



**00070/2010/EN**

**WP 172**

**Raport 01/2010 z drugiej wspólnej akcji wdrożeniowej:**

**Zgodność dostawców usług telekomunikacyjnych i internetowych na poziomie krajowym z wymogami krajowego ustawodawstwa w sprawie danych o ruchu, wprowadzonego na podstawie art. 6 i 9 dyrektywy o prywatności i łączności elektronicznej 2002/58/WE i dyrektywy o zatrzymywaniu danych 2006/24/WE zmieniającej dyrektywę o prywatności i łączności elektronicznej**

**Przyjęte w dniu 13 lipca 2010 r.**

Niniejsza Grupa Robocza została powołana na mocy artykułu 29 Dyrektywy 95/46/WE. Jest to niezależny europejski organ doradczy w sprawach ochrony danych i prywatności. Jego zadania opisane zostały w artykule 30 Dyrektywy 95/46/WE i artykule 15 Dyrektywy 2002/58/WE.

## Streszczenie

- Akcja wdrożeniowa została podjęta przez Grupę Roboczą art. 29 w celu zbadania zgodności z przepisami wprowadzonymi na mocy dyrektywy 2006/24/WE, z uwzględnieniem zaleceń i uwag zawartych przez Grupę Roboczą w poprzednich opiniach na ten temat.
- Wdrażanie wspomnianej powyżej dyrektywy przez dostawców usług łączności elektronicznej i usług internetowych wiąże się z wysokim poziomem ryzyka, który wymaga zastosowania odpowiednich zabezpieczeń technicznych i organizacyjnych, ze względu na fakt, że dostępność danych o ruchu pozwala na ujawnienie preferencji, opinii i postaw i może jednocześnie zakłócać życie prywatne użytkowników i wywierać istotny wpływ na poufność połączeń oraz prawa podstawowe takie jak wolność wypowiedzi.
- Akcja oparta na kwestionariuszu oraz inspekcjach przeprowadzonych w siedzibach największych krajowych operatorów i dostawców usług internetowych, obejmujących znaczną część rynku, sprawdzała zastosowanie rozmaitych środków wdrożeniowych, ze szczególnym uwzględnieniem wprowadzonych zabezpieczeń.
- Istnieją znaczące rozbieżności co do zatrzymywanych kategorii danych o ruchu w internecie, okresy zatrzymywania także są różne w poszczególnych państwach członkowskich, natomiast w przypadku kategorii danych o ruchu w sieciach telefonicznych, sytuacja jest bardziej jednolita. Należy podkreślić, że w ustawodawstwie wielu państw członkowskich preferowany okres zatrzymywania danych jest krótszy od najdłuższego dozwolonego na mocy dyrektywy.
- W związku z powyższym, Grupa Robocza Art. 29 wyraża zaniepokojenie faktem, że dyrektywa nie została wprowadzona w jednolity sposób na poziomie krajowym. W szczególności, państwa członkowskie uznały, że dyrektywa pozostawia im dowolność w kwestii zakresu, tzn. nie określa, czy jej celem jest odejście od ogólnego obowiązku usuwania danych o ruchu po zakończeniu łączności elektronicznej, czy też upoważnienie do zatrzymywania danych wszystkich dostawców, którzy mieli już prawo do ich przechowywania dla celów określonych w art. 6(2) dyrektywy 2002/58. Druga z tych interpretacji jest właściwa w ocenie Grupy Roboczej Art. 29, została także potwierdzona w wydanym niedawno wyroku ETS w sprawie Irlandia przeciw Komisji (C-301/06).
- Zastosowane zabezpieczenia są różne w zależności od wielkości dostawcy; logiczne środki bezpieczeństwa nie zawsze są odpowiednie do wrażliwego charakteru informacji zawartych w danych o ruchu. Co istotne, procedury przekazywania w danych o ruchu na żądanie organów wymiaru sprawiedliwości są w znacznym stopniu niejednolite i obejmują szeroką gamę rozwiązań i różnych poziomów bezpieczeństwa przekazywania.
- Akcja ujawniła również, że jedynie kilka spośród państw członkowskich przesłało do Komisji żądane statystyki dotyczące wykorzystywania danych o ruchu zatrzymywanych na mocy dyrektywy i że rozpowszechnioną praktyką, szczególnie wśród drobnych operatorów, jest outsourcing, co budzi wątpliwości co do zgodności z wymogami ochrony danych.

Brak dostępnych statystyk utrudnia ocenę, czy cel dyrektywy został osiągnięty. Z raportu jasno wynika, że brak jest harmonizacji, a wdrażanie na poziomie krajowym nie jest jednolite. W oczekiwaniu na decyzję Komisji, czy dyrektywę należy poprawić lub uchylić, Grupa Robocza uznała za stosowne udzielenie szczegółowych zaleceń w celu zapewnienia większej harmonizacji, bezpieczniejszego przekazywania danych i zestandaryzowanych procedur przekazywania, obejmujących w szczególności:

- **Kategorie zatrzymywanych danych:** Lista danych o ruchu, które mają obowiązkowo być zatrzymywane, winna być traktowana jako zamknięta, a zatem, zgodnie z dyrektywą, na dostawców nie wolno nakładać obowiązku zatrzymywania żadnych innych danych.
- **Okresy zatrzymywania:** aby zapewnić wszystkim takie same warunki, maksymalny okres zatrzymywania powinien zostać skrócony i ograniczony do jednolitego terminu, którego winni przestrzegać wszyscy dostawcy w UE, jak stwierdzono w opinii WP113 Grupy Roboczej Art. 29. W szerszej perspektywie, Komisja winna ponownie rozważyć kwestie

związane z bezpieczeństwem danych o ruchu jako takich.

- **Techniczne i organizacyjne środki bezpieczeństwa:** określono dodatkowe środki (takie jak skuteczna identyfikacja i szczegółowe procedury zarządzania logami dostępu) oraz sugerowany standard przekazywania danych do organów wymiaru sprawiedliwości w celu przyspieszenia i zwiększenia rzetelności przekazywania danych, pozwalającego na zbieranie informacji statystycznych i rozliczania dostępu do danych. W związku z tym, pojęcie „poważnego przestępstwa” wymaga wyjaśnienia na poziomie krajowym w państwach członkowskich, a lista podmiotów upoważnionych do uzyskiwania dostępu do danych winna zostać przedstawiona wszystkim zainteresowanym stronom.

## **I. Informacje ogólne - wdrażanie**

Po publikacji pierwszego raportu o wdrażaniu dyrektywy o ochronie danych w maju 2003 roku, Komisja Europejska poprosiła Grupę Roboczą Art. 29 o rozważenie przeprowadzenia kontroli sektorowych na poziomie UE i ujednolicenie standardów w tym zakresie. Grupa Robocza, w deklaracji z dnia 25 listopada 2004 r., uznała promowanie jednolitego zastosowania ustawodawstwa w zakresie ochrony danych i harmonizację zgodności z nim za jeden ze swoich strategicznych, stałych celów.

Po pierwszej wspólnej akcji wdrożeniowej, której zakres objął prywatnych ubezpieczycieli zdrowotnych (raport 1/2007 przyjęty dnia 20 czerwca – WP137) i na podstawie zebranych przy tej okazji doświadczeń, Grupa Robocza postanowiła przeprowadzić drugą wspólną kontrolę i objąć nią wypełnianie na poziomie krajowym, przez dostawców usług telekomunikacyjnych i internetowych, zobowiązań nałożonych przez krajowe ustawodawstwo w zakresie danych o ruchu na podstawie art. 6 i 9 dyrektywy o prywatności i łączności elektronicznej 2002/58/WE oraz dyrektywy o zatrzymywaniu danych 2006/24/WE. Kontrola ta, stanowiąca jeden z priorytetów w Programie Prac, miała sprawdzić, czy zasady ochrony danych zharmonizowane na poziomie unijnym są stosowane w jednolity sposób.

W czerwcu 2008 roku Grupa Robocza udzieliła Zespołowi ds. Wdrażania (Enforcement Task Force – ETF) mandatu do zaplanowania i wykonania działań niezbędnych do przeprowadzenia akcji zgodnie z zasadami określonymi w dokumencie WP152.

Temat ten został wybrany na podstawie kombinacji kryteriów określonych w dokumencie WP101, choć Grupa Robocza zdawała sobie sprawę, że proces wdrażania dyrektywy o zatrzymywaniu danych nie został jeszcze zakończony – czy to z powodu opóźnień na poziomie krajowym, czy różnych terminów, w jakich państwa członkowskie miały wprowadzić obowiązek zatrzymywania również w odniesieniu do danych o ruchu w internecie.

Decyzja taka została podjęta ze względu na szczegółowy zakres dyrektywy 2006/24/WE, która odstępuje od ogólnej zasady określonej w dyrektywie o prywatności i łączności elektronicznej (2002/58/WE) – zgodnie z której art. 6(1) „Dane o ruchu dotyczące abonentów i użytkowników przetwarzane i przechowywane przez dostawcę publicznej sieci łączności lub publicznie dostępnych usług łączności elektronicznej muszą zostać usunięte lub uczynione anonimowymi, gdy nie są już potrzebne do celów transmisji komunikatu”. Ogólny obowiązek przechowywania danych o ruchu nakłada jedynie art. 6 ust. 2, jeśli dane takie są niezbędne „do celów naliczania opłat abonenta i opłat rozliczeń międzyoperatorskich” – jest to jednak dopuszczalne jedynie „do końca okresu, w którym rachunek może być zgodnie z prawem zakwestionowany lub w którym należy uiścić opłatę”. Należy przypomnieć, że celem dyrektywy 2006/24/WE (patrz art. 1) jest „zbliżenie przepisów (...) w zakresie zatrzymywania pewnych danych generowanych lub przetwarzanych [przez dostawców ogólnie dostępnych usług łączności elektronicznej lub publicznych sieci łączności]”. Dane takie mogą być przechowywane „do celu dochodzenia, wykrywania i ścigania poważnych przestępstw, określonych w ustawodawstwie każdego państwa członkowskiego”.

Ponadto, Grupa Robocza Art. 29 wydała trzy opinie w sprawie dyrektywy o zatrzymywaniu danych i projektów tego instrumentu prawnego. W opiniach tych, w szczególności w dokumentach WP113 i WP119, zgłoszono zastrzeżenia związane z faktem, że przepisy dyrektywy mają istotne skutki dla wszystkich obywateli europejskich i ich prywatności, jako że decyzja o zobowiązaniu dostawców usług telefonicznych i internetowych do zatrzymywania danych o ruchu wszystkich abonentów i użytkowników była – i jest – bezprecedensowa. Stanowi ona ingerencję w codzienne życie obywateli i może zagrażać podstawowym wartościom i prawom, z których korzystają i którymi cieszą się wszyscy obywatele Europy. W związku z powyższym, Grupa Robocza uznaje w swych opiniach za niezwykle istotne „zharmonizowaną interpretację i wdrażanie przepisów dyrektywy w celu zapewnienia obywatelom na terenie całej Unii Europejskiej tego samego poziomu ochrony”.

Grupa Robocza zaniepokojona była niejasnym celem opisanym jako „walka z poważną przestępczością”, biorąc pod uwagę brak wspólnej definicji poważnej przestępczości i brak jasnego określenia, które organy mają prawo dostępu do zatrzymywanych danych i jakie mechanizmy zatrzymywania danych stosują dostawcy, by zapewnić, że informacje będą dostępne jedynie dla celów określonych w dyrektywie 2006/24. Grupa Robocza Art. 29 zaleciła wprowadzenie zabezpieczeń co najmniej w odniesieniu do określenia celu, ograniczenia dostępu, minimalizacji danych, zakazu *data mining*, niezależnego/sądowego nadzoru nad upoważnieniem dostępu, zakazu korzystania przez dostawców z danych zatrzymywanych jedynie dla celów porządku publicznego na mocy dyrektywy o zatrzymywaniu – co doprowadziło do zalecenia utworzenia odrębnego systemu i zdefiniowania minimalnych standardów w zakresie środków bezpieczeństwa stosowanych przez dostawców.

Zatrzymane dane o ruchu pozwalają monitorować i śledzić całą sieć relacji danej osoby oraz tworzyć mapę jej ruchów i wykorzystywanych przy nich narzędzi. Wszelkie ograniczenia przysługującego obywatelom prawa do ochrony prywatności i danych osobowych winny być niezbędne, odpowiednie i proporcjonalne, dokonywać się w ramach demokratycznego społeczeństwa i służyć celom związanym z porządkiem publicznym – bezpieczeństwu i obronie narodowej lub śledzeniu, wykrywaniu i zwalczaniu przestępczości. Ograniczenia takie muszą co najmniej uwzględniać prawa, wolności i zasady zapisane w Karcie Praw Podstawowych UE oraz Europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności.

Analiza dotychczasowego sposobu wdrażania dyrektywy w prawie krajowym stanowić miała narzędzie sprawdzające zastrzeżenia Grupy Roboczej Art. 29 i osiągniętą do tej pory harmonizację.

Choć proces transpozycji przepisów UE jeszcze się nie zakończył, dzięki ustaleniom dokonany podczas akcji Grupa Robocza może zapewnić przydatne informacje Komisji, która ma przedstawić raport z oceny do dnia 15 września 2010 r.

## **II. Ramy prawne**

Jak już wspomniano, celem dyrektywy 2006/24/WE (dalej zwanej dyrektywą o zatrzymywaniu danych) jest harmonizacja krajowych przepisów w zakresie obowiązku zatrzymywania związanego z określonymi danymi o ruchu. W tym kontekście należy wspomnieć o art. 5, 6 i 7 dyrektywy o zatrzymywaniu danych, w których określone są kategorie zatrzymywanych danych, odpowiednie okresy zatrzymywania oraz środki ochrony danych i zabezpieczenia. Należy także wspomnieć, że zobowiązania nałożone przez dyrektywę mogą mieć – i mają – różny zakres w zależności od interpretacji i sposobu wdrażania art. 3 – czyli założenia, że dyrektywa odchodzi od ogólnej zasady, że dane o ruchu powinny zostać usunięte, kiedy nie są już potrzebne dla celów łączności (jak stanowi art. 6(1) dyrektywy 2002/58), bądź że jedynie wprowadza ona obowiązkowy okres zatrzymywania dla danych już zbieranych i przechowywanych przez dostawców dla celów wymienionych w art. 6(2) dyrektywy 2002/58 („do celów naliczania opłat abonenta i opłat rozliczeń międzyoperatorskich”).

Wobec powyższego należy przypomnieć, że postanowienia powyższych artykułów mają być stosowane przez państwa członkowskie w sposób restrykcyjny, tj. że prawo krajowe wdrażające dyrektywę może zostać wprowadzone przez te państwa jedynie jeśli jest całkowicie zgodne z wymogami określonymi w dyrektywie o zatrzymywaniu danych.

Należy również wspomnieć, że na mocy dyrektywy o zatrzymywaniu danych każde państwo członkowskie ma obowiązek wyznaczyć organ publiczny odpowiedzialny za monitorowanie zastosowania przepisów dyrektyw 95/46/WE i 2002/58/WE oraz środków ochrony i bezpieczeństwa danych wspomnianych w art. 7 dyrektywy o zatrzymywaniu – mają one stanowić minimum ochrony zapewnianej przez każde z państw członkowskich. Należy zauważyć, że dyrektywa o zatrzymywaniu danych jasno stanowi w art. 9, że takimi organami publicznymi mogą być krajowe organy ochrony danych i że ich działalność nadzorcza musi mieć w pełni niezależny charakter.

Ponadto, dyrektywa o zatrzymywaniu danych stanowi, że komisja winna do 15 września 2010 r. przedstawić Parlamentowi Europejskiemu i Radzie ocenę zastosowania dyrektywy i jej skutków, w celu ustalenia czy konieczne jest poprawienie dyrektywy uwzględniające, w szczególności, kategorie danych i okresy zatrzymywania. Dokonując tej oceny Komisja winna uwzględnić uwagi zgłoszone przez państwa członkowskie i Grupę Roboczą Art. 29 oraz statystyki w zakresie zatrzymywania danych, które państwa członkowskie muszą corocznie przedstawiać Komisji na podstawie art. 10 wspomnianej dyrektywy. Statystyki takie powinny obejmować przede wszystkim przypadki, w których informacje zostały przekazane do organów wymiaru sprawiedliwości, czas jaki upłynął od zatrzymania informacji do zażądania ich przez te organy oraz przypadki, w których dane nie mogły zostać udostępnione.

Jak już wspomniano, w momencie tworzenia niniejszego sprawozdania nie wszystkie państwa członkowskie wdrożyły dyrektywę o zatrzymywaniu. W niektórych krajach (Niemcy, Rumunia), Sąd Najwyższy lub Trybunał Konstytucyjny uznały, że przepisy wdrażające ustawę łamią zasady konstytucji.

### **III. Akcja wdrożeniowa**

#### **A. Uzasadnienie**

Akcja wdrożeniowa miała ocenić, jak dostawcy usług łączności elektronicznej i usług internetowych wdrożyli zobowiązania wynikające z dyrektywy o zatrzymywaniu danych w zakresie kategorii zatrzymywanych danych o ruchu (art. 5), okresów zatrzymywania (art. 6) oraz technicznych i organizacyjnych środków bezpieczeństwa (art. 7). W państwach członkowskich, które nie dokonały jeszcze transpozycji dyrektywy do prawa krajowego uwzględniono zobowiązania nałożone na dostawców przez obowiązujące prawo krajowe zgodne z dyrektywą o prywatności i łączności elektronicznej (dyrektywą 2002/58/WE) – w szczególności z jej art. 6 i 9. Odniesiono się także do minimalnego poziomu zabezpieczeń zaproponowanego w opinii 3/2006 (WP 119).

Zgodnie z dyrektywami 2006/24/WE i 2002/58/WE, zabezpieczenie danych osobowych winno być proporcjonalne do zagrożeń wynikających z przetwarzania tych danych i do charakteru tych danych. Z tego punktu widzenia, nie ulega wątpliwości, że wdrażanie dyrektywy o zatrzymywaniu danych niesie za sobą określone zagrożenia dla osób, których dane dotyczą, związane z charakterem danych o ruchu. Z tego względu inspekcje przeprowadzone przez członków Grupy Roboczej Art. 29 miały posłużyć zebraniu konkretnych informacji o tych zagrożeniach w celu zbadania, czy obawy wyrażone wcześniej przez Grupę Roboczą pozostają w mocy.

Jak już wspomniano, dostępność danych o ruchu pozwala na ujawnienie preferencji, opinii i postaw i może jednocześnie zakłócać życie prywatne użytkowników i wywierać istotny wpływ na poufność połączeń oraz prawa podstawowe takie jak wolność słowa. Niestety, może się to

stać zarówno wskutek zamierzonych działań jak i niedbałych mechanizmów zatrzymywania. Nieuprawnione ujawnianie lub dostęp do informacji związanych z łącznością elektroniczną – które mogą zostać powiązane z danymi lokalizacyjnymi – może wywrzeć znaczący wpływ na prywatność osób, których dane dotyczą. W świetle powyższego, wdrażanie dyrektywy o zatrzymywaniu danych przez dostawców usług łączności elektronicznej i usług internetowych wiąże się nieuchronnie z wysokim poziomem ryzyka, wymagającym zastosowania odpowiednich środków technicznych i organizacyjnych.

Jeśli chodzi o ryzyko, należy przypomnieć, że dyrektywa zakazuje zatrzymywania danych związanych z treścią połączeń; ponadto, sama dostępność danych o ruchu (tj. danych wymienionych w art. 5 dyrektywy o zatrzymywaniu danych) pozwala prześledzić kilka rodzajów informacji związanych z osobami, których dane dotyczą (w tym danych szczególnie chronionych) na podstawie ogólnego obrazu (np. profili behawioralnych poszczególnych użytkowników), jaki można zbudować na podstawie ich interakcji społecznych. Informacje takie można umieścić w kontekście czasowym i przestrzennym i skategoryzować w sposób bardzo szczegółowy za pomocą narzędzi *data mining*, korzystających z wielkiej mocy obliczeniowej dostępnej poprzez serwery i komputery osobiste. Techniki takie są szczególnie efektywne w przypadku dużych ilości danych o ruchu obejmujących długi okres czasu. Jeśli chodzi o usługi internetowe, mogą one nieść za sobą więcej zagrożeń niż dane o ruchu telefonicznym, ponieważ informacje takie jak adres IP mogą same w sobie zdradzać treści; podobnie jak informacje o powiązaniach społecznościowych mogą ujawnić najbardziej intymne preferencje osób, których dane dotyczą. Jednym z celów akcji wdrożeniowej była ocena, do jakiego stopnia dostawcy łączności elektronicznej i usług internetowych zdawali sobie sprawę z tych zagrożeń i stosowali zabezpieczenia, by ich uniknąć.

## **B. Metodologia i etapy**

Inspekcję przeprowadziły organy ochrony danych z następujących krajów: *Belgia, Bułgaria, Cypr, Czechy, Dania, Estonia, Finlandia, Francja, Niemcy, Grecja, Węgry, Irlandia, Włochy, Łotwa, Lichtenstein, Luksemburg, Litwa, Malta, Holandia, Polska, Rumunia, Słowacja, Słowenia, Hiszpania i Wielka Brytania*. Należy nadmienić, że komentarze do wyników przesłały również Szwedzka Agencja Pocztovo-Telekomunikacyjna i Komisja Europejska.

Na podstawie doświadczeń zebranych podczas pierwszej akcji wdrożeniowej i zaleceń zawartych w ostatecznym sprawozdaniu z tej akcji, Grupa Robocza zdecydowała o przeprowadzeniu drugiej akcji w dwóch etapach – przesłaniu kwestionariusza i ocenie odpowiedzi organów ochrony danych oraz inspekcjach na miejscu.

Standardowy kwestionariusz (przyjęty przez Grupę Roboczą w grudniu 2008 r.) wraz ze standardowym pismem do wszystkich dostawców usług łączności elektronicznej i usług internetowych wybranych w poszczególnych państwach członkowskich. Kontrolowane firmy wybrano na podstawie rynku, na którym działały (telefonii naziemnej i komórkowej, operatorzy prowadzący różne rodzaje działalności, operatorzy zajmujący się jedynie usługami internetowymi) i rozmiaru (mali dostawcy i wielcy operatorzy telekomunikacyjni) tak, by objąć inspekcją znaczną część rynku.

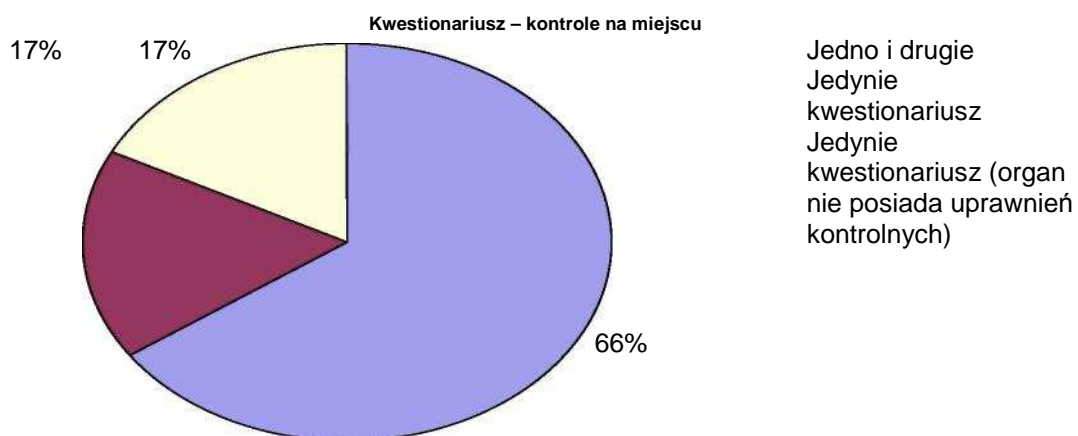
Kwestionariusz podzielony był na 10 rozdziałów odnoszących się do typu zatrzymywanych danych, okresu zatrzymywania i rozwiązań technologicznych wprowadzonych w związku z zatrzymywaniem oraz kwestii szczególnie istotnych z punktu widzenia zatrzymywania danych (np. bezpieczeństwa informatycznego, ochrony logicznej, identyfikacji/upoważniania, logów, szyfrowania, protokołów ujawniania/transmisji, zabezpieczeń fizycznych, kopii zapasowych). Ograniczono liczbę pytań i sformułowano je w możliwie jasny sposób, uwzględniając problemy napotkane podczas pierwszej akcji wdrożeniowej i kryteria selekcji respondentów.

Inspekcje na miejscu były prowadzone w przypadkach, w których organy ochrony danych uznały to za niezbędne i w których było to możliwe w aspekcie uprawnień kontrolnych organu

i dostępności doświadczonych pracowników. Inspekcje miały na celu ocenę wiarygodności odpowiedzi na kwestionariusz i pozyskanie bardziej szczegółowych informacji o kwestiach związanych z wdrażaniem. Inspekcje odegrały podstawową rolę w ocenie przestrzegania odpowiednich wymogów przez administratorów.

Następnie każdy z biorących udział w akcji organów ochrony danych opracował raport opisujący jego sytuację i najistotniejsze uwagi. Tabela podsumowująca informacje podane przez organy stanowi Załącznik 1 do niniejszego sprawozdania.

Poniższy wykres pokazuje rozkład statystyczny organów, które wykonały kontrole na miejscu, tych, które wysłały kwestionariusz i tych, które nie posiadają odpowiednich uprawnień kontrolnych.



## C. Wyniki

Ogólnie rzecz biorąc, odpowiedzi na kwestionariusz wykazały znaczące zróżnicowanie sposobów wdrażania, w szczególności w odniesieniu do środków bezpieczeństwa (patrz Załącznik 1, kolumny P i Q). Jedynie dzięki dogłębnym inspekcjom na miejscu udało się ustalić, że niektóre z odpowiedzi były niedokładne, co doprowadziło do nałożenia doraźnych sankcji i wprowadzenia określonych środków technicznych i organizacyjnych.

***Biorąc pod uwagę różną wartość informacji uzyskanych za pomocą inspekcji i kwestionariusza, w szczególności organy ochrony danych posiadające uprawnienia kontrolne winny mieć świadomość zagrożeń nieodłącznie związanych z ogólnym obowiązkiem zatrzymywania danych o ruchu, prowadzić kampanie podnoszące świadomość i w razie potrzeby kontynuować monitoring systemów w siedzibach dostawców łączności elektronicznej i usług internetowych. Ponadto, należy unikać ograniczenia działalności egzekucyjnej organów ochrony danych przez różne czynniki, w tym tajemnicę biznesową/branżową, jeśli dzięki nim dostawcy mogliby uchylać się od podawania żądanych informacji. Niezbędne jest przyznanie organom ochrony danych szerokich uprawnień egzekucyjnych, w tym prawa dostępu do informacji objętych tajemnicą zawodową/branżową – w przeciwnym razie trudno będzie otrzymać pełny obraz sytuacji.***

### i. Kategorie zatrzymywanych danych

W kwestii kategorii danych o ruchu podlegających obowiązkowi zatrzymywania, ustalono, że dane o ruchu telefonicznym zatrzymywane przez indywidualnych dostawców (patrz Załącznik 1, kolumny I i J) były co do zasady zgodne z wymienionymi w art. 5 dyrektywy o zatrzymywaniu danych. Jeśli natomiast chodzi o zatrzymywanie danych o ruchu dla usług internetowych (Załącznik 1, kolumna K), zanotowano znaczące rozbieżności.

Poza kilkoma wyjątkami (w szczególności przypadkiem, kiedy w jednym z państw członkowskich okazało się, że treść wiadomości tekstowych jest zatrzymywana i dostępna przez kilka miesięcy, by ułatwić działanie służb bezpieczeństwa), w odniesieniu do usług telefonicznych zatrzymywane są dane niezbędne do identyfikacji źródła i odbiorcy połączenia, rozpoczęcia i zakończenia połączenia oraz usług i terminali wykorzystywanych przez użytkowników. Szczególny powód do niepokoju stanowi zatrzymywanie danych lokalizacyjnych, zbieranych nieustannie podczas rozmów telefonicznych lub połączeń z Internetem, ze względu na możliwość śledzenia ruchów użytkowników.

Inna jest sytuacja w zakresie zatrzymywania danych o ruchu w internecie. Poza kategoriami danych wymienionymi w art. 5 dyrektywy, w pewnych przypadkach zatrzymywane są również inne kategorie danych, związane z treścią przesyłanych komunikatów i jako takie wykraczające poza zakres obecnych ram regulacyjnych (patrz Załącznik 1, kolumna K) – takie jak adresy IP i adresy URL stron internetowych, nagłówki wiadomości e-mail, listy wszystkich odbiorców wiadomości kopii na serwerze poczty przychodzącej czy numer portu przypisany użytkownikowi przez dostawcę usług internetowych.

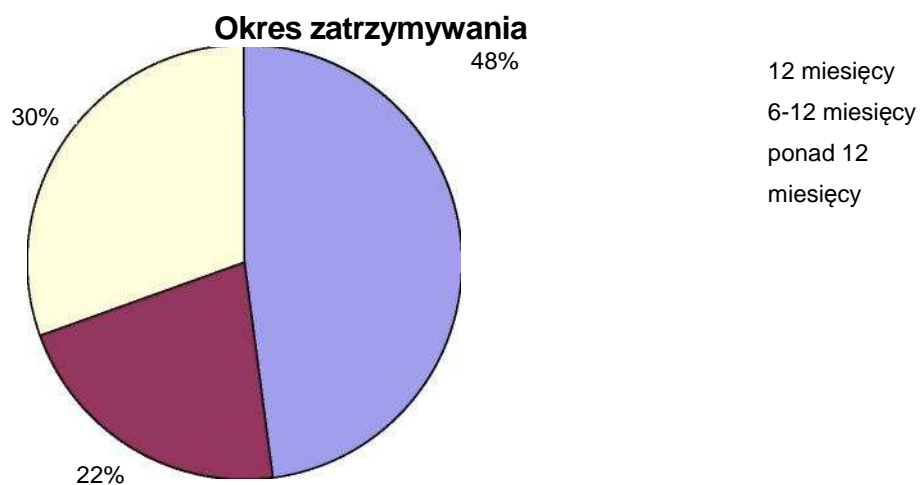
***W związku z powyższym należy przypomnieć, że dyrektywa 2006/24/WE odchodzi od przepisów dyrektywy 2002/58/WE i że lista danych o ruchu, które mają obowiązkowo być zatrzymywane ma charakter zamknięty – zgodnie z dyrektywą o zatrzymywaniu danych, na dostawców nie można nakładać żadnych dodatkowych zobowiązań w zakresie zatrzymywania.***

Z drugiej strony, Grupa Robocza Art. 29 ma świadomość problemów związanych z możliwym rozszerzeniem zakresu zastosowania dyrektywy o zatrzymywaniu zgodnie z prawem krajowym – w szczególności wątpliwości, czy organy wymiaru sprawiedliwości mogą zbierać jedynie dane o ruchu, których zatrzymywanie przez dostawców jest dozwolone na mocy art. 6 ust. 2 dyrektywy, czy również inne dane o ruchu, niewymienione w dyrektywie 2002/58/WE.

### ii. Okres zatrzymywania

Dla celów niniejszej analizy, na podstawie wyników akcji wdrożeniowej, potencjalny okres zatrzymywania (6-24 miesięcy) został rozbity na trzy limity czasowe: a) 12-miesięczny, b)

krótszy niż 12 miesięcy i c) dłuższy niż 12 miesięcy. Ustalono, że 48% respondentów zatrzymuje dane na okres 12 miesięcy, zaś grupy b) i c) okazały się dość liczne i porównywalne – ich udział wynosił odpowiednio 22% i 30%. Poniższy wykres ilustruje rozkład procentowy w państwach członkowskich UE:



Okresy zatrzymywania danych określone przez ustawodawców wdrażających dyrektywę o zatrzymywaniu w poszczególnych krajach znacząco różnią się między sobą (patrz Załącznik 1, kolumny L, M, N), choć w wielu krajach (patrz wykres poniżej) preferowane jest stosowanie okresu krótszego niż maksymalny dozwolony – co wskazuje na możliwość dalszej harmonizacji zakresu czasowego określonego w dyrektywie o zatrzymywaniu danych.

***W tym celu zalecane byłoby rozważenie skrócenia maksymalnego okresu zatrzymywania i ustanowienie jednolitego, krótszego okresu, obowiązującego wszystkich dostawców w UE, jak wskazano w opinii WP113 Grupy Roboczej Art. 29.***

Na podstawie kontroli stwierdzono, że dostawcy, z którymi się skontaktowano lub u których przeprowadzono kontrolę wypełniali opisane powyżej wymogi w zakresie zachowywania danych. Jednak w kilku przypadkach sytuacja była inna ze względu na różne praktyki w zakresie przechowywania lub zobowiązania odnoszące się do zastosowania danych o ruchu dla celów komercyjnych (dane takie były przechowywane przez okres dłuższy niż określony w dyrektywie o zatrzymywaniu danych). W niektórych przypadkach okres przechowywania wynosił nawet 36 miesięcy, a w jednym – aż 10 lat.

Ponadto, stwierdzono, że w wielu przypadkach nie stosowano zautomatyzowanych procedur usuwania danych po upływie odpowiedniego okresu zatrzymywania. W związku z tym należy przypomnieć, że zastosowania procedur manualnych lub inicjowanych przez pracowników nie można uznać za zgodne z dyrektywą o zatrzymywaniu, ponieważ pozwala ono na wydłużenie okresów przechowywania o nieokreślony czas upływający pomiędzy zakończeniem okresu zatrzymywania a rozpoczęciem manualnej procedury usuwania danych. Procedury zautomatyzowane należy zastosować również do kopii zapasowych.

Należy wskazać również, że dostawcy łączności elektronicznej i usług internetowych przechowują dane w kilku systemach i wykorzystują te dane do różnych celów operacyjnych i związanych z zarządzaniem, przewidzianych prawem lub regulowanych przez umowy SLA bądź umowy świadczenia usług. Ponadto, wszelkie dane o ruchu przechowywane w systemach dostępnych dla organów wymiaru sprawiedliwości były przedtem przechowywane w innych systemach, dostępnych dla różnych celów, takich jak rozwiązywanie problemów, wykrywanie fałszerstw, billingi itp., przez rozmaite podmioty w obrębie dostawcy, zwykle podlegające mniej restrykcyjnej kontroli.

***W związku z powyższym, konieczne wydaje się podkreślenie potrzeby dokonania przez Komisję i inne kompetentne instytucje oceny działania dyrektywy o zatrzymywaniu danych z uwzględnieniem wrażliwego charakteru danych o ruchu jako takich i ponownego przeanalizowania ich bezpieczeństwa – niezależnie od tego, czy takie dane przechowywane są w systemach i dla celów innych niż opisane w dyrektywie o zatrzymywaniu danych – w celu dokonania ogólnej oceny wdrażania tej dyrektywy. Dopuszczenie stosowania przez systemy zawierające kategorie danych o ruchu wymienione w dyrektywie o ochronie danych innych poziomów bezpieczeństwa i okresów zatrzymywania danych niż w przypadku systemów zawierających dane o ruchu wykorzystywane w innych, biznesowych celach oznacza obniżenie ogólnego bezpieczeństwa danych o ruchu i niespełnienie wymogów określonych w dyrektywie o zatrzymywaniu danych – zatrzymywania danych o ruchu na ograniczony okres czasu i udzielanie dostępu do nich na określonych warunkach.***

### *iii. Techniczne i organizacyjne środki bezpieczeństwa*

Art. 7(b) dyrektywy o zatrzymywaniu danych nakłada wymóg zatrzymywania danych z zachowaniem odpowiednich zabezpieczeń technicznych i organizacyjnych w celu minimalizacji ryzyka przypadkowego lub nieuprawnionego zniszczenia, zmiany, dostępu lub przetwarzania danych.

Dyrektywa o zatrzymywaniu danych nie wymaga wprowadzenia dodatkowych środków

bezpieczeństwa poza opisanymi w dyrektywach 2002/58/WE i 95/46/WE. Jak jednak podkreślano już we wcześniejszych opiniach Grupy Roboczej Art. 29, należy uznać, że poziom ryzyka związanego z danymi o ruchu jako takimi wymaga zastosowania surowych, odpowiednich do niego standardów bezpieczeństwa, wprowadzonych z uwzględnieniem charakteru danych, ilości przechowywanych danych i okresów zatrzymywania.

W tym kontekście akcja wdrożeniowa wykazała, że techniczne i organizacyjne środki bezpieczeństwa stosowane przez dostawców łączności elektronicznej i usług internetowych odzwierciedlają ich świadomość zagrożeń związanych z danymi o ruchu telefonicznym i internetowym. W przypadku nieotrzymania szczegółowych wskazówek lub nieodpowiedniej oceny zagrożeń istnieje duże ryzyko zastosowania nieodpowiednich środków.

***Aby wypełnić wymogi dyrektywy o zatrzymywaniu danych, dostawcy łączności elektronicznej i usług internetowych winni oceniać zagrożenia związane z danymi o ruchu w sposób regularny i możliwie najbardziej obiektywny, w celu określenia wszystkich istotnych czynników ryzyka i ich możliwego wpływu, ze szczególnym uwzględnieniem kontroli dostępu i dostępności danych. Regularnie prowadzone audyty zewnętrzne mogłyby przyczynić się do niezależnej i obiektywnej oceny ryzyka.***

Jeśli chodzi o bezpieczeństwo informacji, kontrola nie dała jasnego obrazu – w istocie, zarówno na podstawie kwestionariusza (patrz Załącznik 1, kolumny P i Q) i inspekcji prowadzonych na miejscu można stwierdzić, że środki bezpieczeństwa zmieniają się w zależności od wielkości firmy dostawcy.

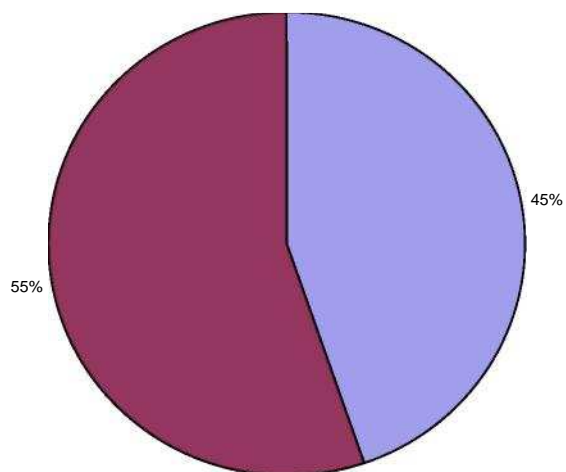
Wysoki poziom bezpieczeństwa obowiązywał w odniesieniu do fizycznego dostępu do systemów zatrzymywania danych o ruchu (patrz Załącznik 1, kolumna Q). Zdarzają się drobne rozbieżności, jednak większość dostawców łączności elektronicznej i usług internetowych posługuje się wideonadzorem, pracownikami powołanymi do nadzoru, systemami kontroli nadzoru i procedurach awaryjnych w celu zapewnienia stałego monitoringu wyżej wymienionych systemów.

Więksi dostawcy stosowali środki techniczne i organizacyjne mogące zapewnić odpowiedni poziom bezpieczeństwa zatrzymywanych danych o ruchu, mniejsi zapewniali niższy poziom bezpieczeństwa – w istocie, większość z nich, głównie ze względu na strategie finansowe ograniczające koszty, nie jest zdolna do zastosowania zabezpieczeń informatycznych z najwyższej półki, chroniących dane o ruchu w takim samym stopniu jak w przypadku liderów rynku. W takim wypadku, zadania powierzone pracownikom przetwarzającym dane mogą się pokrywać i pracownicy ci mogą mieć dostęp do różnych systemów, gdzie dane przechowywane są dla różnych celów. Nie wszystkie systemy przetwarzające dane dla celów komercyjnych zostały zaprojektowane lub wdrożone z uwzględnieniem potrzeby zapewnienia odpowiedniego poziomu ochrony danych o ruchu. Zdaje się, że poziom świadomości w zakresie zagrożeń związanych z zatrzymywaniem danych o ruchu nie jest jednolity.

W odniesieniu, w szczególności, do wstępnej oceny ryzyka, stwierdzono, że co do zasady zadanie to realizowane jest wewnętrznie w danej firmie – co może wpływać na bezstronność opinii i zagraża bagatelizowaniem ryzyka. Poniższy wykres przedstawia odsetek dostawców, którzy przeprowadzają kontrole zewnętrzne lub poddają się certyfikacji bezpieczeństwa przez strony trzecie w porównaniu z całkowitą liczbą dostawców.

**Kontrole zewnętrzne**

Kontrole zewnętrzne  
Brak kontroli zewnętrznych



Dane o ruchu z natury rzeczy winny być traktowane jako szczególnie chronione, a zatem podobnie jak szczególne kategorie danych wymienione w art. 8 dyrektywy 95/46/WE. Zatrzymywanie danych o ruchu winno być przystosowane do ich wrażliwego charakteru, a dostęp do nich i dalsze przekazywanie do organów wymiaru sprawiedliwości – prowadzone ze szczególną ostrożnością. Aby to zapewnić, należy w jasny sposób określić w przepisach warunki dostępu do zatrzymywanych danych i ich dalszego przekazywania. Dyrektywa o zatrzymywaniu danych została opracowana w okresie przed wprowadzeniem Traktatu z Lizbony, w oparciu o inny podział kompetencji prawnych, i nie zawiera konkretnych zasad w tej kwestii – choć Grupa Robocza Art. 29 wzywała do ich opracowania. Ponadto, można stwierdzić, że w takiej sytuacji samoregulacja nie jest wystarczającym rozwiązaniem, w szczególności ze względu na brak równowagi pomiędzy uprawnieniami dostawców usług z jednej strony, a organów wymiaru sprawiedliwości z drugiej. Dostawcy usług nie mają możliwości egzekwowania własnej polityki bezpieczeństwa w kontaktach z organami wymiaru sprawiedliwości.

*Można zaproponować następujące środki dodatkowe w stosunku do już istniejących zabezpieczeń, w pełni zgodne z zasadą neutralności technologicznej, w celu zapewnienia dostępu do danych jedynie upoważnionym pracownikom, zgodnie z art. 7(c) dyrektywy o zatrzymywaniu danych, które na chwilę obecną nie są stosowane przez wszystkich dostawców:*

- *skuteczna kontrola dostępu do zatrzymywanych danych poprzez zdefiniowanie obowiązków użytkownika i profili użytkownika o różnych uprawnieniach;*
- *skuteczna identyfikacja przy dostępie do systemu, oparta na podwójnych mechanizmach identyfikacji (hasło+biometria lub hasło+token), w celu zapewnienia fizycznej obecności osoby odpowiedzialnej za przetwarzanie danych o ruchu;*
- *szczegółowe śledzenie operacji przetwarzania i dostępu poprzez zachowywanie logów zawierających przynajmniej informacje o tożsamości użytkownika, terminie dostępu i nazwie przeglądanego pliku;*
- *zastosowanie zarządzania logami w celu zapewnienia ich wiarygodności poprzez technologie szyfrujące;*
- *oddzielenie logiczne od innych systemów przetwarzających dane o ruchu dla celów komercyjnych;*
- *inne środki niezbędne dla zapewnienia poufności danych*

Ponadto, z punktu widzenia organizacji/zarządzania należy przywiązywać szczególną wagę do administratorów systemów, w których dane o ruchu są zatrzymywane dla potrzeb organów wymiaru sprawiedliwości; *role i zadania takich administratorów winny zostać dokładnie określone, w tym w dokumentach doraźnie regulujących politykę, a obsługa systemu winna zostać poddana dogłębnej kontroli.*

W celu dalszego wzmocnienia środków bezpieczeństwa odnoszących się do danych o ruchu, niezbędne są liczne, skoordynowane działania. *Wdrożenie takich środków przez dostawców może ułatwić włączenie zarówno polityki wewnętrznej jak i środków technicznych sensu stricte do programu certyfikacji bezpieczeństwa prowadzonego regularnie – najlepiej przez stronę trzecią – zgodnie z międzynarodowymi standardami w celu oceny trwałości zastosowanych środków w kontekście zmieniających się zagrożeń. Do tego celu mogą być przydatne również inne środki, takie jak przyznanie organom ochrony danych uprawnień kontrolnych lub udostępnienie im wyników kontroli prowadzonych przez strony trzecie.*

Niejednolite wypełnianie wymogów technicznych i organizacyjnych w zakresie bezpieczeństwa przekłada się na niepełne osiągnięcie harmonizacji, jaką ma na celu dyrektywa i wpływa na koszty ponoszone przez indywidualne podmioty ze względu na różnice w ich wielkości i pozycji na rynku oraz zmienną dynamikę rynku, co w efekcie prowadzi do niezharmonizowanego zastosowania dyrektywy o ochronie danych i uniemożliwia obywatelom UE korzystanie z tego samego poziomu ochrony.

Kwestia art. 7(d) dyrektywy o zatrzymywaniu danych (dane udostępnione) – art. 7(d)

dyrektywy o zatrzymywaniu danych przewiduje wyjątek odnoszący się do zatrzymywania danych udostępnionych organom wymiaru sprawiedliwości – których okres przechowywania można *de facto* wydłużyć na czas nieokreślony.

Należy rozważyć, czy dostawcy usług łączności elektronicznej i usług internetowych powinni zostać zobowiązani do opracowania dodatkowych środków zabezpieczeń, mających zastosowanie do kategorii „dane udostępnione”, jako że w dyrektywie nie zapisano żadnych konkretnych wymogów w tym zakresie, czy też dane takie winny później znaleźć się w odpowiednich aktach spraw, a stosowanie odpowiednich zabezpieczeń należy powierzyć właściwym organom (wydaje się, że tak właśnie jest w tej chwili). Dane takie obarczone są poważnym ryzykiem, ponieważ mogą zdradzić istotne informacje o użytkownikach (w tym dane szczególnie chronione).

Powszechny dostęp do danych o ruchu i wydłużenie okresu zatrzymywania takich danych mogą być postrzegane jako mechanizmy pozwalające ominąć wymogi ustanowione dyrektywą. ***Konieczność wydłużenia okresów zatrzymywania danych należy ocenić według ściśle określonych kryteriów, w każdym przypadku przewidując usunięcie udostępnionych danych zgodnie z wymogami zawartymi w dyrektywie 95/46/WE i instrumentach międzynarodowych (w tym w rekomendacji Rady Europy R(87)15).***

#### *iv. Procedury przekazywania*

Ustalono, że procedury przekazywania danych o ruchu na wniosek organów wymiaru sprawiedliwości są w znaczącym stopniu niejednolite. Zarówno w kwestionariuszu jak i podczas inspekcji na miejscu wykryto i opisano szeroką gamę rozwiązań – w tym przekazywanie na podstawie wypisywanych ręcznie dokumentów, w formie przesyłek kurierskich lub standardowych przesyłek pocztowych – oraz poziomów bezpieczeństwa przekazywania – od wiadomości e-mail i faksów po dedykowane, szyfrowane kanały. ***Należy przywiązywać szczególną wagę do osiągnięcia harmonizacji w tym obszarze poprzez opracowanie standardowych procedur przekazywania danych organom wymiaru sprawiedliwości.***

W związku z powyższym należy wspomnieć, że dyrektywa o zatrzymywaniu danych zawiera zamkniętą listę danych, jakie dostawcy mogą przekazywać organom wymiaru sprawiedliwości. Dane te stanowią zamknięty zbiór, ponadto poważne przestępstwa, na których ściganiu musi być oparty wniosek o udostępnienie danych, organy sądownicze upoważnione do udostępniania danych oraz możliwości dostępu winny być określone w jasny i wyczerpujący sposób.

***Protokół wymiany danych oparty na powyższych założeniach mógłby zostać rozwinięty w standardową procedurę informatyczną, obecnie kwestia ta jest pozostawiona uznaniu poszczególnych zainteresowanych stron – przynajmniej w odniesieniu do udostępnionych informacji. Określenie standardowej procedury przekazywania, uwzględniającej również kierunek przekazywania (opartego na protokołach PUSH) umożliwiłoby szybsze i bardziej rzetelne przekazywanie, pociągające za sobą mniejsze koszty dla obu zainteresowanych stron (dostawców i organów wymiaru sprawiedliwości). W istocie, mogliby oni skorzystać ze standardowych rozwiązań opracowanych na podstawie ujednoliconych ram referencyjnych i wdrożonych na wielką skalę. Znacząco różniłyby się one od rozwiązań dostępnych obecnie na rynku, które mają inny charakter i są droższe.***

Należy zaznaczyć, że dokładne określenie zarówno zainteresowanych stron jak i zakresu danych, jakie mogą one przekazywać znacznie podniosłoby ogólny poziom bezpieczeństwa procedury przekazywania. Można to uzasadnić na kilka sposobów: takie rozwiązanie pozwoliłoby na wzajemne szyfrowanie, zostałyby spełnione warunki wstępne dla zastosowania szyfrowanych połączeń oraz zaufanych i bezpiecznych kanałów komunikacji opartych na wymianie klucza i certyfikatu podpisu elektronicznego, które zapewniłyby integralność, poufność i możliwość określenia tożsamości nadawcy i odbiorcy przekazywanych danych; znacznie obniżyłoby ryzyko ataków man-in-the-middle – przechwytywania kanału

komunikacji i przejmowania lub kopiowania przekazywanych treści; pozwoliłoby na wprowadzenie wszystkich narzędzi niezbędnych do skutecznego rozliczania udostępniania danych; umożliwiłoby poszczególnym zainteresowanym stronom kategoryzację wniosków według celu lub kategorii udostępnianych danych – co, jak można się spodziewać, ułatwiłoby opracowanie jednolitych raportów statystycznych w państwach członkowskich. Wszystkie te możliwości, w przypadku ich wykorzystania, pozwoliłyby na zmniejszenie liczby przypadków nieuprawnionego dostępu do danych i umożliwiłoby organom ochrony danych skuteczną kontrolę dostępu. Organy sądownicze również powinny uczestniczyć w procesie przekazywania – jako zaufane podmioty, które mogłyby decydować w poszczególnych przypadkach, które dane i pod jakimi warunkami mogą zostać przekazane organom wymiaru sprawiedliwości. Cele powinny zostać wybrane z dostępnej listy poważnych przestępstw, tak, aby wiernie odtworzyć procedurę komunikacji przewidzianą w dyrektywie o danych o ruchu.

***Z powyższych powodów, ogólnoeuropejski standard przekazywania mógłby zawierać następujące elementy:***

- punkt kontaktowy u każdego dostawcy usług;
- jednolity format przekazywania danych obejmujący co najmniej następujące pola, umożliwiające bezpieczne, wiarygodne przekazywanie i dostęp do danych przez zainteresowane strony:
  - o dane użytkowników, w tym znana, określona liczba pól związanych z subskrypcjami i terminalami udostępnionymi użytkownikom;
  - o dane o ruchu, w tym znana, określona liczba pól związanych z wdrażaniem na szczeblu krajowym listy danych określonej w art. 5 dyrektywy o zatrzymywaniu danych;
  - o kod dostawcy, zawierający unikalny, ogólnoeuropejski identyfikator dostawcy usług łączności elektronicznej lub usług internetowych;
  - o kod organu wymiaru sprawiedliwości, zawierający identyfikator organu upoważnionego do uzyskiwania dostępu do danych o ruchu;
  - o kod sądowiczy, zawierający unikalny, ogólnoeuropejski identyfikator organu sądowiczego uprawnionego do udostępniania danych na ruchu;
  - o znacznik czasu i numer wniosku, pozwalające na ustalenie daty i kolejności wniosków o dostęp i zezwoleń udzielonych na ich podstawie;
  - o rodzaj wniosku, z uwzględnieniem kategorii (np. według rodzaju poważnego przestępstwa lub ilości żądanych danych o ruchu).

Wprowadzenie protokołu przekazania danych zawierającego wspomniane powyżej elementy pozwoliłoby na zminimalizowanie problemów, na które kilka organów ochrony danych wskazało podczas niniejszej akcji – takich jak naciski wywierane przez organy wymiaru sprawiedliwości na dostawców w celu pozyskania dodatkowych danych użytkowników, niewymienionych w dyrektywie o zatrzymywaniu danych, żądanie dostępu bez formalnych nakazów lub składanie wniosków o dostęp przez organy nieuprawnione (niebędące organami wymiaru sprawiedliwości).

W tym kontekście należy przypomnieć, że ***na poziomie krajowym należy stworzyć listy poważnych przestępstw w oparciu o prawo krajowe, z uwzględnieniem kwestii poruszonych w dokumentach WP113 i WP119. Wyczerpująca lista podmiotów uprawnionych do uzyskania dostępu do danych zgodnie z dyrektywą o zatrzymywaniu powinna zostać przedstawiona wszystkim zainteresowanym stronom.***

W związku z powyższym warto wspomnieć, że Europejski Instytut Norm Telekomunikacyjnych (ETSI) prowadził efektywne prace nad wzorcem referencyjnym dla przekazywania danych o ruchu organom wymiaru sprawiedliwości i model ten może podlegać dalszej analizie i ocenie.

#### **D. Statystyki zgodne z art. 10 dyrektywy o zatrzymywaniu danych**

Zgodnie z art. 10 dyrektywy o zatrzymywaniu danych, państwa członkowskie gwarantują

przekazanie Komisji corocznych statystyk na temat wykorzystania danych zatrzymanych na podstawie odpowiednich przepisów; art. 14 stanowi, że wszelkie zmiany w dyrektywie winny uwzględniać statystyki udostępnione przez państwa członkowskie. Poza bardzo nielicznymi wyjątkami, nie udało się potwierdzić wypełniania tego obowiązku.

Jedynie kilka państw członkowskich przedstawiło żądane informacje, dotyczące liczby wniosków otrzymanych przez dostawców, przypadków, w których żądane informacje zostały udostępnione i w których dostawca nie mógł udostępnić żądanych danych oraz ilości czasu, jaka upłynęła pomiędzy datą przechowywania danych a datą zażądania przekazania tych danych przez właściwe organy.

Choć statystyki opracowane na podstawie art. 10 nie mogą stanowić jedynej podstawy dla rozstrzygnięcia o przyszłości dyrektywy o zatrzymywaniu danych, dostępność i odpowiednia analiza tych informacji mają fundamentalne znaczenie dla oceny, czy cele przyświecające dyrektywie (w tym konieczność wprowadzenia zharmonizowanych zasad odnoszących się do wszystkich państw członkowskich UE) zostały osiągnięte – w szczególności w świetle krytycznych uwag zgłaszanych w trakcie debaty przed wprowadzeniem dyrektywy i po niej (patrz decyzje sądów najwyższych i trybunałów konstytucyjnych niektórych państw europejskich).

Brak wiarygodnych statystyk może utrudniać ocenę, która jest istotnym warunkiem wstępnym dla ewentualnej nowelizacji dyrektywy – w szczególności w odniesieniu do listy danych wymienionej w art. 5 i okresów zatrzymywania określonych w art. 6.

Wykorzystanie niepełnych lub niejednorodnych statystyk może skutkować podejmowaniem decyzji mających znaczny wpływ na prywatność osób, których dane dotyczą bez względu na lepszą harmonizację, do jakiej dąży się w dyrektywie.

Również w tym przypadku należy uwzględnić fakt, że część przeszkód można by usunąć dzięki wprowadzeniu standardowej procedury przekazywania danych. Dzięki istnieniu ściśle określonych zasad przekazywania danych, każda z zainteresowanych stron mogłaby stworzyć statystyki spójne z opracowanymi przez inne strony – co pozwoliłoby na zwiększenie wiarygodności analizy efektywności wykorzystania danych o ruchu w celu ścigania „poważnych przestępstw”.

*W związku z pierwszą oceną wdrażania dyrektywy 2006/24/WE, jaką Komisja ma przeprowadzić do 15 września 2010 r., bardzo istotne jest, by każde państwo członkowskie, które wdrożyło dyrektywę, przedstawiło niezbędne statystyki. Grupa Robocza Art. 29 uważa dostarczenie tych informacji za absolutnie niezbędne dla umożliwienia określenia w sposób obiektywny przydatności i efektywności dyrektywy o zatrzymywaniu danych.*

*Ponadto, niezwykle istotne jest, by statystykom towarzyszyły informacje o wpływie wymienionych danych, według ich wieku, na walkę z poważną przestępczością.*

## **E. Kwestia outsourcingu**

W toku akcji wdrożeniowej ustalono, że coraz częstsze jest stosowanie outsourcingu rozmaitych działań związanych z zatrzymywaniem danych – w szczególności w przypadku mniejszych dostawców, dążących do ograniczenia kosztów. Ta praktyka nie zawsze idzie w parze z dokładnym określeniem ról, w szczególności w odniesieniu do zgodności z krajowym ustawodawstwem w zakresie ochrony danych i wyznaczania podmiotów przetwarzających dane oraz rozdzielaniem zadań związanych z przetwarzaniem odpowiednim pracownikom.

Należy przypomnieć, że rynek sieci i usług łączności elektronicznej złożony jest z wielu podmiotów dysponujących bardzo zróżnicowanymi zasobami finansowymi i ludzkimi – jest to oczywistą przeszkodą dla osiągnięcia harmonizacji wymaganej na mocy dyrektywy o zatrzymywaniu. Ustalono na przykład, że rozmiar firmy przechowującej dane był w niektórych

przypadkach znacznie większy niż dostawcy usług łączności elektronicznej – co w oczywisty sposób utrudnia temu ostatniemu (czyli administratorowi danych) dokładne monitorowanie przetwarzania prowadzonego przez podwykonawcę. Dodatkowe problemy pojawiają się, jeśli dane o ruchu są przechowywane poza granicami kraju, co nie jest sytuacją niezwykłą (patrz wykres poniżej), sytuacja taka jest jednak zwykle ograniczona do dużych firm działających w mniejszych państwach członkowskich i korzystających z usług świadczonych w siedzibie głównej. Z możliwości takiej korzystają także mniejsi dostawcy i operatorzy wirtualni, korzystający z usług międzynarodowych firm specjalizujących się w rozwiązaniach informatycznych. W takiej sytuacji wzywa się organy nadzorcze do zwiększenia poziomu wzajemnej współpracy i pomocy, pozwalającego na uzyskanie dostępu do danych i wykonywanie koniecznych uprawnień egzekucyjnych.

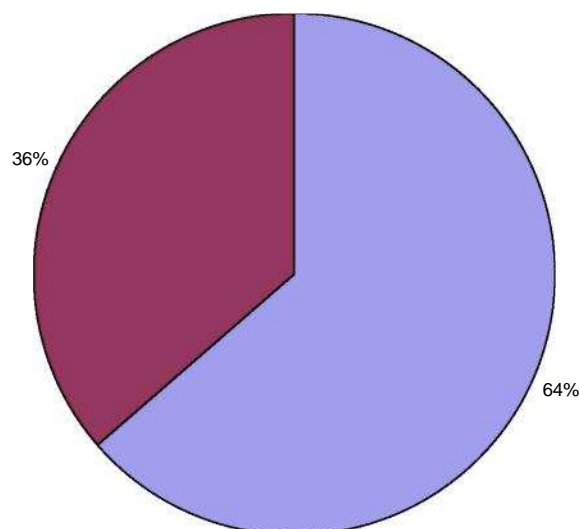
***Aby spełnić wymogi określone w dyrektywie bez znaczącego zwiększania kosztów, można zastosować rozwiązania federacyjne, wykorzystywane już – głównie na szczeblu krajowym, przez małych dostawców usług internetowych*** – w których jeden ze sfederowanych dostawców lub oddelegowana strona trzecia tworzy i wdraża systemy zatrzymywania danych, zarządza kolejnymi fazami identyfikacji, i partycjami pamięci przydzielonymi każdemu z dostawców. Takie rozwiązanie ocenić można pozytywnie, wymaga ono jednak odpowiednio zharmonizowanych, sformalizowanych i szczegółowych reguł.

W każdym przypadku przekazywanie zatrzymanych danych do innych krajów winno odbywać się zgodnie z warunkami określonymi w dyrektywie 95/46/WE. W szczególności przekazywanie danych wytworzonych na terytorium UE, które mają być wykorzystywane poza tym terytorium winno być poddane ocenie odpowiedności zgodnie z dyrektywą.

Ponadto, przepisy dyrektywy 95/46/WE odnoszące się do przekazywania danych osobowych do krajów trzecich nie mogą być stosowane odrębnie od pozostałych przepisów tej dyrektywy, w tym regulujących związek pomiędzy administratorem i przetwarzającym.

Zatrzymywanie za granicą (również na terytorium UE)

Nie Tak



***Kwestia outsourcingu winna zostać poddana pogłębionej analizie przez organy ochrony danych w celu bardziej efektywnej oceny zgodności z wymogami na poziomie krajowym (np. w zakresie wyznaczania przetwarzających dane), w tym klauzul umownych, które powinny określać konkretne, odpowiednie środki bezpieczeństwa.***

#### **IV. Dalsze działania i zalecenia**

W świetle ustaleń wspólnej kontroli, po uwzględnieniu rozważonych kwestii indywidualnych, poczynić można poniższe zalecenia. Większość z nich adresowana jest do dostawców, którzy dysponują środkami technicznymi pozwalającymi na zastosowanie się do nich, jednak dotyczą one także roli organów publicznych, w tym Komisji Europejskiej, państw członkowskich i krajowych organów ochrony danych – również w związku z kwestią kosztów, które mogą pociągać za sobą zaniedbywanie zastosowania niezbędnych narzędzi ochrony danych i prywatności, a z drugiej strony – spowodować zakłócenia na rynku. **Ponadto, Grupa Robocza pragnie przypomnieć, że samoregulacja jako taka nie jest w tej sytuacji wystarczająca, przede wszystkim ze względu na brak równowagi pomiędzy uprawnieniami dostawców usług i organami wymiaru sprawiedliwości. Ponadto, kwestie finansowe i konkurencja mogą prowadzić do samoregulacji niezapewniającej wysokich standardów bezpieczeństwa.**

##### ***- Kategorie zatrzymywanych danych***

Ponieważ dyrektywa 2006/24/WE odchodzi od przepisów dyrektywy 2002/58/WE, lista danych o ruchu, które mają być obowiązkowo zatrzymywane winna być uznana za wyczerpującą, a zatem zgodnie z dyrektywą, prawo krajowe nie może nakładać na dostawców dodatkowych zobowiązań do zatrzymywania danych. Z drugiej strony, Grupa Robocza Art. 29 pragnie podkreślić, że zgodnie z dyrektywą o zatrzymywaniu danych organy wymiaru sprawiedliwości nie mają prawa żądać od dostawców usług zbierania danych wykraczających poza zakres kategorii wymienionych w dyrektywie.

##### ***- Okresy zatrzymywania***

- a. Brak harmonizacji w kwestii okresów zatrzymywania ujawniony podczas niniejszej kontroli ma znaczący wpływ na zasadę, zgodnie z którą obywatele UE „mogą korzystać z tego samego poziomu ochrony w całej Unii Europejskiej”, m.in. ze względu na fakt, że może wpłynąć na poszczególne zainteresowane podmioty w sferze ekonomicznej, jako że wiąże się z kosztami i konkurencyjnością. W związku z tym, Grupa Robocza Art. 29 sądzi, że korzystne byłoby rozważenie skrócenia maksymalnego okresu zatrzymywania danych i ustanowienie jednolitego, krótszego limitu, którego mieliby przestrzegać wszyscy dostawcy w UE – jak stwierdzono w opinii WP113 Grupy Roboczej Art. 29.
- b. W związku z różnicami w celach i okresach zatrzymywania danych (do celów komercyjnych lub dla celów egzekwowania prawa), właściwe wydaje się zaproponowanie Komisji ponownego rozważenia ogólnego bezpieczeństwa danych o ruchu jako takich, w celu dokonania ogólnej oceny wdrażania dyrektywy o zatrzymywaniu danych. Nie można pozwolić, by w związku z różnymi celami obowiązywały różne poziomy bezpieczeństwa i okresy zatrzymywania danych. Dyrektywa o zatrzymywaniu stanowi, że dane o ruchu zebrane dla celów wymiaru sprawiedliwości winny być zatrzymywane jedynie przez określony czas, a dostęp do nich powinien mieć miejsce w określonym celu związanym z egzekwowaniem prawa i posiadać jasne podstawy prawne.

##### ***- Techniczne i organizacyjne środki bezpieczeństwa***

- a. Dostawcy łączności elektronicznej i usług internetowych winni regularnie dokonywać możliwie najbardziej obiektywnej oceny zagrożeń związanych z danymi o ruchu w celu wykrycia wszystkich istotnych czynników ryzyka i ich możliwego wpływu, ze szczególnym uwzględnieniem kontroli dostępu i dostępności danych. Do niezależnej i obiektywnej oceny ryzyka przyczynić się może regularne przeprowadzanie audytów zewnętrznych.
- b. Można proponować następujące środki, poza istniejącymi już zabezpieczeniami, niestosowane jeszcze przez wszystkich dostawców, które mogą zostać przyjęte przy zachowaniu pełnej zgodności z zasadą neutralności technologicznej w celu zapewnienia, że, zgodnie z art. 7 (c) dyrektywy o zatrzymywaniu do danych będzie miał dostęp jedynie

upoważniony do tego personel:

- skuteczna kontrola dostępu do zatrzymywanych danych poprzez zdefiniowanie obowiązków użytkownika i profili użytkownika o różnych uprawnieniach;
- skuteczna identyfikacja przy dostępie do systemu, oparta na podwójnych mechanizmach identyfikacji (hasło+biometria lub hasło+token), w celu zapewnienia fizycznej obecności osoby odpowiedzialnej za przetwarzanie danych o ruchu;
- szczegółowe śledzenie operacji przetwarzania i dostępu poprzez zachowywanie logów zawierających przynajmniej informacje o tożsamości użytkownika, terminie dostępu i nazwie przeglądanego pliku;
- zastosowanie zarządzania logami w celu zapewnienia ich wiarygodności poprzez technologie szyfrujące;
- oddzielenie logiczne od innych systemów przetwarzających dane o ruchu dla celów komercyjnych;
- inne środki niezbędne dla zapewnienia poufności danych

c. Należy szczegółowo opisać role i funkcje administratorów systemu, również za pomocą dokumentów doraźnie regulujących politykę, a wszystkie czynności związane z obsługą takich systemów winny być przedmiotem szczegółowej kontroli.

d. W celu dalszego wzmocnienia środków bezpieczeństwa odnoszących się do danych o ruchu, niezbędne są liczne, skoordynowane działania. Wdrożenie takich środków przez dostawców może ułatwić włączenie zarówno polityki wewnętrznej jak i środków technicznych *sensu stricto* do programu certyfikacji bezpieczeństwa prowadzonego regularnie – najlepiej przez stronę trzecią – zgodnie z międzynarodowymi standardami w celu oceny trwałości zastosowanych środków w kontekście zmieniających się zagrożeń. Do tego celu mogą być przydatne również inne środki, takie jak przyznanie organom ochrony danych uprawnień kontrolnych lub udostępnienie im wyników kontroli prowadzonych przez strony trzecie.

Potrzeba rozważenia dłuższych okresów zachowywania danych winna być oceniana zgodnie z jasno określonymi kryteriami, które w każdym przypadku powinny umożliwiać usunięcie takich danych zgodnie z wymogami określonymi w dyrektywie 95/46/WE i instrumentach międzynarodowych (w tym rekomendacji Rady Europy R(87)15 ).

#### **- Procedury przekazywania**

- a. Należy wypracować na szczeblu europejskim standardowe procedury przekazywania danych do organów wymiaru sprawiedliwości w celu zwiększenia harmonizacji. Protokół wymiany danych mógłby zostać przekształcony w standardową procedurę informatyczną, uwzględniając również kierunek przekazywania (które powinno być oparte na protokołach PUSH). Pozwoliłoby to na szybsze i bardziej rzetelne przekazywanie danych i zmniejszenie kosztów dla obu zainteresowanych stron (dostawców i organów wymiaru sprawiedliwości). Standard przekazywania winien uwzględniać co najmniej poniższe parametry lub wydarzenia: dane użytkownika, rodzaj danych o ruchu, kod dostawcy usług, kod organu wymiaru sprawiedliwości, kod sądowiczy, znacznik czasu oraz sygnaturę i rodzaj wniosku.
- b. Na poziomie krajowym należy stworzyć listy poważnych przestępstw w oparciu o prawo krajowe, z uwzględnieniem kwestii poruszonych w dokumentach WP113 i WP119. Wyczerpująca lista podmiotów uprawnionych do uzyskania dostępu do danych zgodnie z dyrektywą o zatrzymywaniu powinna zostać przedstawiona wszystkim zainteresowanym stronom.

#### **- Statystyki**

Państwa Członkowskie winny możliwie jak najszybciej zapewnić Komisji niezbędne statystyki – w każdym przypadku z odpowiednim wyprzedzeniem przed ostatecznym terminem raportu z oceny dyrektywy o zatrzymywaniu, który ma sporządzić Komisja. Jeśli to możliwe, statystykom takim powinny towarzyszyć informacje o wpływie zatrzymywanych

danych o ruchu na walkę z poważną przestępczością – według wieku tych danych.

**- Outsourcing**

a. Kwestia outsourcingu winna zostać poddana pogłębionej analizie przez organy ochrony danych w celu bardziej efektywnej oceny zgodności z wymogami na poziomie krajowym (np. w zakresie wyznaczania przetwarzających dane), w tym klauzul umownych, które powinny określać konkretne, odpowiednie środki bezpieczeństwa.

b. Można wspomnieć o rozwiązaniach federacyjnych, wprowadzonych już na poziomie krajowym przez drobnych dostawców usług internetowych.