, Narodowa Gwardia Republikańska, Państwowe Biuro Bezpieczeństwa, Żandarmeria Wojskowa, Departament ds. Granic i Cudzoziemców, Policja Morska. | Przekazanie danych wymaga zezwolenia sędziego i musi być uzasadnione tym, że dostęp ma kluczowe znaczenie dla odkrycia prawdy lub że zdobycie dowodów w inny sposób byłoby niemożliwe lub bardzo trudne. Rozpatrując wniosek o wydanie zezwolenia, sędzia bierze pod uwagę wymogi konieczności i proporcjonalności. |
| Rumunia | Brak transpozycji | |
| Słowenia[59]: | Policja, agencje wywiadu i bezpieczeństwa, agencje obronności odpowiedzialne za wywiad i kontrwywiad oraz misje bezpieczeństwa. | Dostęp wymaga zezwolenia sądu. |
| Słowacja[60], | Organy ścigania, sądy. | Wniosek musi być w formie pisemnej. |
| Finlandia[61] | Policja, straż graniczna, organy celne (w przypadku zatrzymanych danych dotyczących abonenta, danych o ruchu i o lokalizacji). Centrum Reagowania Kryzysowego, służby ratownictwa morskiego, oddział ratownictwa morskiego (dla identyfikacji i lokalizacji | Wszystkie właściwe organy mogą uzyskać dostęp do danych o abonencie bez konieczności uzyskania zezwolenia sądu. Pozostałe dane wymagają nakazu sądowego. |

53 Artykuł 5 ust. 2 pkt 1 oraz art. 9 ust. 2 ustawy z dnia 24 lipca 2010 r. (organy); Artykuł 67-1, kodeksu postępowania karnego (warunki).

54 Artykuł 68 lit. ust. 1 i art. 69 ust. 1 lit. c) i d), ustawa XXXIV z 1994 r.; Artykuł 9 lit. a pkt 1 ustawy V z 1972 r.; Artykuł 71 ust. 1, 3 i 4, art. 178 lit. A ust. 4, art. 200, art. 201, art. 268 ust. 2 ustawy XIX z 1998 r.; Artykuł 40 ust. 1, art. 40 ust. 2, art.53 ust. 1, art. 54 ust. 1 lit j) ustawy CXXV z 1995 r.

55 Artykuł 20 ust. 1 oraz art. 20 ust. 3, Legal Notice 198/2008.

56 Artykuł 126ni, kodeks postępowania karnego.

57 Artykuł 179 ust. 3 ustawy – Prawo telekomunikacyjne z dnia 16 lipca 2004 r. zmienionej art. 1 ustawy z dnia 24 kwietnia 2009 r.

58 Artykuł 2 ust. 1, art. 3 ust. 2 i art. 9 ustawy 32/2008.

59 Artykuł 107c ustawy o łączności elektronicznej; Artykuł 149b kodeksu postępowania karnego; artykuł 24 lit. b) ustawy o agencji wywiadu i bezpieczeństwa; Artykuł 32 ustawy o obronności.

60 Artykuł 59a ust. 8 ustawy o łączności elektronicznej.

| Tabela 2: Dostęp do zatrzymanych danych telekomunikacyjnych | | |
|---|---|---|
| | *Właściwe organy krajowe* | *Proces i warunki* |
| | danych w przypadkach kryzysowych). | |
| Szwecja | Brak transpozycji | |
| Zjednoczone Królestwo[62] | Policja, służby wywiadowcze, organy podatkowe i celne, inne organy publiczne wyznaczone w prawodawstwie wtórnym. | Dostęp jest dozwolony pod warunkiem uzyskania zezwolenia „wyznaczonej osoby" oraz sprawdzenia konieczności i proporcjonalności, w szczególnych przypadkach i okolicznościach, w których ujawnienie danych jest dozwolone lub wymagane na mocy prawa. Z operatorami ustalono konkretne procedury. |

Komisja oceni potrzebę większego stopnia harmonizacji w odniesieniu do organów mających dostęp do zatrzymanych danych i procedur uzyskiwania danych oraz warianty umożliwiające osiągnięcie tego celu. Mogłyby one obejmować ściślejsze zdefiniowanie wykazu właściwych organów, niezależny lub sądowy nadzór nad wnioskami o udostępnienie danych oraz minimalne normy proceduralne dla operatorów w przypadkach udzielania dostępu właściwym organom.

### 4.4. Zakres zatrzymywanych danych i kategorie danych objętych zatrzymaniem (art. 1 ust. 2, art. 3 ust. 2 i art. 5)

Dyrektywa ma zastosowanie do obszaru telefonii stacjonarnej, telefonii komórkowej, dostępu internetowego, elektronicznej poczty internetowej i telefonii internetowej. W dyrektywie (art. 5) określono kategorie danych przeznaczonych do zatrzymywania, mianowicie dane niezbędne do ustalenia:

(a) źródła połączenia;

(b) odbiorcy połączenia;

(c) daty, godziny i czasu trwania połączenia;

(d) rodzaju połączenia;

(e) urządzenia komunikacji lub tego, co może służyć za urządzenie komunikacji; oraz

(f) lokalizacji urządzenia komunikacji ruchomej.

Dyrektywa obejmuje również (art. 3 ust. 2) nieudane próby połączenia, to znaczy nawiązanie łączności, w przypadku którego połączenie nie zostało odebrane lub nastąpiła interwencja sieci, i w odniesieniu do którego dane są generowane, przetwarzane i przechowywane lub rejestrowane przez operatorów. Zgodnie z dyrektywą nie można zatrzymywać danych, które

---

61 Artykuł 35 ust. 1 i art. 36 ustawy o łączności elektronicznej; Artykuły 31-33 ustawy o policji; artykuł 41 ustawy o straży granicznej.

62 Artykuł 25, harmonogram 1, ustawa o regulacji władzy dochodzeniowej (RIPA) z 2000 r.; Artykuł 7 rozporządzenia o zatrzymywaniu danych. Artykuł 22 ust. 2 RIPA określa cele, dla jakich organy mogą uzyskać dostęp do danych.

ujawniają treść komunikatu. Wyjaśniono również później, że treść zapytań używanych do wyszukiwania, tzn. dane zarejestrowane przy korzystaniu z oferowanych usług wyszukiwania, także pozostają poza zakresem dyrektywy ponieważ uznawane są raczej za treść komunikatu niż za dane o ruchu[63].

Dwadzieścia jeden państw członkowskich przewiduje zatrzymywanie tych kategorii danych w swoich przepisach służących transpozycji. Belgia nie przewidziała zatrzymywania danych telefonicznych, nie ma też żadnych przepisów na temat danych związanych z Internetem. Respondenci udzielający odpowiedzi na kwestionariusz Komisji nie uznali za konieczne uzupełnienia kategorii zatrzymywanych danych, mimo że Parlament Europejski skierował do Komisji pisemną deklarację wzywającą do rozszerzenia zakresu dyrektywy o wyszukiwarki „w celu szybkiego zwalczania pornografii dziecięcej oraz przypadków wykorzystywania seksualnego”[64]. W swoim sprawozdaniu na temat drugiego etapu egzekwowania Grupa Robocza Art. 29 wskazywała, że kategorie ustanowione w dyrektywie powinny być uznawane za wyczerpujące i że operatorów nie należy obciążać dodatkowymi obowiązkami w zakresie zatrzymywania danych. Komisja zbada konieczność wszystkich tych kategorii danych.

### 4.5. Okresy zatrzymywania (art. 6 i 12 )

Państwa członkowskie mają obowiązek zapewnienia zatrzymywania kategorii danych wymienionych w art. 5 na okres nie krótszy niż 6 miesięcy oraz nie dłuższy niż dwa lata. Maksymalny okres zatrzymania może zostać przedłużony przez państwo członkowskie „znajdujące się w szczególnych okolicznościach, uzasadniających przedłużenie maksymalnego okresu zatrzymywania […] o ograniczony okres czasu”; takie przedłużenie trzeba zgłosić Komisji, która w ciągu sześciu miesięcy od dnia zgłoszenia może podjąć decyzję o zatwierdzeniu lub odrzuceniu przedłużenia. Maksymalny okres zatrzymania może zostać przedłużony, nie ma jednak przepisu przewidującego możliwość skrócenia minimalnego, sześciomiesięcznego okresu. Wszystkie państwa członkowskie, które transponowały dyrektywę, stosują okresy zatrzymania mieszczące się w tych granicach i Komisja nie otrzymała żadnych zgłoszeń o przedłużeniu. Jednak w obrębie UE nie ma jednolitego podejścia.

Piętnaście państw członkowskich określiło jednolity okres w odniesieniu do wszystkich kategorii danych: jedno państwo członkowskie (Polska) ustanowiło dwuletni okres zatrzymania, jedno półtoraroczny okres (Łotwa), w dziesięciu państwach (Bułgaria, Dania, Estonia, Grecja, Hiszpania, Francja, Niderlandy, Portugalia, Finlandia i Zjednoczone Królestwo) wynosi on jeden rok, a w trzech (Cypr, Luksemburg i Litwa) sześć miesięcy. Pięć państw członkowskich określiło różne okresy zatrzymania w odniesieniu do różnych kategorii danych: dwa państwa członkowskie (Irlandia i Włochy) ustanowiły dwuletni okres zatrzymania w odniesieniu do danych dotyczących telefonii stacjonarnej i komórkowej oraz roczny okres w odniesieniu do dostępu internetowego, elektronicznej poczty internetowej i telefonii internetowej; jedno państwo członkowskie (Słowenia) ustanowiło czternastomiesięczny okres w odniesieniu do danych telefonicznych oraz ośmiomiesięczny w odniesieniu do danych dotyczących Internetu; jedno państwo członkowskie (Słowacja)

---

63 Opinia Grupy Robocza Art. 29 z dnia 4 kwietnia 2008 r. dotycząca zagadnień ochrony danych związanych z wyszukiwarkami.

64 Pisemna deklaracja na podstawie zasady 123 regulaminu dotycząca ustanowienia europejskiego systemu szybkiego ostrzegania o pedofilach i przestępcach seksualnych, 19.4.2010 r., 0029/2010.

zgłosiło roczny okres w odniesieniu do telefonii stacjonarnej i komórkowej oraz sześciomiesięczny w odniesieniu do danych dotyczących Internetu; jedno państwo członkowskie (Malta) ustanowiło roczny okres w odniesieniu do telefonii stacjonarnej, komórkowej oraz internetowej oraz sześciomiesięczny w odniesieniu do dostępu internetowego i elektronicznej poczty internetowej. Jedno państwo członkowskie (Węgry) zatrzymuje wszystkie dane na jeden rok, z wyjątkiem danych dotyczących nieudanych prób połączenia, które zatrzymywane są jedynie na okres sześciu miesięcy. Jedno państwo członkowskie (Belgia) nie sprecyzowało żadnych okresów przechowywania kategorii danych określonych w dyrektywie. Szczegółowe informacje zawiera tabela 3.

| **Tabela 3: okresy zatrzymania ustanowione w przepisach krajowych** | |
|---|---|
| Belgia[65] | Od roku do 36 miesięcy w przypadku ogólnie dostępnych usług telefonicznych. Brak przepisów na temat danych dotyczących Internetu. |
| Bułgaria | Jeden rok (udostępnione dane mogą być zatrzymywane na wniosek przez kolejnych sześć miesięcy). |
| Republika Czeska | Brak transpozycji |
| Dania | Jeden rok |
| Niemcy | Brak transpozycji |
| Estonia | Jeden rok |
| Irlandia | Dwa lata w odniesieniu do telefonii stacjonarnej i komórkowej, jeden rok w odniesieniu do dostępu internetowego, elektronicznej poczty internetowej i telefonii internetowej. |
| Grecja | Jeden rok |
| Hiszpania | Jeden rok |
| Francja | Jeden rok |
| Włochy | Dwa lata w odniesieniu do telefonii stacjonarnej i komórkowej, jeden rok w odniesieniu do dostępu internetowego, elektronicznej poczty internetowej i telefonii internetowej. |
| Cypr | Sześć miesięcy |
| Łotwa | Osiemnaście miesięcy |
| Litwa | Sześć miesięcy |
| Luksemburg | Sześć miesięcy |
| Węgry | Sześć miesięcy w przypadku nieudanych prób połączenia oraz jeden rok w odniesieniu do wszystkich innych danych. |
| Malta | Jeden rok w odniesieniu do telefonii stacjonarnej, komórkowej i internetowej oraz sześć miesięcy w odniesieniu do dostępu internetowego i elektronicznej poczty internetowej. |
| Niderlandy | Jeden rok |
| Austria | Brak transpozycji |
| Polska | Dwa lata |
| Portugalia | Jeden rok |
| Rumunia | Brak transpozycji (sześć miesięcy na podstawie wcześniejszych przepisów transponujących, które zostały uchylone). |
| Słowenia | Czternaście miesięcy w odniesieniu do danych telefonicznych oraz osiem miesięcy w odniesieniu do danych dotyczących Internetu. |
| Słowacja | Jeden rok w odniesieniu do telefonii stacjonarnej i komórkowej, sześć miesięcy w odniesieniu do dostępu internetowego, elektronicznej poczty internetowej i telefonii internetowej. |
| Finlandia | Jeden rok |
| Szwecja | Brak transpozycji |

[65] Artykuł 126 ust. 2 ustawy z dnia 2005 r. o łączności elektronicznej

| Tabela 3: okresy zatrzymania ustanowione w przepisach krajowych | |
|---|---|
| Zjednoczone Królestwo | Jeden rok |

Dyrektywa dopuszcza wprawdzie różnorodne podejścia, jednak w rezultacie zapewnia ona jedynie ograniczoną pewność prawną w UE operatorom, którzy działają w więcej niż jednym państwie członkowskim, oraz obywatelom, których dane dotyczące łączności mogą być przechowywane w różnych państwach członkowskich. Uwzględniając coraz większy międzynarodowy wymiar przetwarzania danych oraz możliwości outsourcingu przechowywania danych, należy rozważyć harmonizację okresów zatrzymywania w obrębie UE. W celu zgodności z zasadą proporcjonalności oraz w świetle jakościowych i ilościowych danych wskazujących na wartość zatrzymanych danych w państwach członkowskich oraz tendencje w dziedzinie łączności i technologii oraz przestępczości i terroryzmu, Komisja rozważy zastosowanie odmiennych okresów do różnych kategorii danych, różnych kategorii poważnych przestępstw lub połączenie tych kryteriów[66]. Przekazane dotychczas przez państwa członkowskie dane ilościowe dotyczące wieku zatrzymanych danych wskazują, że ok. 90 % danych ma sześć miesięcy lub mniej, a około 70 % trzy miesiące lub mniej w momencie składania przez organy ścigania (pierwotnego) wniosku (zob. pkt 5.2).

### 4.6. Ochrona danych i bezpieczeństwo danych oraz organy nadzorujące (art. 7 i 9)

Dyrektywa wymaga od państw członkowskich zapewnienia przestrzegania przez operatorów co najmniej czterech zasad dotyczących bezpieczeństwa, zgodnie z którymi zatrzymywane dane:

(a) będą takiej samej jakości i będą podlegać takim samym zasadom bezpieczeństwa i ochrony, jak dane publicznej sieci łączności;

(b) będą podlegać właściwym środkom technicznym i organizacyjnym w celu ochrony tych danych przed przypadkowym lub bezprawnym zniszczeniem, przypadkową utratą lub zmianą, nieupoważnionym lub bezprawnym przechowywaniem, przetwarzaniem, dostępem lub ujawnieniem;

(c) będą podlegać właściwym środkom technicznym i organizacyjnym w celu zapewnienia, by dostęp do danych miał jedynie upoważniony do tego personel; oraz

(d) będą, z wyjątkiem danych udostępnionych i zachowanych [w celu określonym w dyrektywie], niszczone pod koniec okresu zatrzymania.

Zgodnie z dyrektywą o ochronie danych oraz dyrektywą o e-prywatności operatorzy nie mają prawa przetwarzać zatrzymanych na podstawie dyrektywy danych dla innych celów, chyba że dane zostały zatrzymane z innego powodu[67]. Państwa członkowskie są zobowiązane do wyznaczenia organu władzy publicznej odpowiedzialnego za nadzorowanie w sposób w pełni niezależny stosowania powyższych zasad, przy czym może być to ten sam organ, który wymagany jest na podstawie dyrektywy o ochronie danych[68].

---

66 Wniosek Komisji w sprawie dyrektywy dotyczącej zatrzymywania danych z 2005 r. przewidywał jednoroczny okres zatrzymywania danych telefonicznych i sześciomiesięczny danych internetowych.

67 Artykuł 13 ust. 1 dyrektywy 95/46/WE.

68 Artykuł 28 dyrektywy 95/46/WE.

Piętnaście państw członkowskich transponowało wszystkie wymienione zasady do odpowiednich przepisów krajowych. Cztery państwa członkowskie (Belgia, Estonia, Hiszpania i Łotwa) transponowały dwie lub trzy z wymienionych zasad, jednak nie wprowadziły wyraźnych przepisów nakazujących zniszczenie danych po upływie okresu zatrzymania. Dwa państwa członkowskie (Włochy i Finlandia) przewidują niszczenie danych. Nie jest jasne, które konkretne techniczne i organizacyjne środki bezpieczeństwa, takie jak wzmocnione uwierzytelnienie oraz zarządzanie szczegółowymi protokołami dostępu[69], zostały zastosowane. Dwadzieścia jeden państw członkowskich posiada organ nadzorczy odpowiedzialny za monitorowanie zastosowania zasad. W większości przypadków jest to organ do spraw ochrony danych. Szczegółowe informacje zawiera tabela 4.

**Tabela 4: ochrona danych i bezpieczeństwo danych oraz organy nadzorujące**

| *Państwo członkowskie* | *Ochrona danych i krajowe przepisy dotyczące bezpieczeństwa danych* | *Organ nadzoru* |
|---|---|---|
| Belgia | Operatorzy muszą zagwarantować, by przesyłane dane nie mogły zostać przechwycone przez osoby trzecie oraz muszą wypełniać normy ETSI w zakresie bezpieczeństwa łączności i legalnego przechwytywania[70].<br>Wydaje się, że nie uregulowano zasady obowiązkowego zniszczenia danych na koniec okresu zatrzymania. | Instytut Usług Pocztowych i Telekomunikacji |
| Bułgaria | Przepisy transponujące obejmują wymóg wdrożenia czterech zasad[71]. | Komisja Ochrony Danych Osobowych monitoruje przetwarzanie i przechowywanie danych w celu zapewnienia zgodności z wymogami. Parlamentarna komisja w Zgromadzeniu Narodowym monitoruje procedury udzielania zezwoleń i dostępu do danych |
| Republika Czeska[72]. | Brak transpozycji. | |
| Dania | Cztery zasady zostały uwzględnione [73]. | Krajowa Agencja Informatyczno-Telekomunikacyjna monitoruje spełnienie wymogów, zgodnie z którymi dostawcy sieci i usług łączności elektronicznej muszą dopilnować, aby sprzęt i systemy techniczne pozwoliły policji na dostęp do informacji o ruchu telekomunikacyjnym. |
| Niemcy | Brak transpozycji. | |

69 Wzmocnione uwierzytelnienie wymaga podwójnego mechanizmu uwierzytelnienia, takiego jak hasło plus dane biometryczne lub hasło plus token w celu zapewnienia fizycznej obecności osoby odpowiedzialnej za przetwarzanie danych o ruchu. Zarządzanie szczegółowymi protokołami dostępu wiąże się ze szczegółowym śledzeniem dostępu i operacji przetwarzania poprzez zatrzymywanie protokołów rejestrujących tożsamość użytkownika, czas dostępu i pliki, do których nastąpił dostęp.

70 Artykuł 6 dekretu królewskiego z dnia 9 stycznia 2003 r.

71 Artykuł 4 ust. 1 stawy o łączności elektronicznej z 2010 r. (z późn. zm.)

72 Artykuł 87 ust. 3 oraz art. 88, ustawa 127/2005, zmieniona ustawą 247/2008; art. 2 ustawy 336/2005; art. 3 ust. 4 ustawy 485/2005; art. 28 ust. 1 ustawy 101/2000.

73 Ustawa o przetwarzaniu danych osobowych; Rozporządzenie nr 714 z dnia 26 czerwca 2008 r. w sprawie dostarczania sieci i usług łączności elektronicznej.

| Tabela 4: ochrona danych i bezpieczeństwo danych oraz organy nadzorujące | | |
|---|---|---|
| *Państwo członkowskie* | *Ochrona danych i krajowe przepisy dotyczące bezpieczeństwa danych* | *Organ nadzoru* |
| Estonia | Przepisy transponujące obejmują trzy spośród czterech zasad. Brak wyraźnych przepisów dotyczących czwartej zasady, jednak każda osoba, której prywatność została naruszona w wyniku działań związanych z nadzorowaniem, może w oparciu o wyrok sądowy domagać się zniszczenia danych[74]. | Odpowiedzialnym organem jest Urząd Nadzoru Technicznego. |
| Irlandia[75] | Przepisy transponujące obejmują wymóg wdrożenia czterech zasad. | Wyznaczony sędzia ma prawo do prowadzenia dochodzenia oraz składania sprawozdania w sprawie tego, czy właściwe organy krajowe postępują zgodnie z przepisami transponującymi. |
| Grecja[76] | Przepisy transponujące obejmują wymóg realizacji czterech zasad, przewidując dodatkowo wymóg przygotowania i realizacji przez operatorów planu zagwarantowania zgodności przez wyznaczoną osobę zarządzającą bezpieczeństwem danych. | Urząd ds. Ochrony Danych Osobowych oraz Urząd ds. Ochrony Prywatności Komunikacji |
| Hiszpania[77] | Przepisy z zakresu bezpieczeństwa danych gwarantują trzy z czterech zasad (jakość i bezpieczeństwo zatrzymywanych danych, dostęp osób upoważnionych i ochronę przed nieupoważnionym przetwarzaniem). | Organem odpowiedzialnym jest Urząd Ochrony Danych. |
| Francja[78] | Przepisy transponujące obejmują wymóg wdrożenia czterech zasad. | Krajowa Komisji ds. Technologii Informatycznych i Swobód nadzoruje wypełnianie obowiązków. |
| Włochy | Brak wyraźnych przepisów w zakresie bezpieczeństwa zatrzymanych danych, aczkolwiek istnieje wymóg zniszczenia lub anonimizacji danych o ruchu oraz o przetwarzaniu danych o ruchu za zgodą[79]. | Organ ds. ochrony danych monitoruje zgodność działań operatora z dyrektywą. |
| Cypr[80] | Przepisy transponujące zapewniają obowiązywanie wszystkich czterech zasad. | Stosowanie przepisów transponujących nadzoruje Komisarz ds. Ochrony Danych Osobowych. |
| Łotwa[81] | Przepisy transponujące zapewniają obowiązywanie dwóch zasad: zasady poufności zatrzymanych danych oraz autoryzowanego dostępu do nich, a także zasadę zniszczenia danych na koniec okresu zatrzymania. | Państwowy Inspektorat Danych nadzoruje ochronę danych osobowych w sektorze łączności elektronicznej, ale nie nadzoruje dostępu do zatrzymanych danych i ich przetwarzania. |

74 Artykuł 111 ust. 9 ustawy o łączności elektronicznej; Artykuł 122 ust. 2 kodeksu postępowania karnego.

75 Artykuły 4, 11 i 12 ustawy o łączności (zatrzymywanie danych) z 2009 r.

76 Artykuł 6 ustawy 3917/2011.

77 Artykuł 8 ustawy 25/2007, art. 38 ust. 3 ogólnej ustawy telekomunikacyjnej. Ustawa (w art. 9) odnosi się do wyjątku w zakresie praw dostępu i anulowania zapisanych w ustawie organicznej 15/1999 w sprawie ochrony danych osobowych (art. 22 i 23).

78 Artykuł D.98-5, CPCE; artykuł L-34-1(V), CPCE; artykuł 34 ustawy nr 78/-17; artykuł 34-1, CPCE; art. 11 ustawy nr 78-17 z dnia 6 stycznia 1978 r.

79 Artykuły 123 i 126 kodeksu ochrony danych.

80 Artykuły 14 i 15 ustawy 183(I)/2007.

81 Artykuł 4 ust. 4 oraz art. 71 ust. 6-8 ustawy o łączności elektronicznej.

| Tabela 4: ochrona danych i bezpieczeństwo danych oraz organy nadzorujące | | |
|---|---|---|
| *Państwo członkowskie* | *Ochrona danych i krajowe przepisy dotyczące bezpieczeństwa danych* | *Organ nadzoru* |
| Litwa[82] | Przepisy transponujące zapewniają obowiązywanie czterech zasad. | Państwowy Inspektorat ds. Ochrony Danych nadzoruje wykonanie przepisów transponujących i jest odpowiedzialny za udostępnianie Komisji Europejskiej danych statystycznych. |
| Luksemburg[83] | Przepisy transponujące zapewniają obowiązywanie czterech zasad. | Organ ds. ochrony danych. |
| Węgry[84] | Przepisy transponujące zapewniają obowiązywanie czterech zasad. | Parlamentarny Komisarz ds. Ochrony Danych oraz Wolności Informacyjnej |
| Malta[85] | Przepisy transponujące zapewniają obowiązywanie czterech zasad. | Komisarz ds. ochrony danych. |
| Niderlandy[86] | Przepisy transponujące zapewniają obowiązywanie czterech zasad. | Agencja Komunikacji Radiowej nadzoruje realizację zobowiązań przez dostawców Internetu i usług telefonicznych; organ ds. ochrony danych pełni ogólny nadzór nad przetwarzaniem danych osobowych; szczegóły dotyczące współpracy tych dwóch organów zawarte zostały w protokole. |
| Austria | Brak transpozycji. | |
| Polska | Przepisy transponujące zapewniają obowiązywanie czterech zasad[87]. | Organ ds. ochrony danych. |
| Portugalia | Przepisy transponujące zapewniają obowiązywanie czterech zasad[88]. | Portugalski organ ds. ochrony danych. |
| Rumunia | Brak transpozycji. | |
| Słowenia[89]: | Przepisy transponujące zapewniają obowiązywanie czterech zasad. | Komisarz ds. informacji. |
| Słowacja[90] | Przepisy transponujące zapewniają obowiązywanie czterech zasad. | Ochronę danych osobowych nadzoruje krajowy organ regulacyjny i organ ds. polityki cenowej w obszarze łączności elektronicznej. |
| Finlandia | Przepisy transponujące wprowadzają wyraźnie jedynie wymóg niszczenia danych na koniec okresu zatrzymania[91]. | Zgodność działań operatora z przepisami dotyczącymi zatrzymywania danych nadzoruje fiński organ regulacyjny ds. łączności.<br>Nadzór nad tym, czy przetwarzanie danych osobowych jest ogólnie zgodne z prawem, pełni inspektor ochrony danych. |
| Szwecja | Brak transpozycji. | |

82 Artykuł 12 ust. 5, art. 66 ust. 8 i 9 ustawy o łączności elektronicznej, zmienionej dnia 14 listopada 2009 r.

83 Artykuł 1 ust. 5 ustawy z dnia 24 lipca 2010 r.

84 Artykuł 157 ustawy C/2003 zmienionej ustawą CLXXIV/2007; art. 2 rozporządzenia 226/2003; oraz ustawa LXIII/1992 w sprawie ochrony danych.

85 Artykuły 24 i 25, Legal Notice 198/2008; art. 40 lit. b) ustawa o ochronie danych.(Cap.440).

86 Artykuł 13 ust. 5 ustawy o telekomunikacji; pełny tytuł protokołu o współpracy brzmi następująco: *Samenwerkingsovereenkomst tussen Agentschap Telecom en het College bescherming persoonsgegevens met het oog op de wijzigingen in de Telecommunicatiewet naar aanleiding van de Wet bewaarplicht telecommunicatiegegevens.*

87 Artykuł 180a i 180e ustawy o telekomunikacji.

88 Artykuły 7 ust. 1i 5 oraz art.11 ustawy 32/2008; art. 53 i 54 ustawy o ochronie danych osobowych.

89 Artykuł 107a ust. 6 i art. 107c ustawy o łączności elektronicznej.

90 Artykuł 59a ustawy o łączności elektronicznej; art. S33 ustawy nr 428/2002 o ochronie danych osobowych.

91 Artykuł 16 ust. 3 ustawy o łączności elektronicznej;

| Tabela 4: ochrona danych i bezpieczeństwo danych oraz organy nadzorujące | | |
|---|---|---|
| *Państwo członkowskie* | *Ochrona danych i krajowe przepisy dotyczące bezpieczeństwa danych* | *Organ nadzoru* |
| Zjednoczone Królestwo | Przepisy transponujące zapewniają obowiązywanie czterech zasad[92]. | Zatrzymywanie lub przetwarzanie danych z zakresu łączności (lub jakichkolwiek innych danych osobowych) oraz odpowiednie kontrole dotyczące ochrony danych leżą w gestii komisarza ds. informacji.<br>Nabywanie danych z zakresu łączności realizowane w oparciu o ustawę RIPA jest nadzorowane przez komisarza ds. podsłuchu (sędzia wyższej rangi – urzędujący lub emerytowany).<br>Trybunał Dochodzeniowy rozpatruje skargi dotyczące niewłaściwego wykorzystania danych, jeżeli dostęp do nich nastąpił na podstawie przepisów transponujących (RIPA). |

Transpozycja artykułu 7 jest niespójna. Zatrzymywane dane mogą być bardzo osobiste lub mieć szczególnie chroniony charakter; w trakcie całego procesu należy w sposób spójny i przejrzysty stosować wysokie normy ochrony danych i bezpieczeństwa danych, w odniesieniu do ich przechowywania, pobierania i wykorzystywania, w celu minimalizacji ryzyka naruszenia prywatności i utrzymania zaufania obywateli. Komisja rozważy warianty zwiększenia bezpieczeństwa danych oraz norm ochrony danych, w tym wprowadzenie rozwiązań zgodnych z zasadą domyślnej ochrony prywatności w celu zagwarantowania, by standardy te spełniane były zarówno w zakresie przechowywania, jak i przesyłania danych. Uwzględni ona również zalecenia dotyczące minimalnych gwarancji oraz technicznych i organizacyjnych środków bezpieczeństwa poczynione przez Grupę Roboczą Art. 29 w sprawozdaniu dotyczącym drugiego etapu egzekwowania[93].

### 4.7. Dane statystyczne (art. 10)

Państwa członkowskie mają obowiązek dostarczać Komisji roczne statystki na temat zatrzymywania danych, obejmujące:

– przypadki, w których właściwym organom udzielone zostały informacje zgodnie z odpowiednim prawem krajowym;

– czas, jaki upłynął między datą zarejestrowania zatrzymywanych danych, a datą wniosku o przekazanie danych złożonego przez właściwy organ (tzn. wiek danych); oraz

– przypadki, w których wnioski nie mogły zostać zrealizowane.

Zwracając się o statystyki na podstawie tego przepisu, Komisja poprosiła państwa członkowskie o udostępnienie szczegółowych informacji na temat poszczególnych przypadków występowania z wnioskami o dane. Niemniej jednak udostępnione dane statystyczne różniły się pod względem zakresu i szczegółowych aspektów: niektóre państwa członkowskie rozróżniały w swoich odpowiedziach między różnymi rodzajami połączeń, niektóre wskazywały na wiek danych w momencie składania wniosku, natomiast inne przedstawiały jedynie statystyki roczne bez szczegółowego podziału. Dziewiętnaście państw

[92] Artykuł 6 rozporządzenia o zatrzymywaniu danych.

[93] Opinia 3/2006 Grupy Roboczej Art. 29 (WP119); sprawozdanie 01/2010.

członkowskich[94] udostępniło statystyki dotyczące liczby wniosków o dane za rok 2009 i 2008; znalazły się wśród nich Irlandia, Grecja i Austria, gdzie składane są wnioski o dane mimo braku przepisów transponujących, jak również Republika Czeska i Niemcy, gdzie przepisy o zatrzymywaniu danych zostały uchylone. Siedem spośród państw członkowskich, które dokonały transpozycji dyrektywy, nie dostarczyło statystyk, chociaż Belgia przekazała szacunkową liczbę wniosków składanych każdego roku o dane telefoniczne (300 000).

Wiarygodne dane jakościowe i ilościowe mają zasadnicze znaczenie dla wykazania konieczności i wartości środków bezpieczeństwa, takich jak zatrzymywanie danych. Uznano to w planie działania w zakresie statystyki dotyczącej przestępczości i wymiaru sprawiedliwości w sprawach karnych z roku 2006[95], który obejmował cel w postaci opracowania metod regularnego gromadzenia danych zgodnie z dyrektywą oraz uwzględniania statystyk w bazie danych Eurostatu (pod warunkiem, że spełniają one kryteria jakościowe). Spełnienie tego celu nie było możliwe, biorąc pod uwagę, że większość państw członkowskich dokonała pełnej transpozycji dyrektywy dopiero w dwóch ostatnich latach i zastosowała różne interpretacje co do źródła danych statystycznych. Komisja w swoim przyszłym wniosku dotyczącym rewizji ram zatrzymywania danych, obok przeglądu planu działania w zakresie statystyk, będzie zmierzać do opracowania nadających się do praktycznego stosowania wskaźników pomiarowych oraz procedur sprawozdawczych, które umożliwiają przejrzyste i rzeczowe monitorowanie zatrzymywania danych, i które nie nakładają nadmiernych obciążeń na systemy wymiaru sprawiedliwości w sprawach karnych oraz organy ścigania.

### 4.8. Transpozycja w państwach EOG

Przepisy dotyczące zatrzymywania danych obowiązują także na Islandii, w Liechtensteinie i w Norwegii[96].

### 4.9. Decyzje trybunałów konstytucyjnych w sprawie przepisów transponujących

W październiku 2009 r. rumuński Trybunał Konstytucyjny, w marcu 2010 r. niemiecki federalny Trybunał Konstytucyjny, a w marcu 2011 r. czeski Trybunał Konstytucyjny uchyliły ustawy transponujące dyrektywę w ich jurysdykcji na tej podstawie, że są one sprzeczne z konstytucją. Trybunał rumuński[97] uznał, że ingerencja w prawa podstawowe może być dopuszczalna, gdy jest realizowana z poszanowaniem pewnych reguł oraz gdy wiąże się z odpowiednimi i wystarczającymi zabezpieczeniami przed potencjalnie arbitralnym działaniem państwa. Jednakże w oparciu o orzecznictwo Europejskiego Trybunału Praw Człowieka[98] rumuński trybunał uznał, że przepisy transponujące mają zbyt nieprecyzyjny zakres i cel oraz przewidują niedostateczne gwarancje, stwierdzając, że „stały obowiązek

---

94 Republika Czeska, Dania, Niemcy, Estonia, Irlandia, Grecja, Hiszpania, Francja, Cypr, Łotwa, Litwa, Malta, Niderlandy, Austria, Polska, Słowenia, Słowacja, Finlandia, Zjednoczone Królestwo.

95 Komunikat Komisji (2006) 437, „Opracowanie kompleksowej i spójnej strategii UE w zakresie statystyk dotyczących przestępczości i wymiaru sprawiedliwości w sprawach karnych: plan działania UE na lata 2006–2010".

96 Na Islandii ustawą transponującą jest ustawa telekomunikacyjna 81/2003 (zmieniona w kwietniu 2005 r.); w Liechtensteinie jest to ustawa telekomunikacyjna z 2006 r. W Norwegii przepisy transponujące zostały zatwierdzone w dniu 5 kwietnia 2011 r. i ustawa oczekuje obecnie na sankcję królewską.

97 Orzeczenie rumuńskiego Trybunału Konstytucyjnego nr 1258 z dnia 8 października 2009 r.

98 ECtHR, Rotaru przeciwko Rumunii z 2000 r., Sunday Times przeciwko Zjednoczonemu Królestwu z 1979 r. oraz Prince Hans-Adam of Liechtenstein przeciwko Rumunii z 2001 r.

prawny" zatrzymywania wszelkich danych o ruchu przez okres sześciu miesięcy jest nie do pogodzenia z prawami do prywatności i swobody wyrazu zapisanymi w art. 8 Europejskiej konwencji praw człowieka.

Niemiecki Trybunał Konstytucyjny[99] stwierdził, że zatrzymywanie danych sprawia wrażenie nadzoru, który mógłby przeszkadzać w swobodnej realizacji praw podstawowych. Trybunał wyraźnie uznał, że zatrzymywanie danych w ściśle określonym celu i przy zapewnieniu wystarczająco wysokiego poziomu bezpieczeństwa danych nie musi koniecznie oznaczać naruszenia niemieckiej ustawy zasadniczej. Równocześnie jednak Trybunał podkreślił, że zatrzymywanie takich danych stanowi poważne ograniczenie prawa do prywatności i dlatego powinno być dopuszczalne w szczególnie ograniczonej liczbie przypadków, oraz że okres zatrzymywania wynoszący sześć miesięcy stanowi górną granicę (*an der Obergrenze*) okresu, który może zostać uznany za proporcjonalny (pkt 215). Wniosek o dane należy składać jedynie wtedy, gdy zaistniało podejrzenie poważnego przestępstwa lub gdy istnieje zagrożenie dla bezpieczeństwa państwa, a pobierania danych należy zakazać w przypadku niektórych rodzajów połączeń (np. związanych z potrzebami emocjonalnymi lub socjalnymi), które uznaje się za poufne. Dane powinny być także kodowane przy zapewnieniu przejrzystego nadzoru wykorzystania danych.

Czeski Trybunał Konstytucyjny[100] uchylił przepisy transponujące na tej podstawie, że jako środek, który stanowił ingerencję w prawa podstawowe, przepisy transponujące zostały sformułowane bez dostatecznej precyzji i jasności. Trybunał skrytykował zbyt wąski zakres zasady celowości w porównaniu ze skalą i zakresem obowiązku zatrzymywania danych. Orzekł on, że definicja organów uprawnionych do uzyskiwania dostępu do danych i ich wykorzystywania oraz procedury uzyskiwania takiego dostępu nie zostały w przepisach transponujących określone na tyle jasno, by zapewnić integralność i poufność danych. Indywidualny obywatel nie został zatem wyposażony w dostateczne gwarancje i zabezpieczenia przed potencjalnymi nadużyciami ze strony organów publicznych. Trybunał nie skrytykował samej dyrektywy, zaznaczając, że zapewniała ona Republice Czeskiej dostateczną swobodę, by mogła ona dokonać transpozycji zgodnie z konstytucją. Równocześnie jednak w niewiążącej części orzeczenia Trybunał wyraził wątpliwości co do konieczności, efektywności i właściwości zatrzymywania danych o ruchu, biorąc pod uwagę pojawienie się nowych metod działań przestępczych, takich jak wykorzystywanie anonimowych kart SIM.

Te trzy państwa członkowskie rozważają obecnie, w jaki sposób dokonać ponownej transpozycji dyrektywy. Sprawy dotyczące zatrzymywania danych zostały również skierowane do trybunałów konstytucyjnych: w Bułgarii, co spowodowało rewizję ustawy transponującej; Cypru, w którym uznano, że nakazy sądowe wystawione na podstawie ustawy transponującej były niezgodne z konstytucją; oraz na Węgrzech, gdzie sprawa dotycząca braku określenia w ustawie transponującej prawnych celów przetwarzania danych jest w toku[101].

---

99 Bundesverfassungsgericht, 1 BvR 256/08 z dnia 2 marca 2010 r., pkt 1-345.

100 Wyrok czeskiego Trybunału Konstytucyjnego z dnia 22 marca w sprawie ustawy nr 127/2005 oraz dekretu nr 485/2005; zob. w szczególności pkt 45-48, 50-51 oraz 56.

101 Bułgarski Naczelny Trybunał Administracyjny, orzeczenie nr 13627 z dnia 11 grudnia 2008 r.; Sąd Najwyższy Cypru sprawa odwoławcza nr 65/2009, 78/2009, 82/2009 i 15/2010-22/2010 z dnia 1 lutego 2011 r.; węgierska skarga konstytucyjna została złożona przez węgierską Unię Swobód Obywatelskich w dniu 2 czerwca 2008 r.

Komisja rozważy kwestie podniesione w orzecznictwie krajowym w swoim przyszłym wniosku dotyczącym rewizji ram zatrzymywania danych.

### 4.10. Dalsze wdrażanie dyrektywy

Komisja oczekuje od państw członkowskich, które nie dokonały dotąd pełnej transpozycji dyrektywy, albo które nie przyjęły jeszcze przepisów zastępujących przepisy transponujące uchylone przez sądy krajowe, do uczynienia tego jak najszybciej. W przeciwnym przypadku Komisja zastrzega sobie prawo skorzystania z kompetencji przysługujących jej na mocy Traktatów UE. Dwa państwa członkowskie, które nie dokonały transpozycji dyrektywy (Austria i Szwecja), zostały już uznane przez Trybunał Sprawiedliwości za winne naruszenia zobowiązań wynikających z prawa UE[102]. W kwietniu 2011 r. Komisja zdecydowała się skierować sprawę Szwecji ponownie do Trybunału ze względu na brak podporządkowania się wyrokowi w sprawie C-185/09, występując o nałożenie sankcji finansowych na mocy art. 260 Traktatu o funkcjonowaniu Unii Europejskiej, w następstwie decyzji szwedzkiego parlamentu o odłożeniu przyjęcia przepisów transponujących o 12 miesięcy. Komisja nadal ściśle monitoruje sytuację w Austrii, która ustanowiła terminarz szybkiego przyjęcia przepisów transponujących.

## 5. ROLA ZATRZYMANYCH DANYCH W WYMIARZE SPRAWIEDLIWOŚCI W SPRAWACH KARNYCH I EGZEKWOWANIU PRAWA

W poniższej sekcji podsumowano funkcje zatrzymywanych danych opisane przez państwa członkowskie w materiałach nadesłanych przez nie na potrzeby oceny.

### 5.1. Ilość zatrzymanych danych, do których uzyskały dostęp właściwe organy krajowe

Wzrasta ilość przesyłanych danych telekomunikacyjnych, jak również ilość wniosków o dostęp do danych o ruchu. Dane statystyczne dostarczone przez 19 państw członkowskich za 2008 lub 2009 r. wskazują, że ogółem w UE każdego roku przedkłada się 2 mln wniosków, przy czym istnieją znaczne różnice między państwami członkowskimi – od mniej niż 100 wniosków rocznie (na Cyprze) do ponad miliona (Polska). Zgodnie z informacjami o rodzaju danych, których dotyczą wnioski, dostarczonymi przez 12 państw członkowskich za 2008 lub 2009 r., najczęściej wnioski dotyczyły telefonii komórkowej (zob. tabele 5, 8 i 12). Statystyki nie wskazują dokładnie celu, w jakim złożone zostały poszczególne wnioski. Republika Czeska, Łotwa i Polska zaznaczyły, że w przypadku danych o telefonii komórkowej właściwe organy musiały przesyłać ten sam wniosek do każdego z głównych operatorów telefonii komórkowej, dlatego faktyczna liczba wniosków w każdej sprawie była dużo niższa niż sugerowałyby to statystyki.

Brakuje prostego wytłumaczenia tych różnic, chociaż na pewno rolę odgrywają tu takie czynniki jak liczba ludności, dominujące tendencje w przestępczości, stosowanie zasady celowości oraz warunki i koszty pozyskania danych.

---

[102] Odpowiednio sprawy C-189/09 i C-185/09.

## 5.2. Wiek danych, do których uzyskano dostęp

Na podstawie danych statystycznych dostarczonych przez dziewięć państw członkowskich[103] za 2008 r. (zob. zestawienie w tabeli 5 oraz dalsze szczegóły w załączniku), ok. 90% danych, do których uzyskano dostęp, miało sześć miesięcy lub mniej, a ok. 70% danych trzy miesiące lub mniej w momencie składania (pierwotnego) wniosku o dostęp.

**Tabela 5: Zestawienie wieku zatrzymanych danych, do których uzyskano dostęp w dziewięciu państwach członkowskich, które przedstawiły statystyki z podziałem na rodzaje danych za 2008 r.**

| *Wiek* | *Telefonia stacjonarna* | *Telefonia komórkowa* | *Dane internetowe* | *Razem* |
|---|---|---|---|---|
| Poniżej 3 miesięcy | 61% | 70% | 56% | 67% |
| 3-6 miesięcy | 28% | 18% | 19% | 19% |
| 6-12 miesięcy | 8% | 11% | 18% | 12% |
| Ponad rok | 3% | 1% | 7% | 2% |

Według większości państw członkowskich wykorzystanie danych mających powyżej trzech lub nawet sześciu miesięcy jest rzadsze, może mieć jednak kluczowe znaczenie. Zazwyczaj można je było przyporządkować do jednej z trzech kategorii. Po pierwsze, o dane związane z Internetem występowano zazwyczaj później w porównaniu z innymi formami dowodów w trakcie dochodzenia karnego. Analiza danych pochodzących z telefonii stacjonarnej i komórkowej często prowadzi do odkrycia potencjalnych nowych tropów, co z kolei skutkuje dalszymi wnioskami, o starsze dane. Jeżeli przykładowo w trakcie dochodzenia analizując dane pochodzące z telefonii stacjonarnej lub komórkowej, natrafiono na określone nazwisko, śledczy mogą dążyć do zidentyfikowania adresu protokołu internetowego (IP) wykorzystywanego przez tę osobę oraz ustalić, z kim dana osoba kontaktowała się w danym okresie, wykorzystując swój adres IP. W takim scenariuszu śledczy przypuszczalnie wystąpią o dane umożliwiające prześledzenie także komunikacji z innymi adresami IP oraz tożsamości osób, które korzystały z tych adresów IP.

Po drugie, dochodzenia prowadzone w sprawie bardzo poważnych przestępstw, szeregu przestępstw, przestępczości zorganizowanej oraz zamachów terrorystycznych opierały się zazwyczaj na starszych danych – co wynikało z dłuższego okresu planowania tych przestępstw – w celu identyfikacji modeli przestępczego zachowania oraz stosunków między współsprawcami przestępstwa, jak również w celu ustalenia zamiaru przestępczego. Działania powiązane ze skomplikowanymi przestępstwami finansowymi wykrywane są często dopiero po upływie szeregu miesięcy. Po trzecie, w wyjątkowych okolicznościach państwa występowały o dane o ruchu przechowywane w innym państwie członkowskim, które może zazwyczaj przekazać te dane za zgodą sędziego w odpowiedzi na wniosek o pomoc prawną skierowany przez sędziego w występującym państwie członkowskim. Udzielanie tego rodzaju pomocy prawnej może okazać się długotrwałym procesem, co tłumaczy dlaczego niektóre z danych, o które wystąpiono, pochodziły sprzed ponad 6 miesięcy.

[103] Republika Czeska, Dania, Estonia, Irlandia, Hiszpania, Cypr, Łotwa, Malta, Zjednoczone Królestwo.

### 5.3. Transgraniczne wnioski o zatrzymane dane

Postępowanie przygotowawcze i sądowe w sprawach karnych może wiązać się z analizą dowodów i zeznań świadków pochodzących z więcej niż jednego państwa członkowskiego lub zdarzeń, które miały tam miejsce. Ze statystyk dostarczonych przez państwa członkowskie wynika, że mniej niż 1% wniosków o zatrzymane dane dotyczyło danych przechowywanych w innym państwie członkowskim. Organy ścigania zaznaczyły, że wolą występować o dane od operatorów krajowych, którzy mogli zgromadzić właściwe dane, niż uruchamiać procedurę wzajemnej pomocy prawnej, która może okazać się czasochłonna bez gwarancji uzyskania dostępu do danych. Decyzja ramowa 2006/960/WSiSW w sprawie uproszczenia wymiany informacji i danych wywiadowczych między organami ścigania państw członkowskich Unii Europejskiej[104], która określa terminy na udzielenie informacji w odpowiedzi na wniosek innego państwa członkowskiego, nie ma zastosowania, ponieważ zatrzymane dane uznawane są za informacje uzyskane w trybie przymusowym, które pozostają poza zakresem tego instrumentu. Tym niemniej żadne z państw członkowskich ani organów ścigania nie wezwało do dalszego ułatwienia takiej współpracy transgranicznej.

### 5.4. Wartość zatrzymanych danych w postępowaniach przygotowawczych i sądowych w sprawach karnych

Chociaż bezwzględna liczba zgłoszonych wniosków o dane niekoniecznie odzwierciedla wartość danych w indywidualnych dochodzeniach karnych, państwa członkowskie na ogół stwierdzały, że zatrzymywanie danych było co najmniej wartościowe, a w niektórych przypadkach niezbędne[105] do zapobiegania przestępczości i zwalczania jej, w tym ochrony pokrzywdzonych oraz oczyszczenia z zarzutów niewinnych osób będących podmiotem postępowania karnego. Wyroki skazujące opierają się na przyznaniu się do winy, zeznaniach świadków lub dowodach kryminalistycznych. Zgodnie z relacjami zatrzymane dane telekomunikacyjne okazały się niezbędne do uzyskania kontaktu ze świadkami zdarzenia, których w inny sposób nie udało by się zidentyfikować, oraz do uzyskania dowodów, lub też tropów pozwalających ustalić współodpowiedzialność za przestępstwo. Niektóre państwa członkowskie[106] stwierdziły dalej, że wykorzystanie zatrzymanych danych umożliwiło oczyszczenie z zarzutów osób podejrzewanych o przestępstwo, bez potrzeby uciekania się do innych metod nadzoru, takich jak podsłuch czy rewizja domowa, które mogłyby zostać uznane za bardziej ingerencyjne.

W UE nie ma ogólnej definicji „poważnego przestępstwa", nie ma też zatem ogólnounijnych statystyk w zakresie skali poważnej przestępczości oraz postępowań przygotowawczych i sądowych prowadzonych w takich sprawach, chociaż dane na temat przestępczości i wymiaru sprawiedliwości są regularnie publikowane. Z danych przekazanych przez 19 państw członkowskich, które przekazały choć niektóre dane za 2009 lub 2008 r., wynika, że łączna

---

104 Decyzja ramowa Rady 2006/960/WSiSW z dnia 18 grudnia 2006 r. w sprawie uproszczenia wymiany informacji i danych wywiadowczych między organami ścigania państw członkowskich Unii Europejskiej, Dz.U. L 386 z 18.12.2006. , s. 89-100 oraz Dz.U. L 200 z 1.8.2007, s. 637-648.

105 Republika Czeska uznała, że zatrzymywanie danych jest „całkowicie niezbędne w znacznej liczbie spraw". Węgry stwierdziły, że jest ono „niezbędne do regularnych działań [organów ścigania]". Słowenia zaznaczyła, że brak zatrzymanych danych „sparaliżowałby działalność organów ścigania". Agencja policyjna Zjednoczonego Królestwa określiła dostępność danych o ruchu jako „absolutnie kluczową dla prowadzenia dochodzeń w sprawie zagrożeń terrorystycznych i poważną przestępczością".

106 Niemcy, Polska, Słowenia, Zjednoczone Królestwo.

liczba wniosków o zatrzymane dane wyniosła ok. 2,6 mln. Na tle najnowszych statystyk dotyczących przestępczości i wymiaru sprawiedliwości w sprawach karnych dostępnych w odniesieniu do tych 19 państw członkowskich – które odnoszą się do wszystkich zgłoszonych przestępstw, nie tylko poważnych – można stwierdzić, że na każdego funkcjonariusza policji przypadały nieco ponad dwa wnioski, lub też 11 wniosków na każde 100 odnotowanych przestępstw[107].

Na podstawie dostarczonych statystyk i ilustrujących przykładów, wiążących wykorzystanie zatrzymanych historycznych danych komunikacyjnych z liczbą wyroków skazujących i uniewinniających, przypadków umorzenia postępowania oraz zapobieżenia przestępstwu, można wyciągnąć szereg wniosków jeżeli chodzi o rolę i wartość zatrzymanych danych w dochodzeniu karnym.

*Uzyskiwanie śladów dowodowych*

Po pierwsze zatrzymane dane umożliwiają ustalenie śladów dowodowych prowadzących do przestępstwa. Są one używane do podważenia lub potwierdzenia innych form dowodów dotyczących działalności i powiązań między podejrzanymi. Zarówno organy ścigania, jak i oskarżeni wykorzystywali w szczególności dane dotyczące lokalizacji w celu wykluczenia możliwości przebywania przez podejrzanych w miejscu popełnienia przestępstwa oraz weryfikacji alibi. Dowody te mogą zatem doprowadzić do wykluczenia osób z kręgu podejrzanych, eliminując tym samym potrzebę stosowania bardziej ingerencyjnych metod dochodzeniowych, lub też prowadzą do wyroków uniewinniających na rozprawie. Belgia wskazała na przykład skazania w 2008 r. sprawców porwania w celu wymuszenia jednego z pracowników sądu karnego w Antwerpii, w którym to przypadku dane o lokalizacji pozwoliły na połączenie działalności prowadzonej przez nich w trzech różnych miastach i były dla przysięgłych decydującym dowodem ich udziału. W innej sprawie dotyczącej morderstwa przypisywanego gangowi motocyklowemu w 2007 r. dane o lokalizacji uzyskane z telefonów komórkowych sprawców wykazały, że przebywali oni na obszarze, na którym popełniono morderstwo, prowadząc do częściowego przyznania się do winy[108]. Według Belgii, Irlandii i Zjednoczonego Królestwa dochodzenie w sprawie niektórych przestępstw związanych z komunikowaniem się za pośrednictwem Internetu może być prowadzone *wyłącznie* poprzez zatrzymanie danych: przykładowo groźby karalne wysunięte na czatach internetowych nie pozostawiają żadnego innego śladu oprócz danych o ruchu w cyberprzestrzeni. Podobna sytuacja dotyczy przestępstw popełnianych za pośrednictwem telefonu. Węgry i Polska podały przykład oszustw popełnianych na szkodę starszych osób pod koniec 2009 r. i na początku 2010 r., których sprawcy telefonowali do tych osób, podając się za członków ich rodziny potrzebujących pożyczki, których udało się zidentyfikować wyłącznie dzięki zatrzymanym danym telefonicznym.

*Wszczynanie dochodzeń*

Po drugie odnotowano przypadki, w których, w braku dowodów kryminalistycznych lub zeznań naocznych świadków, dochodzenie mogło być wszczęte jedynie dzięki zapoznaniu się

---

107 W 2007 r. w UE-27 było 1,7 mln funkcjonariuszy policji, z czego 1,2 mln w 19 państwach członkowskich, które dostarczyły statystyk w zakresie wniosków o zatrzymane dane. W 2007 r. policja w UE odnotowała 29,2 mln przestępstw, z czego 24 mln w 19 państwach członkowskich, które dostarczyły statystyk. (Źródło: Eurostat, 2009 r.).

108 National Policing Improvement Agency (Zjednoczone Królestwo), *The Journal of Homicide and Major Incident Investigation*, Tom 5, Nr 1, wiosna 2009, s. 39-51.

z zatrzymanymi danymi. Niemcy podały przykład zabójstwa funkcjonariusza policji, kiedy to sprawca uciekł samochodem ofiary, który następnie porzucił. Udało się ustalić, że wykonał on następnie telefon w celu uzyskania alternatywnego środka transportu. Nie było żadnych dowodów kryminalistycznych ani naocznych świadków pozwalających ustalić tożsamość mordercy i organy ścigania mogły prowadzić dochodzenie wyłącznie na podstawie tych danych telekomunikacyjnych. W powiązanych z Internetem przypadkach seksualnego wykorzystywania dzieci zatrzymanie danych było warunkiem udanego dochodzenia. Obok innych technik dochodzeniowych zatrzymane dane umożliwiają identyfikację osób pobierających treści ze scenami wykorzystywania dzieci[109] oraz ułatwiają identyfikację i ratowanie dzieci będących ofiarami tych praktyk. Republika Czeska podała, że bez dostępu do zatrzymanych danych internetowych niemożliwe byłoby rozpoczęcie dochodzeń w ramach „Operacji Vilma" skierowanej przeciwko sieci osób rozpowszechniających pornografię dziecięcą i korzystających z niej. Na szczeblu ogólnounijnym w skutecznej realizacji operacji „Ratunek" (wspieranej przez Europol) pod względem ochrony dzieci przed nadużyciami przeszkadzał brak przepisów transponujących normy o zatrzymaniu danych, który uniemożliwił niektórym państwom członkowskim prowadzenie dochodzeń wobec członków rozległej międzynarodowej sieci pedofilskiej na podstawie adresów IP, które mogą pochodzić z okresu do jednego roku.

W dochodzeniach dotyczących cyberprzestępstw pierwszym śladem jest często adres IP. Organy ścigania na podstawie danych o ruchu mogą zidentyfikować abonenta, któremu przypisany jest dany adres IP przed rozstrzygnięciem, czy można wszcząć dochodzenie. Policjanci mogą też dzięki temu ostrzec potencjalne ofiary cyberataków: kiedy policji udaje się przechwycić serwer kontrolno-sterujący używany przez operatorów botnetu, widzą oni jedynie adresy IP powiązane z tym serwerem. Jednak dzięki wglądowi do zatrzymanych danych policja może zidentyfikować i ostrzec potencjalne ofiary, do których należą te adresy IP.

*Zatrzymane dane stanowią integralny element dochodzenia karnego*

Po trzecie, chociaż organy ścigania i sądy w większości państw członkowskich nie gromadzą statystyk w zakresie tego, jaki rodzaj dowodów okazał się kluczowy dla wydania wyroku skazującego lub uniewinniającego, zatrzymane dane stanowią integralny element postępowania przygotowawczego i sądowego w UE. Niektóre państwa członkowskie podały, że nie mogą ustalić, w jakim zakresie zatrzymane dane przyczyniły się do powodzenia postępowania przygotowawczego i sądowego, ponieważ sądy analizują wszystkie przedłożone im dowody i rzadko stwierdzają, że jeden element dowodu okazał się decydujący[110]. Niderlandy podały, że od stycznia do lipca 2010 r. historyczne dane o ruchu były decydującym czynnikiem w 24 wyrokach sądowych. Finlandia podała, że w 56% z 3405 wniosków zatrzymane dane okazały się „istotne" lub „kluczowe" dla wykrycia lub ścigania przestępstw. Zjednoczone Królestwo dostarczyło danych, które miały służyć zbadaniu wpływu zatrzymanych danych na postępowanie przed sądami karnymi; wynikało z nich, że w przypadku trzech agencji organów ścigania z tego państwa zatrzymane dane były potrzebne w

---

109 Projekt „Pomiary i analiza aktywności p2p w zakresie treści pedofilskich" wspierany w ramach programu „Bezpieczniejszy Internet" dostarczył precyzyjnych informacji na temat działalności pedofilskiej w systemie peer-to-peer eDonkey, umożliwiając identyfikację 178 000 (na 89 mln skontrolowanych użytkowników), którzy pobierali treści pedofilskie.

110 Belgia, Republika Czeska, Litwa.

większości, jeżeli nie we wszystkich dochodzeniach, które doprowadziły do wszczęcia postępowania sądowego lub skazania.

### 5.5. Ewolucja technologiczna i wykorzystywanie przedpłaconych kart SIM

Po czwarte, organy ścigania muszą dotrzymywać kroku postępom technologicznym wykorzystywanym do popełnienia przestępstwa lub ułatwiającym jego popełnienie. Zatrzymanie danych należy do narzędzi dochodzeniowych niezbędnych do tego, by sprostać współczesnym wyzwaniom w zakresie przestępczości, wobec ich różnorodności, ilości i tempa, w sposób kontrolowany i efektywny pod względem kosztów. Szereg coraz powszechniejszych form komunikacji znajduje się poza zakresem zastosowania dyrektywy. Wirtualne sieci prywatne (VPNs), przykładowo na uniwersytetach i w dużych korporacjach, umożliwiają wielu uczestnikom uzyskiwanie dostępu do Internetu za pośrednictwem jednej bramy i z wykorzystaniem tego samego adresu IP. Obecnie jednak wprowadzana jest nowa technologia umożliwiająca przydzielenie adresów indywidualnym użytkownikom VPN.

Udział użytkowników telefonii komórkowej korzystających z usług przedpłaconych jest zróżnicowany. Niektóre państwa członkowskie stwierdziły, że anonimowe, przedpłacone karty SIM, zwłaszcza zakupione w innym państwie członkowskim, mogą być wykorzystywane także przez osoby zamieszane w działalność przestępczą dla uniknięcia identyfikacji w dochodzeniu karnym[111]. Sześć państw członkowskich (Dania, Hiszpania, Włochy, Grecja, Słowacja i Bułgaria) przyjęły środki wymagające rejestracji przedpłaconych kart SIM. Te i inne państwa członkowskie (Polska, Cypr i Litwa) opowiedziały się za ogólnounijnymi środkami na rzecz obowiązkowej rejestracji tożsamości użytkowników przedpłaconych usług. Nie dostarczono żadnych danych co do skuteczności tych krajowych środków. Wskazano natomiast na potencjalne ograniczenia, przykładowo w przypadku kradzieży tożsamości lub w przypadku gdy karta SIM została nabyta przez osobę trzecią albo użytkownik wykorzystuje kartę nabytą w państwie trzecim. Ogólnie Komisja nie jest przekonana o tym, że na obecnym etapie istnieje potrzeba działania w tej dziedzinie na szczeblu UE.

## 6. WPŁYW ZATRZYMYWANIA DANYCH NA OPERATORÓW I KONSUMENTÓW

### 6.1. Operatorzy i konsumenci

We wspólnym oświadczeniu Komisja i pięć dużych organizacji branżowych stwierdziły, że skutki ekonomiczne dyrektywy były „znaczące” lub „ogromne” dla niewielkich usługodawców, ponieważ dyrektywa „nie pozostawia żadnej swobody manewru”[112]. Ośmiu operatorów przedłożyło bardzo różniące się między sobą szacunki kosztów kapitałowych i operacyjnych związanych z przestrzeganiem dyrektywy. Ich potwierdzeniem mogą być dane dotyczące kwot wypłacanych operatorom tytułem zwrotu poniesionych wydatków przedstawione przez cztery państwa członkowskie (zob. tabela 6).

W analizie przeprowadzonej przed transpozycją dyrektywy w większości państw członkowskich szacowano koszty ustanowienia systemu zatrzymywania danych przez

---

111 Konkluzje Rady w sprawie walki z wykorzystywaniem do celów przestępczych łączności elektronicznej i jej anonimowości

112 http://www.gsmeurope.org/documents/Joint_Industry_Statement_on_DRD.PDF

jednego dostawcę internetowego obsługującego bazę 500 tys. klientów na ok. 375 240 EUR w pierwszym roku oraz 9 870 EUR kosztów operacyjnych miesięcznie po tym okresie[113], natomiast koszty ustanowienia systemu pobierania danych na 131 190 EUR, gdzie koszty operacyjne wynosiłyby 28 960 EUR. Jednakże niemiecki Trybunał Konstytucyjny w wyroku z dnia 2 marca 2010 r. orzekł, że nałożenie obowiązku przechowywania danych „nie było nadmiernym obciążeniem dla zainteresowanych usługodawców ani też nie powodowało nadmiernych kosztów finansowych dla przedsiębiorstw w wyniku obowiązku przechowywania"[114]. Koszty zatrzymania jednej jednostki danych są odwrotnie proporcjonalne do wielkości operatora oraz poziomu normalizacji przyjętego przez państwa członkowskie w zakresie współdziałania z operatorami[115].

Większość operatorów w odpowiedzi udzielonej na kwestionariusz Komisji nie było w stanie ocenić wpływu dyrektywy na konkurencję, ceny detaliczne dla konsumentów lub inwestycje w nową infrastrukturę i usługi.

Brakuje dowodów na jakikolwiek wymierny lub istotny wpływ dyrektywy na ceny dla konsumentów usług łączności elektronicznej. Żaden z przedstawicieli konsumentów nie zabrał głosu w trakcie konsultacji publicznych w 2009 r. Badanie przeprowadzone w Niemczech w imieniu organizacji społeczeństwa obywatelskiego wykazało, że konsumenci zamierzali zmienić sposób korzystania z narzędzi komunikacyjnych i unikać używania usług łączności elektronicznej w pewnych okolicznościach, jednakże brakuje dowodów potwierdzających, że taka zmiana faktycznie nastąpiła w tym państwie lub ogólnie w UE[116].

Komisja zamierza ocenić wpływ przyszłych zmian w dyrektywie na branżę i konsumentów, w tym, ewentualnie, poprzez specjalny kwestionariusz Eurobarometru, by zbadać opinie społeczne.

### 6.2. Zwrot wydatków

Dyrektywa nie reguluje zwrotu wydatków poniesionych przez operatorów w związku z obowiązkiem zatrzymywania danych. Wydatki te można podzielić na:

(a) *wydatki operacyjne*, tzn. koszty prowadzenia działalności lub stałe wydatki związane z funkcjonowaniem przedsiębiorstwa, urządzenia, składnika, elementu wyposażenia lub środka; oraz

(b) *wydatki kapitałowe*, tzn. koszty poniesione w celu uzyskania korzyści w przyszłości lub koszty stworzenia lub dostarczenia trwałych części produktu lub systemu, mogące obejmować wydatki na pracowników oraz wydatki związane z funkcjonowaniem środka, np. koszty najmu czy mediów.

Wszystkie państwa członkowskie zapewniają określoną formę zwrotu, jeżeli o dane występuje się w kontekście postępowania przed sądem karnym. Dwa państwa członkowskie

---

113 Wilfried Gansterer & Michael Ilger, Data Retention – The EU Directive 2006/24/EC from a Technological Perspective, Wiedeń: Verlag Medien und Recht, 2008

114 Bundesverfassungsgericht, 1 BvR 256/08 z dnia 2 marca 2010 r., pkt 299.

115 http://www.etsi.org/website/technologies/lawfulinterception.aspx

116 Badanie zostało przeprowadzone przez Forsa na zlecenie AK Vorratsdatenspeicherung. http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf

podały, że zwracają zarówno wydatki operacyjne, jak i kapitałowe. Sześć państw zwraca jedynie wydatki operacyjne. Komisji nie zgłoszono żadnego innego systemu zwrotów. Szczegółowe informacje zawiera tabela 6.

| **Tabela 6: państwa członkowskie zwracające wydatki** | | | |
|---|---|---|---|
| **Państwo członkowskie** | **Wydatki operacyjne** | **Wydatki kapitałowe** | **Roczne koszty zwrotu (mln EUR)** |
| Belgia | Tak | Nie | 22 (2008) |
| Bułgaria | Nie | Nie | - |
| Republika Czeska | Brak transpozycji [117] | | |
| Dania | Tak | Nie | - |
| Niemcy | Brak transpozycji | | |
| Estonia | Tak | Nie | - |
| Irlandia | Nie | Nie | - |
| Grecja | Nie | Nie | - |
| Hiszpania | Nie | Nie | - |
| Francja | Tak | Nie | - |
| Włochy | - | - | - |
| Cypr | Nie | Nie | - |
| Łotwa | Nie | Nie | - |
| Litwa | Tak, na wniosek i jeżeli zwrot jest uzasadniony | Nie | - |
| Luksemburg | Nie | Nie | - |
| Węgry | Nie | Nie | - |
| Malta | Nie | Nie | - |
| Niderlandy | Tak | Nie | - |
| Austria | Brak transpozycji | | |
| Polska | Nie | Nie | - |
| Portugalia | Nie | Nie | - |
| Rumunia | Brak transpozycji | | |
| Słowenia | Nie | Nie | - |
| Słowacja | Nie | Nie | - |
| Finlandia | Tak | Tak | 1 |
| Szwecja | Brak transpozycji | | |
| Zjednoczone Królestwo | Tak | Tak | 55 (łączny zwrot wydatków poniesionych w ciągu trzech lat) |

Z powyższych danych wynikałoby, że nie udało się w pełni osiągnąć wyznaczonego w dyrektywie celu dotyczącego stworzenia równych warunków dla operatorów w UE. Komisja rozważy warianty maksymalnego zmniejszenia przeszkód w funkcjonowaniu rynku wewnętrznego poprzez zagwarantowanie, by operatorom systematycznie zwracano wydatki poniesione w związku z wypełnianiem obowiązków w zakresie przetrzymywania danych, zwracając szczególną uwagę na małych i średnich operatorów.

[117] Przed uchyleniem czeskiej ustawy transponującej Republika Czeska zwracała zarówno wydatki operacyjne, jak i kapitałowe, podając, że w 2009 r. dokonała zwrotu wydatków na kwotę 6,8 mln EUR.

## 7. IMPLIKACJE ZATRZYMYWANIA DANYCH DLA PRAW PODSTAWOWYCH

### 7.1. Podstawowe prawa do prywatności i ochrony danych osobowych

Zatrzymanie danych stanowi ograniczenie prawa do życia prywatnego i ochrony danych osobowych stanowiących prawa podstawowe w UE[118]. Zgodnie z art. 52 ust. 1 Karty praw podstawowych ograniczenie to musi „być przewidziane ustawą i szanować istotę tych praw i wolności, z zastrzeżeniem zasady proporcjonalności" i być uzasadnione jako konieczne i rzeczywiście odpowiadające celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób. W praktyce oznacza to, że wszelkie ograniczenia muszą[119]:

(a) być sformułowane w sposób jasny i przewidywalny;

(b) być konieczne do osiągnięcia celu leżącego w interesie ogólnym lub ochrony praw i swobód innych;

(c) być proporcjonalne do założonego celu; oraz

(d) zachować istotę danego prawa podstawowego.

Także w art. 8 ust. 2 Europejskiej konwencji praw człowieka uznano, że ingerencja władzy publicznej w korzystanie z prawa do prywatności może być uzasadniona, jeżeli jest konieczna ze względu na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub zapobieganie przestępczości[120]. Artykuł 15 ust. 1 dyrektywy o „e-prywatności" oraz motywy w dyrektywie o zatrzymywaniu danych powtarzają te zasady leżące u podstaw unijnego podejścia do kwestii zatrzymywania danych.

W kolejnych orzeczeniach Europejskiego Trybunału Sprawiedliwości i Europejskiego Trybunału Praw Człowieka rozwinięto teorię warunków, jakie spełniać muszą wszelkie ograniczenia prawa do prywatności. Orzeczenia te mają znaczenie w kontekście ewentualnych zmian w dyrektywie, szczególnie jeżeli chodzi o warunki dostępu do zatrzymanych danych i korzystania z nich.

*Wszelkie ograniczenia prawa do prywatności muszą być precyzyjne i zapewniać przewidywalność*

W sprawie *Österreichischer Rundfunk* Europejski Trybunał Sprawiedliwości orzekł, że wszelkie ingerencje w prawo do prywatności muszą być „wystarczająco precyzyjnie, aby umożliwić adresatom tej ustawy odpowiednie dostosowanie ich zachowania…oraz tym samym odpowiadać wymogowi przewidywalności".

---

118 Artykuły 7 i 8 Karty praw podstawowych Unii Europejskiej (Dz.U. C 83 z 30.3.2010, s. 389) gwarantują każdemu prawo do „ochrony danych osobowych, które go dotyczą". Prawo to zapisano także w art. 16 Traktatu o funkcjonowaniu Unii Europejskiej (Dz.U. C 83 z 30.3.2010, s. 1).

119 Zob. listę kontrolną Komisji dotycząca praw podstawowych w odniesieniu do wszelkich wniosków ustawodawczych w komunikacie Komisji COM (2010) 573/4 „Strategia skutecznego wprowadzania w życie Karty praw podstawowych przez Unię Europejską".

120 Artykuł 8 Konwencji o ochronie praw człowieka i podstawowych wolności (ETS nr 5), Rada Europy, 4.11.1950 r.

*Wszelkie ograniczenia prawa do prywatności muszą być konieczne i niezbędne są minimalne gwarancje*

W sprawie Copland przeciwko Zjednoczonemu Królestwa, która dotyczyła monitorowania przez państwo rozmów telefonicznych, poczty elektronicznej i korzystania z Internetu, Europejski Trybunał Praw Człowieka orzekł, że takie ograniczenie prawa do prywatności może być uznane za konieczne, jeżeli jest oparte na właściwych przepisach krajowych[121]. W sprawie S. i Marper przeciwko Zjednoczonemu Królestwu, która dotyczyła zatrzymywania profili DNA lub odcisków palców osób, wobec których wydano wyrok uniewinniający lub których sprawy umorzono przed wydaniem wyroku skazującego, Trybunał orzekł, że takie ograniczenie prawa do prywatności może być uzasadnione jedynie wtedy, gdy stanowi odpowiedź na naglącą potrzebę społeczną, jeżeli było proporcjonalne do zakładanego celu oraz jeżeli przyczyny podane przez władzę publiczną mające je uzasadniać są istotne i dostateczne[122]. Podstawowe zasady ochrony danych wymagają, by zatrzymywanie danych było proporcjonalne w stosunku do celu gromadzenia, a okres ich przechowywania był ograniczony[123]. W przypadku podsłuchu telefonicznego, niejawnej obserwacji oraz niejawnego gromadzenia danych wywiadu kryminalnego „konieczne jest posiadanie jasnych, szczegółowych przepisów regulujących zakres i stosowanie środków, jak również minimalnych gwarancji dotyczących, między innymi, długości czasu, przechowywania, korzystania, dostępu osób trzecich, procedur służących zachowaniu integralności i poufności danych oraz procedur ich niszczenia, zapewniając tym samym dostateczne gwarancje przed ryzykiem nadużyć i arbitralności".

*Wszelkie ograniczenia prawa do prywatności muszą być proporcjonalne do chronionego interesu powszechnego*

Podobnie Europejski Trybunał Sprawiedliwości, w orzeczeniu w sprawie Schecke & Eifert dotyczącej opublikowania wszystkich beneficjentów subsydiów rolnych w Internecie[124] stwierdził, że, jak się wydaje, unijny prawodawca nie podjął wszelkich właściwych kroków by wyważyć, z jednej strony, konieczność poszanowania esencji prawa do prywatności i, z drugiej strony, ochronę interesu powszechnego (przejrzystość) uznawanego przez UE. W szczególności Trybunał ustalił, że prawodawcy nie rozważyli innych metod, które odpowiadałyby zakładanemu celowi, równocześnie stanowiąc mniejszą ingerencję w prawo beneficjentów subsydiów do poszanowania ich życia prywatnego oraz ochrony ich danych osobowych. W związku z tym Trybunał orzekł, że prawodawcy przekroczyli granice proporcjonalności, a „ograniczenia ochrony danych powinny ograniczać się do tego, co absolutnie konieczne".

### 7.2. Krytyka zasady zatrzymywania danych

Szereg organizacji społeczeństwa obywatelskiego napisało do Komisji, wskazując, że zatrzymanie danych stanowi, co do zasady, nieuzasadnione i niepotrzebne ograniczenie prawa

---

121 Copland przeciwko Zjednoczonemu Królestwu, wyrok Europejskiego Trybunału Praw Człowieka, Strasburg, 3.4.2007, s. 9.

122 Marper przeciwko Zjednoczonemu Królestwu, wyrok Europejskiego Trybunału Praw Człowieka, Strasburg, 4.12.2008, s. 31.

123 Marper, s. 30.

124 C-92/09 Volker i Markus Schecke GbR przeciwko Land Hessen oraz C-93/09 Eifert przeciwko Land Hessen i Bundesanstalt für Landwirtschaft und Ernährung, 9.11.10.

osób fizycznych do prywatności. Uważają oni, że niedobrowolne „blankietowe i masowe" zatrzymywanie danych telekomunikacyjnych osób fizycznych dotyczących ruchu, lokalizacji i abonentów jest bezprawnym ograniczeniem praw podstawowych. W związku ze sprawą wniesioną do sądu w jednym z państw członkowskich (Irlandia) przez jedną z grup obrony praw obywatelskich, kwestia legalności dyrektywy zostanie przypuszczalnie przekazana do rozstrzygnięcia Europejskiemu Trybunałowi Sprawiedliwości[125]. Również Europejski Inspektor Ochrony Danych Osobowych wyraził wątpliwości co do konieczności środka.

### 7.3. Wezwania do poprawy bezpieczeństwa danych i norm ochrony danych

W sprawozdaniu Grupy Roboczej Art. 29 na temat drugiego etapu egzekwowania argumentowano, że przechowywanie jakichkolwiek danych o ruchu nierozerwalnie wiąże się z ryzykiem naruszenia poufności komunikacji i swobody wyrażania opinii. Grupa skrytykowała niektóre aspekty krajowych środków wdrażających, w szczególności rejestrowanie danych, okresy zatrzymania, rodzaj zatrzymywanych danych oraz zabezpieczenie danych. Grupa podała przypadki, w których, poza zakresem dyrektywy, zatrzymano szczegółowe informacje o *treści* komunikatów internetowych, w tym adresy IP odbiorów oraz adresy URL stron internetowych, nagłówki wiadomości elektronicznych i listę odbiorców otrzymujących e-mail „do wiadomości" (z pola DW). Dlatego też wezwała do wyjaśnienia, że kategorie opisane w dyrektywie są wyczerpujące, i że nie powinno się nakładać na operatorów żadnych dodatkowych obowiązków w zakresie zatrzymywania danych.

Europejski Inspektor Ochrony Danych stwierdził, że dyrektywa „nie doprowadziła do harmonizacji krajowych przepisów" i że wykorzystanie zatrzymywanych danych nie jest ściśle ograniczone do zwalczania poważnej przestępczości[126]. Zaznaczył on, że unijny instrument zawierający normy dotyczące obowiązkowego zatrzymywania danych powinien, jeżeli wykazana zostanie taka potrzeba, zawierać także normy dotyczące dostępu organów ścigania oraz dalszego wykorzystywania. Inspektor wezwał również UE do przyjęcia całościowych ram legislacyjnych, które nie tylko nakładają na operatorów obowiązek zatrzymywania danych, lecz także regulują sposób korzystania przez państwa członkowskie z danych na potrzeby egzekwowania prawa, by „zagwarantować obywatelom pewność prawną".

Organy ochrony danych w ogólności wskazywały, że zatrzymywanie danych samo w sobie pociąga za sobą ryzyko naruszeń prywatności, w której to kwestii dyrektywa nie przewiduje środków zaradczych na szczeblu UE, zamiast tego nakładając na państwa członkowskie obowiązek zapewnienia, by przestrzegano krajowe przepisy o ochronie danych. Chociaż nie ma konkretnych przykładów poważnych naruszeń prywatności, ryzyko naruszenia bezpieczeństwa danych pozostanie i może wzrosnąć wraz z rozwojem technologii oraz nowymi tendencjami w zakresie form komunikacji, niezależnie od tego, czy dane przechowywane są do celów handlowych czy bezpieczeństwa, na terytorium UE i poza nim, chyba że ustanowione zostaną dalsze gwarancje.

---

125 W dniu 5 maja 2010 r. irlandzki High Court uznał wniosek Digital Rights Ireland Limited o skierowanie pytania prejudycjalnego do Europejskiego Trybunału Sprawiedliwości na mocy art. 267 Traktatu o funkcjonowaniu Unii Europejskiej.

126 Przemówienie Petera Hustinxa podczas konferencji „Taking on the Data Retention Directive", 3 grudnia 2010 r.

## 8. WNIOSKI I ZALECENIA

W sprawozdaniu ukazano szereg korzyści wynikających z obecnego reżimu zatrzymywania danych w UE, jak również obszary, w których może on zostać udoskonalony. UE przyjęła dyrektywę w okresie, w którym istniało duże poczucie zagrożenia atakami terrorystycznymi. Planowana przez Komisję ocena skutków zapewnia możliwość oceny zatrzymywania danych w UE pod kątem konieczności i proporcjonalności, w odniesieniu do i w interesie bezpieczeństwa wewnętrznego, sprawnego funkcjonowania rynku wewnętrznego oraz większego poszanowania prywatności i podstawowego prawa do ochrony danych osobowych. Wniosek Komisji dotyczący rewizji ram zatrzymywania danych powinien być oparty na następujących wnioskach i zaleceniach.

### 8.1. UE powinna wspierać i regulować zatrzymywanie danych jako jeden ze środków bezpieczeństwa

Większość państw członkowskich przyjmuje stanowisko, że unijne przepisy o zatrzymywaniu danych są nadal potrzebne, jako narzędzie organów ścigania oraz w celu ochrony ofiar i funkcjonowania systemów wymiaru sprawiedliwości w sprawach karnych. Dowody na potwierdzenie tej opinii, w formie statystyk i przykładów przekazanych przez państwa członkowskie, są skromne w niektórych aspektach, jednak ukazują one bardzo istotną rolę zatrzymanych danych w dochodzeniu karnym. Dane te zawierają wartościowe ślady oraz dowody wykorzystywane do zapobiegania przestępstwom i ścigania ich oraz dla zagwarantowania wymiaru sprawiedliwości w sprawach karnych. Ich wykorzystanie doprowadziło do wyroków skazujących za przestępstwa, których, bez zatrzymywania danych, nie udałoby się nigdy rozwikłać. Doprowadziło ono również do oczyszczenia z zarzutów niewinnych osób. Zharmonizowane przepisy w tej dziedzinie powinny gwarantować, by zatrzymywanie danych było skutecznym narzędziem zwalczania przestępczości, by sektor miał pewność prawną w kontekście sprawnego funkcjonowania rynku wewnętrznego oraz by na terytorium całej UE spójnie zapewniany był wysoki poziom ochrony prywatności i danych osobowych.

### 8.2. Nierówna transpozycja

W 22 państwach członkowskich obowiązują przepisy transponujące. Znaczna swoboda pozostawiona państwom członkowskim w zakresie przyjmowania środków zatrzymywania danych na mocy art. 15 ust. 1 dyrektywy w sprawie e-prywatności czyni ocenę dyrektywy o zatrzymywaniu danych bardzo problematyczną. Istnieją znaczne różnice między przepisami wdrażającymi w takich dziedzinach jak zasada celowości, dostęp do danych, okresy zatrzymania, ochrona danych oraz bezpieczeństwo danych i statystyki. Trzy państwa członkowskie naruszyły dyrektywę, ponieważ ustanowione przez nie przepisy transponujące zostały uchylone przez ich właściwe trybunały konstytucyjne. Dwa inne państwa członkowskie nie dokonały jeszcze transpozycji. Komisja będzie nadal współpracować z wszystkimi tymi państwami członkowskimi, by pomóc im w skutecznym wdrożeniu dyrektywy. Komisja będzie również nadal dbać o egzekwowanie prawa UE, w ostateczności wszczynając postępowania w sprawie uchybienia zobowiązaniom, jeżeli okaże się to konieczne.

### 8.3. Dyrektywa nie doprowadziła do pełnej harmonizacji podejścia do zatrzymywania danych ani nie zapewniła równych warunków operatorom

Dzięki dyrektywie obecnie w większości państw członkowskich dane są zatrzymywane. Dyrektywa sama w sobie nie gwarantuje natomiast, że zatrzymane dane są przechowywane, pobierane i wykorzystywane w zgodności z prawem do prywatności i ochroną danych osobowych. Odpowiedzialność za zagwarantowanie przestrzegania tych praw spoczywa na państwach członkowskich. Dyrektywa miała jedynie na celu częściową harmonizację podejścia do zatrzymywania danych. Dlatego nie jest zaskakujące, że brakuje wspólnego podejścia, czy to w kontekście szczególnych przepisów dyrektywy, takich jak zasada celowości i okres zatrzymywania, czy też jeżeli chodzi o aspekty leżące poza jej zakresem, takie jak zwrot wydatków. Jednakże poza stopniem zróżnicowania wyraźnie przewidzianym przez dyrektywę, różnice w krajowym stosowaniu systemu zatrzymywania danych powodowały znaczne trudności dla operatorów.

### 8.4. Operatorzy powinni w sposób spójny uzyskiwać zwrot poniesionych wydatków

Przedstawiciele sektora nadal borykają się z brakiem pewności prawnej. Obowiązek zatrzymania i pobierania danych powoduje znaczne koszty dla operatorów, w szczególności mniejszych, a operatorzy ponoszący takie koszty otrzymują ich zwrot w różnym stopniu, w zależności od danego państwa członkowskiego, przy czym nie ma dowodów na negatywny wpływ dyrektywy na sektor telekomunikacyjny w ogólności. Komisja rozważy sposoby zapewnienia spójnego systemu zwrotu wydatków operatorom.

### 8.5. Zagwarantowanie proporcjonalności w zintegrowanym procesie przechowywania, pobierania i wykorzystywania

Komisja dopilnuje, by wszelkie przyszłe projekty dotyczące zatrzymywania danych były zgodne z zasadą proporcjonalności oraz odpowiadały realizacji celu, jakim jest zwalczanie poważnej przestępczości i terroryzmu oraz nie wykraczały poza to, co jest niezbędne do jego osiągnięcia. Komisja uzna, że wszelkie wyjątki i ograniczenia w zakresie ochrony danych osobowych powinny mieć zastosowanie wyłącznie w niezbędnym zakresie. Komisja oceni bardzo dokładnie wpływ bardziej rygorystycznych regulacji w zakresie przechowywania danych o ruchu, uzyskiwania dostępu do nich oraz korzystania z nich na skuteczność i efektywność systemów wymiaru sprawiedliwości w sprawach karnych i egzekwowania prawa, na prywatność oraz koszty dla administracji publicznej i operatorów. W ocenie skutków należy zbadać w szczególności następujące dziedziny:

- spójne stosowanie zasady celowości w odniesieniu do zatrzymywania danych oraz określenie przestępstw, w przypadku których można uzyskiwać dostęp do danych i korzystać z nich;

- większa harmonizacja oraz ewentualne skrócenie okresów obowiązkowego zatrzymywania danych;

- zagwarantowanie niezależnego nadzoru nad wnioskami o uzyskanie dostępu oraz ogólnym reżimem zatrzymywania danych i uzyskiwania do nich dostępu we wszystkich państwach członkowskich;

- ograniczenie liczby organów upoważnionych do dostępu do danych;

- ograniczenie liczby kategorii danych, które powinny być zatrzymywane;
- wytyczne dotyczące technicznych i organizacyjnych środków bezpieczeństwa w zakresie uzyskiwania dostępu do danych, w tym procedur przekazywania;
- wytyczne dotyczące korzystania z danych, w tym zapobiegania eksploracji danych; oraz
- opracowanie nadających się do praktycznego stosowania wskaźników pomiarowych oraz procedur sprawozdawczych w celu ułatwienia porównywania oraz oceny przyszłego instrumentu.

Komisja rozważy również czy i w jaki sposób unijne podejście do zabezpieczania danych może stanowić uzupełnienie zatrzymywania danych.

W odniesieniu do „listy kontrolnej" w zakresie praw podstawowych oraz podejścia do zarządzania informacjami w obszarze wolności, bezpieczeństwa i sprawiedliwości[127] Komisja rozważy każdą z tych dziedzin w świetle zasad proporcjonalności oraz wymogu przewidywalności. Komisja zapewni również spójność z przeprowadzanym obecnie przeglądem unijnych ram ochrony danych[128].

### 8.6. Kolejne kroki

W świetle tej oceny Komisja zaproponuje rewizję obecnych ram zatrzymywania danych. Przedstawi ona szereg wariantów w konsultacji z organami ścigania, sędziami, przedstawicielami sektora i grupami konsumenckimi, organami ochrony danych oraz organizacjami społeczeństwa obywatelskiego. Komisja przeanalizuje jeszcze dokładniej publiczny odbiór kwestii zatrzymywania danych oraz wpływ tego procesu na zachowanie. Ustalenia te zostaną wykorzystane w ocenie skutków zidentyfikowanych wariantów strategicznych, które stanowić będą podstawę wniosku prawodawczego Komisji.

---

127 Zob. powyższy przepis dotyczący komunikatu w sprawie realizacji Karty praw podstawowych; „Przegląd zarządzania informacjami w przestrzeni wolności, bezpieczeństwa i sprawiedliwości", COM(2010)385, 20.07.2010 r.

128 COM (2010) 609 z 2010.11.4.

## Załącznik: Dodatkowe statystyki na temat zatrzymywania danych o ruchu

Uwagi do załącznika:

1. Wiek danych oznacza czas, jaki upłynął między datą zarejestrowania zatrzymywanych danych, a datą wniosku o przekazanie danych złożonego przez właściwy organ.

2. Dane związane z Internetem oznaczają dane dotyczące dostępu oraz poczty i telefonii internetowej.

3. W odniesieniu do statystyk dotyczących Republiki Czeskiej, Łotwy i Polski obowiązuje zastrzeżenie (zob. pkt 5.1).

### Statystyki przedłożone przez państwa członkowskie za 2008 r.

| Tabela 7: Wnioski o zatrzymane dane o ruchu z podziałem na wiek w 2008 r. | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Wiek danych, których dotyczył wniosek (miesiące)/państwo członkowskie** | **0-3** | **3-6** | **6-9** | **9-12** | **12-15** | **15-18** | **18-21** | **21-24** | **Suma** |
| Belgia | Nie przekazano danych | | | | | | | | |
| Bułgaria | Nie przekazano danych | | | | | | | | |
| Republika Czeska | 102691 | 18440 | 10110 | 319 | 0 | 0 | 0 | 0 | 131560 |
| Dania | 2669 | 672 | 185 | 37 | 23 | 2 | 7 | 4 | 3599 |
| Niemcy | 9363 | 2336 | 985 | 0 | 0 | 0 | 0 | 0 | 12684 |
| Estonia | 2773 | 733 | 157 | 827 | 0 | 0 | 0 | 0 | 4490 |
| Irlandia | 8981 | 2016 | 936 | 1855 | 90 | 85 | 78 | 54 | 14095 |
| Grecja | Nie dokonano podziału ze względu na wiek | | | | | | | | 584 |
| Hiszpania | 22629 | 15868 | 10298 | 4783 | 0 | 0 | 0 | 0 | 53578 |
| Francja | Nie dokonano podziału ze względu na wiek | | | | | | | | 503437 |
| Włochy | Nie przekazano danych | | | | | | | | |
| Cypr | 30 | 4 | 0 | 0 | 0 | 0 | 0 | 0 | 34 |
| Łotwa | 10539 | 2739 | 1368 | 1211 | 597 | 438 | 0 | 0 | 16892 |
| Litwa | 55735 | 23817 | 5251 | 512 | 0 | 0 | 0 | 0 | 85315 |
| Luksemburg | Nie przekazano danych | | | | | | | | |
| Węgry | Nie przekazano danych | | | | | | | | |
| Malta | 810 | 59 | 0 | 0 | 0 | 0 | 0 | 0 | 869 |
| Niderlandy | Nie dokonano podziału ze względu na wiek | | | | | | | | 85000 |
| Austria | Nie dokonano podziału ze względu na wiek | | | | | | | | 3093 |
| Polska | Nie przekazano danych | | | | | | | | |
| Portugalia | Nie przekazano danych | | | | | | | | |
| Rumunia | Nie przekazano danych | | | | | | | | |
| Słowenia | Nie dokonano podziału ze względu na wiek | | | | | | | | 2821 |
| Słowacja | Nie przekazano danych | | | | | | | | |
| Finlandia | 9134 | 1144 | 448 | 214 | 268 | | | | 4008 |
| Szwecja | Nie przekazano danych | | | | | | | | |
| Zjednoczone Królestwo | 315350 | 88339 | 34665 | 19398 | 6385 | 2973 | 1536 | 1576 | 470222 |
| **Suma** | **533504** | **156167** | **64403** | **29156** | **7095*** | **3230*** | **1353*** | **1366*** | **1392281** |

* z wyjątkiem Finlandii

| Tabela 8: Wnioski o zatrzymane dane o ruchu z podziałem na rodzaje w 2008 r. (in brackets number of cases where requests for data could not be met – if provided) | | | | |
|---|---|---|---|---|
| **Type of data/ Państwo członkowskie** | **Telefonia stacjonarna** | **Telefonia komórkowa** | **Dotyczące Internetu** | **Suma** |
| Belgia | Nie przekazano danych | | | |
| Bułgaria | Nie przekazano danych | | | |
| Republika Czeska | 4983 (131) | 125040 (2276) | 1537 (83) | 131560 (2490) |
| Dania | 192 (0) | 3273 (5) | 134 (0) | 3599 (5) |
| Niemcy | Nie dokonano podziału ze względu na rodzaj | | | 12684 (931) |
| Estonia | 4114 (1519) | 376 (7) | Nie przekazano danych | 4490 (1526) |
| Irlandia | 5317 (16) | 5873 (48) | 2905 (33) | 14095 (97) |
| Grecja | Nie dokonano podziału ze względu na rodzaj | | | 584 |
| Hiszpania | 4448 (0) | 40013 (0) | 9117 (0) | 53578 (0) |
| Francja | Nie dokonano podziału ze względu na rodzaj | | | 503437 |
| Włochy | Nie przekazano danych | | | |
| Cypr | 3 (0) | 31 (5) | 0 (0) | 34 (5) |
| Łotwa | 1602 (90) | 14238 (530) | 1052 (76) | 16892 (696) |
| Litwa | 765 (72) | 84550 (5657) | Nie przekazano danych | 85315 (5729) |
| Luksemburg | Nie przekazano danych | | | |
| Węgry | Nie przekazano danych | | | |
| Malta | 29 (0) | 748 (120) | 92 (13) | 869 (133) |
| Niderlandy | Nie dokonano podziału ze względu na rodzaj | | | 85000 |
| Austria | Nie dokonano podziału ze względu na rodzaj | | | 3093 |
| Polska | Nie przekazano danych | | | |
| Portugalia | Nie przekazano danych | | | |
| Rumunia | Nie przekazano danych | | | |
| Słowenia | Nie dokonano podziału ze względu na rodzaj | | | 2821 |
| Słowacja | Nie przekazano danych | | | |
| Finlandia | Nie dokonano podziału ze względu na rodzaj | | | 4008 |
| Szwecja | Nie przekazano danych | | | |
| Zjednoczone Królestwo | 90747 (0) | 329421 (0) | 50054 (0) | 470222 (0) |
| Suma | | | | 1392281 |

| **Tabela 9: Wnioski o zatrzymane dane o ruchu dotyczące *telefonii stacjonarnej*, które zostały przekazane, z podziałem na wiek, w 2008 r.** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Wiek danych, których dotyczył wniosek (miesiące)/państwo członkowskie** | **0-3** | **3-6** | **6-9** | **9-12** | **12-15** | **15-18** | **18-21** | **21-24** | **Suma** |
| Belgia | Nie przekazano danych | | | | | | | | |
| Bułgaria | Nie przekazano danych | | | | | | | | |
| Republika Czeska | 3669 | 916 | 143 | 124 | 0 | 0 | 0 | 0 | 4852 |
| Dania | 133 | 28 | 31 | 0 | 0 | 0 | 0 | 0 | 192 |
| Niemcy | Nie przekazano danych | | | | | | | | |
| Estonia | 1876 | 161 | 74 | 484 | 0 | 0 | 0 | 0 | 2595 |
| Irlandia | 4118 | 712 | 197 | 182 | 32 | 21 | 23 | 16 | 5301 |
| Grecja | Nie przekazano danych | | | | | | | | |
| Hiszpania | 1948 | 1431 | 741 | 328 | 0 | 0 | 0 | 0 | 4448 |
| Francja | Nie przekazano danych | | | | | | | | |
| Włochy | Nie przekazano danych | | | | | | | | |
| Cypr | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 |
| Łotwa | 698 | 213 | 167 | 193 | 104 | 137 | 0 | 0 | 1512 |
| Litwa | 251 | 442 | 0 | 0 | 0 | 0 | 0 | 0 | 693 |
| Luksemburg | Nie przekazano danych | | | | | | | | |
| Węgry | Nie przekazano danych | | | | | | | | |
| Malta | 28 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 29 |
| Niderlandy | Nie przekazano danych | | | | | | | | |
| Austria | Nie przekazano danych | | | | | | | | |
| Polska | Nie przekazano danych | | | | | | | | |
| Portugalia | Nie przekazano danych | | | | | | | | |
| Rumunia | Nie przekazano danych | | | | | | | | |
| Słowenia | Nie przekazano danych | | | | | | | | |
| Słowacja | Nie przekazano danych | | | | | | | | |
| Finlandia | Nie przekazano danych | | | | | | | | |
| Szwecja | Nie przekazano danych | | | | | | | | |
| Zjednoczone Królestwo | 54805 | 27052 | 5340 | 753 | 1135 | 437 | 1050 | 175 | 90747 |
| **Suma** | **67529** | **30956** | **6693** | **2064** | **1271** | **595** | **1073** | **191** | **110372** |

| **Tabela 10: Wnioski o zatrzymane dane o ruchu dotyczące *telefonii komórkowej*, które zostały przekazane, z podziałem na wiek, w 2008 r.** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Wiek danych, których dotyczył wniosek (miesiące)/państwo członkowskie** | **0-3** | **3-6** | **6-9** | **9-12** | **12-15** | **15-18** | **18-21** | **21-24** | **Suma** |
| Belgia | Nie przekazano danych | | | | | | | | |
| Bułgaria | Nie przekazano danych | | | | | | | | |
| Republika Czeska | 98232 | 17013 | 7518 | 1 | 0 | 0 | 0 | 0 | 122764 |
| Dania | 2433 | 628 | 143 | 33 | 20 | 1 | 7 | 3 | 3268 |
| Niemcy | Nie przekazano danych | | | | | | | | |
| Estonia | 248 | 58 | 35 | 28 | 0 | 0 | 0 | 0 | 369 |
| Irlandia | 4326 | 820 | 230 | 240 | 57 | 63 | 52 | 37 | 5825 |
| Grecja | Nie przekazano danych | | | | | | | | |
| Hiszpania | 17403 | 12114 | 7444 | 3052 | 0 | 0 | 0 | 0 | 40013 |
| Francja | Nie przekazano danych | | | | | | | | |
| Włochy | Nie przekazano danych | | | | | | | | |
| Cypr | 23 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 26 |
| Łotwa | 8928 | 2298 | 1085 | 746 | 394 | 257 | 0 | 0 | 13708 |
| Litwa | 55484 | 23375 | 14 | 20 | 0 | 0 | 0 | 0 | 78893 |
| Luksemburg | Nie przekazano danych | | | | | | | | |
| Węgry | Nie przekazano danych | | | | | | | | |
| Malta | 575 | 53 | 0 | 0 | 0 | 0 | 0 | 0 | 628 |
| Niderlandy | Nie przekazano danych | | | | | | | | |
| Austria | Nie przekazano danych | | | | | | | | |
| Polska | Nie przekazano danych | | | | | | | | |
| Portugalia | Nie przekazano danych | | | | | | | | |
| Rumunia | Nie przekazano danych | | | | | | | | |
| Słowenia | Nie przekazano danych | | | | | | | | |
| Słowacja | Nie przekazano danych | | | | | | | | |
| Finlandia | Nie przekazano danych | | | | | | | | |
| Szwecja | Nie przekazano danych | | | | | | | | |
| Zjednoczone Królestwo | 229375 | 52241 | 26228 | 16040 | 3333 | 521 | 339 | 1344 | 329421 |
| **Suma** | **417027** | **108603** | **42697** | **20160** | **3804** | **842** | **398** | **1384** | **594915** |

| **Tabela 11: Wnioski o zatrzymane dane o ruchu dotyczące *Internetu*, które zostały przekazane, z podziałem na wiek, w 2008 r.** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Wiek danych, których dotyczył wniosek (miesiące)/państwo członkowskie** | **0-3** | **3-6** | **6-9** | **9-12** | **12-15** | **15-18** | **18-21** | **21-24** | **Suma** |
| Belgia | Nie przekazano danych | | | | | | | | |
| Bułgaria | Nie przekazano danych | | | | | | | | |
| Republika Czeska | 737 | 412 | 137 | 168 | 0 | 0 | 0 | 0 | 1454 |
| Dania | 102 | 14 | 11 | 2 | 3 | 1 | 0 | 1 | 134 |
| Niemcy | Nie przekazano danych | | | | | | | | |
| Estonia | Nie przekazano danych | | | | | | | | |
| Irlandia | 492 | 460 | 498 | 1422 | 0 | 0 | 0 | 0 | 2872 |
| Grecja | Nie przekazano danych | | | | | | | | |
| Hiszpania | 3278 | 2323 | 2113 | 1403 | 0 | 0 | 0 | 0 | 9117 |
| Francja | Nie przekazano danych | | | | | | | | |
| Włochy | Nie przekazano danych | | | | | | | | |
| Cypr | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Łotwa | 424 | 150 | 75 | 219 | 74 | 34 | 0 | 0 | 976 |
| Litwa | Nie przekazano danych | | | | | | | | |
| Luksemburg | Nie przekazano danych | | | | | | | | |
| Węgry | Nie przekazano danych | | | | | | | | |
| Malta | 76 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 79 |
| Niderlandy | Nie przekazano danych | | | | | | | | |
| Austria | Nie przekazano danych | | | | | | | | |
| Polska | Nie przekazano danych | | | | | | | | |
| Portugalia | Nie przekazano danych | | | | | | | | |
| Rumunia | Nie przekazano danych | | | | | | | | |
| Słowenia | Nie przekazano danych | | | | | | | | |
| Słowacja | Nie przekazano danych | | | | | | | | |
| Finlandia | Nie przekazano danych | | | | | | | | |
| Szwecja | Nie przekazano danych | | | | | | | | |
| Zjednoczone Królestwo | 31170 | 9046 | 3097 | 2605 | 1917 | 2015 | 147 | 57 | 50054 |
| **Suma** | **36279** | **12408** | **5931** | **5819** | **1994** | **2050** | **147** | **58** | **64686** |

## Statystyki przedłożone przez państwa członkowskie za 2009 r.

| Tabela 12: Wnioski o zatrzymane dane z podziałem na wiek w 2009 r. | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Wiek danych, których dotyczył wniosek (miesiące)/państwo członkowskie** | **0-3** | **3-6** | **6-9** | **9-12** | **12-15** | **15-18** | **18-21** | **21-24** | **Suma** |
| Belgia | Nie przekazano danych | | | | | | | | |
| Bułgaria | Nie przekazano danych | | | | | | | | |
| Republika Czeska | 210975 | 56623 | 11620 | 1053 | 0 | 0 | 0 | 0 | 280271 |
| Dania | 2980 | 685 | 179 | 104 | 54 | 38 | 12 | 14 | 4066 |
| Niemcy | Nie przekazano danych | | | | | | | | |
| Estonia | 4299 | 1836 | 1210 | 1065 | 0 | 0 | 0 | 0 | 8410 |
| Irlandia | 8117 | 1652 | 805 | 297 | 168 | 134 | 69 | 41 | 11283 |
| Grecja | Nie przekazano danych | | | | | | | | |
| Hiszpania | 29775 | 19346 | 13999 | 6970 | 0 | 0 | 0 | 0 | 70090 |
| Francja | Nie dokonano podziału ze względu na wiek | | | | | | | | 514813 |
| Włochy | Nie przekazano danych | | | | | | | | |
| Cypr | 31 | 8 | 1 | 0 | 0 | 0 | 0 | 0 | 40 |
| Łotwa | 20758 | 2414 | 1088 | 796 | 565 | 475 | 0 | 0 | 26096 |
| Litwa | 30247 | 35456 | 5886 | 884 | 0 | 0 | 0 | 0 | 72473 |
| Luksemburg | Nie przekazano danych | | | | | | | | |
| Węgry | Nie przekazano danych | | | | | | | | |
| Malta | 3336 | 362 | 151 | 174 | 0 | 0 | 0 | 0 | 4023 |
| Niderlandy | Nie przekazano danych | | | | | | | | |
| Austria | Nie przekazano danych | | | | | | | | |
| Portugalia | Nie przekazano danych | | | | | | | | |
| Rumunia | Nie przekazano danych | | | | | | | | |
| Polska | 642327 | 178306 | 75525 | 52526 | 27098 | 23924 | 13984 | 34628 | 1048318 |
| Słowenia | Nie przekazano danych | | | | | | | | 1918 |
| Słowacja | Nie przekazano danych | | | | | | | | 5214 |
| Finlandia | 2000 | 1310 | 532 | 152 | 76 | 0 | 0 | 0 | 4070 |
| Szwecja | Nie przekazano danych | | | | | | | | |
| Zjednoczone Królestwo | Nie przekazano danych | | | | | | | | |
| **Suma** | **954845** | **297998** | **110996** | **64021** | **27961** | **24571** | **14065** | **34683** | **2051085** |

| Tabela 13: Wnioski o zatrzymane dane z podziałem na rodzaje w 2009 r. (w nawiasach liczba przypadków, w których wnioski o dane nie mogły zostać zrealizowane – jeżeli podano tę informację) | | | | |
|---|---|---|---|---|
| **Type of data/ Państwo członkowskie** | **Telefonia stacjonarna** | **Telefonia komórkowa** | **Dotyczące Internetu** | **Suma** |
| Belgia | Nie przekazano danych | | | |
| Bułgaria | Nie przekazano danych | | | |
| Republika Czeska | 13843 (934) | 256074 (9141) | 10354 (371) | 280271 (10446) |
| Dania | 133 (0) | 3771 (10) | 162 (1) | 4066 (11) |
| Niemcy | Nie przekazano danych | | | |
| Estonia | 6422 (2279) | 902 (21) | 1086 (468) | 8410 (2768) |
| Irlandia | 4542 (16) | 5239 (20) | 1502 (56) | 11283 (92) |
| Grecja | Nie przekazano danych | | | |
| Hiszpania | 5055 (0) | 56133 (0) | 8902 (0) | 70090 (0) |
| Francja | Nie dokonano podziału ze względu na rodzaj | | | 514813 |
| Włochy | Nie przekazano danych | | | |
| Cypr | 0 (0) | 23 (3) | 14 (0) | 40 (3) |
| Łotwa | 1672 (218) | 22796 (102) | 1628 (240) | 26096 (560) |
| Litwa | 1321 (0) | 51573 (6237) | 19579 (343) | 72473 (6580) |
| Luksemburg | Nie przekazano danych | | | |
| Węgry | Nie przekazano danych | | | |
| Malta | 156 (10) | 3693 (882) | 174 (10) | 4023 (902) |
| Niderlandy | Nie przekazano danych | | | |
| Austria | Nie przekazano danych | | | |
| Polska | Nie dokonano podziału ze względu na rodzaj | | | 1048318 |
| Portugalia | Nie przekazano danych | | | |
| Rumunia | Nie przekazano danych | | | |
| Słowenia | Nie przekazano danych | | | 1918 (48) |
| Słowacja | Nie przekazano danych | | | 5214 (157) |
| Finlandia | Nie przekazano danych | | | 4070 |
| Szwecja | Nie przekazano danych | | | |
| Zjednoczone Królestwo | Nie przekazano danych | | | |
| Suma | | | | 2051082 (1069885) |

| Tabela 14: Wnioski o zatrzymane dane dotyczące *telefonii stacjonarnej*, które zostały przekazane, z podziałem na wiek, w 2009 r. | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Wiek danych, których dotyczył wniosek (miesiące)/państwo członkowskie** | **0-3** | **3-6** | **6-9** | **9-12** | **12-15** | **15-18** | **18-21** | **21-24** | **Suma** |
| Belgia | Nie przekazano danych | | | | | | | | |
| Bułgaria | Nie przekazano danych | | | | | | | | |
| Republika Czeska | 9919 | 2907 | 47 | 36 | 0 | 0 | 0 | 0 | 12909 |
| Dania | 105 | 19 | 7 | 2 | 0 | 0 | 0 | 0 | 133 |
| Niemcy | Nie przekazano danych | | | | | | | | |
| Estonia | 2254 | 866 | 599 | 424 | 0 | 0 | 0 | 0 | 4143 |
| Irlandia | 3934 | 337 | 69 | 70 | 50 | 39 | 16 | 11 | 4526 |
| Grecja | Nie przekazano danych | | | | | | | | |
| Hiszpania | 2371 | 1492 | 844 | 348 | 0 | 0 | 0 | 0 | 5055 |
| Francja | Nie przekazano danych | | | | | | | | |
| Włochy | Nie przekazano danych | | | | | | | | |
| Cypr | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Łotwa | 744 | 253 | 157 | 143 | 68 | 89 | 0 | 0 | 1454 |
| Litwa | 469 | 773 | 73 | 6 | 0 | 0 | 0 | 0 | 1321 |
| Luksemburg | Nie przekazano danych | | | | | | | | |
| Węgry | Nie przekazano danych | | | | | | | | |
| Malta | 83 | 25 | 18 | 20 | 0 | 0 | 0 | 0 | 146 |
| Niderlandy | Nie przekazano danych | | | | | | | | |
| Austria | Nie przekazano danych | | | | | | | | |
| Polska | Nie przekazano danych | | | | | | | | |
| Portugalia | Nie przekazano danych | | | | | | | | |
| Rumunia | Nie przekazano danych | | | | | | | | |
| Słowenia | Nie przekazano danych | | | | | | | | |
| Słowacja | Nie przekazano danych | | | | | | | | |
| Finlandia | Nie przekazano danych | | | | | | | | |
| Szwecja | Nie przekazano danych | | | | | | | | |
| Zjednoczone Królestwo | Nie przekazano danych | | | | | | | | |
| **Suma** | **19879** | **6672** | **1814** | **1049** | **118** | **128** | **16** | **11** | **29687** |

| Tabela 15: Wnioski o zatrzymane dane dotyczące *telefonii komórkowej*, które zostały przekazane, z podziałem na wiek, w 2009 r. | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Wiek danych, których dotyczył wniosek (miesiące)/państwo członkowskie** | **0-3** | **3-6** | **6-9** | **9-12** | **12-15** | **15-18** | **18-21** | **21-24** | **Suma** |
| Belgia | Nie przekazano danych | | | | | | | | |
| Bułgaria | Nie przekazano danych | | | | | | | | |
| Republika Czeska | 197620 | 48841 | 472 | 0 | 0 | 0 | 0 | 0 | 246933 |
| Dania | 2777 | 639 | 162 | 98 | 47 | 19 | 12 | 7 | 3761 |
| Niemcy | Nie przekazano danych | | | | | | | | |
| Estonia | 318 | 397 | 96 | 70 | 0 | 0 | 0 | 0 | 881 |
| Irlandia | 3669 | 835 | 220 | 210 | 115 | 92 | 50 | 28 | 5219 |
| Grecja | Nie przekazano danych | | | | | | | | |
| Hiszpania | 24065 | 15648 | 11147 | 5273 | 0 | 0 | 0 | 0 | 56133 |
| Francja | Nie przekazano danych | | | | | | | | |
| Włochy | Nie przekazano danych | | | | | | | | |
| Cypr | 17 | 16 | 0 | 0 | 0 | 0 | 0 | 0 | 23 |
| Łotwa | 18832 | 1912 | 778 | 515 | 394 | 263 | 0 | 0 | 22694 |
| Litwa | 25713 | 19595 | 28 | 0 | 0 | 0 | 0 | 0 | 45336 |
| Luksemburg | Nie przekazano danych | | | | | | | | |
| Węgry | Nie przekazano danych | | | | | | | | |
| Malta | 2332 | 246 | 111 | 122 | 0 | 0 | 0 | 0 | 2811 |
| Niderlandy | Nie przekazano danych | | | | | | | | |
| Austria | Nie przekazano danych | | | | | | | | |
| Polska | Nie przekazano danych | | | | | | | | |
| Portugalia | Nie przekazano danych | | | | | | | | |
| Rumunia | Nie przekazano danych | | | | | | | | |
| Słowenia | Nie przekazano danych | | | | | | | | |
| Słowacja | Nie przekazano danych | | | | | | | | |
| Finlandia | Nie przekazano danych | | | | | | | | |
| Szwecja | Nie przekazano danych | | | | | | | | |
| Zjednoczone Królestwo | Nie przekazano danych | | | | | | | | |
| **Suma** | **275343** | **88119** | **13014** | **6288** | **556** | **374** | **62** | **35** | **383791** |

| **Tabela 16: Wnioski o zatrzymane dane dotyczące *Internetu*, które zostały przekazane, z podziałem na wiek, w 2009 r.** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Wiek danych, których dotyczył wniosek (miesiące)/państwo członkowskie** | **0-3** | **3-6** | **6-9** | **9-12** | **12-15** | **15-18** | **18-21** | **21-24** | **Suma** |
| Belgia | Nie przekazano danych | | | | | | | | |
| Bułgaria | Nie przekazano danych | | | | | | | | |
| Republika Czeska | 3369 | 4811 | 861 | 942 | 0 | 0 | 0 | 0 | 9983 |
| Dania | 98 | 27 | 10 | 4 | 4 | 7 | 0 | 1 | 151 |
| Niemcy | Nie przekazano danych | | | | | | | | |
| Estonia | 315 | 145 | 56 | 102 | 0 | 0 | 0 | 0 | 618 |
| Irlandia | 489 | 455 | 502 | 0 | 0 | 0 | 0 | 0 | 1446 |
| Grecja | Nie przekazano danych | | | | | | | | |
| Hiszpania | 3339 | 2206 | 2008 | 1349 | 0 | 0 | 0 | 0 | 8902 |
| Francja | Nie przekazano danych | | | | | | | | |
| Włochy | Nie przekazano danych | | | | | | | | |
| Cypr | 12 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 14 |
| Łotwa | 852 | 198 | 74 | 90 | 88 | 86 | 0 | 0 | 1388 |
| Litwa | 4060 | 15087 | 1 | 88 | 0 | 0 | 0 | 0 | 19236 |
| Luksemburg | Nie przekazano danych | | | | | | | | |
| Węgry | Nie przekazano danych | | | | | | | | |
| Malta | 150 | 14 | 0 | 0 | 0 | 0 | 0 | 0 | 164 |
| Niderlandy | Nie przekazano danych | | | | | | | | |
| Austria | Nie przekazano danych | | | | | | | | |
| Polska | Nie przekazano danych | | | | | | | | |
| Portugalia | Nie przekazano danych | | | | | | | | |
| Rumunia | Nie przekazano danych | | | | | | | | |
| Słowenia | Nie przekazano danych | | | | | | | | |
| Słowacja | Nie przekazano danych | | | | | | | | |
| Finlandia | Nie przekazano danych | | | | | | | | |
| Szwecja | Nie przekazano danych | | | | | | | | |
| Zjednoczone Królestwo | Nie przekazano danych | | | | | | | | |
| **Suma** | **12684** | **22945** | **3512** | **2575** | **92** | **93** | **0** | **1** | **41902** |