I

(Rezolucje, zalecenia i opinie)

OPINIE

EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Opinia Europejskiego Inspektora Ochrony Danych na temat sprawozdania z oceny Komisji dla Rady i Parlamentu Europejskiego w sprawie dyrektywy w sprawie zatrzymywania danych (dyrektywa 2006/24/WE)

(2011/C 279/01)

EUROPEJSKI INSPEKTOR OCHRONY DANYCH,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, a w szczególności art. 16,

uwzględniając Kartę praw podstawowych Unii Europejskiej, a w szczególności art. 7 i 8,

uwzględniając dyrektywę 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 ([1]),

uwzględniając dyrektywę 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej ([2]),

uwzględniając rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych ([3]), a w szczególności art. 41,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

I. **WPROWADZENIE**

I.1. **Publikacja sprawozdania**

1. W dniu 18 kwietnia 2011 r. Komisja przedstawiła swoje sprawozdanie z oceny na temat dyrektywy w sprawie zatrzymywania danych (zwane dalej „sprawozdaniem z oceny") ([4]). Sprawozdanie zostało przesłane do wiadomości EIOD tego samego dnia. Z powodów określonych w części I.2 poniżej, EIOD wydaje niniejszą opinię z własnej inicjatywy, zgodnie z art. 41 rozporządzenia (WE) nr 45/2001.

2. Przed przyjęciem komunikatu EIOD miał możliwość przekazania nieformalnych uwag. EIOD wyraża zadowolenie, że wiele z tych uwag zostało uwzględnionych przez Komisję przy pracy nad ostateczną wersją dokumentu.

3. Komisja opracowała sprawozdanie z oceny w celu spełnienia obowiązku wynikającego z art. 14 dyrektywy w sprawie zatrzymywania danych, związanego z oceną stosowania dyrektywy, oraz jego wpływu na podmioty gospodarcze i konsumentów, aby stwierdzić, czy konieczna jest zmiana przepisów dyrektywy ([5]). EIOD z zadowoleniem stwierdza, iż mimo że nie jest to ściśle wymagane zgodnie z art. 14, Komisja uwzględniła również w sprawozdaniu „implikacje dyrektywy dla praw podstawowych, w świetle krytyki, którą podnoszono ogólnie w odniesieniu do zatrzymywania danych" ([6]).

I.2. **Przyczyny i cel niniejszej opinii EIOD**

4. Dyrektywa w sprawie zatrzymywania danych stanowiła odpowiedź UE na pilne wyzwania związane z bezpieczeństwem po zamachach terrorystycznych w Madrycie w 2004 r. i Londynie w 2005 r. Pomimo zgodnego z prawem celu ustanowienia mechanizmu zatrzymywania danych, pojawiły się głosy krytyczne w związku z olbrzymim wpływem, jaki środek miał na prywatność obywateli.

5. Obowiązek zatrzymywania danych zgodnie z dyrektywą w sprawie zatrzymywania danych pozwala właściwym władzom krajowym prześledzenie połączeń telefonicznych i internetowych wszystkich osób w UE za każdym razem, kiedy korzystają z telefonu lub Internetu, w okresie do dwóch lat.

([1]) Dz.U. L 281 z 23.11.1995, s. 31.
([2]) Dz.U. L 201 z 31.7.2002, s. 37, zmieniona dyrektywą Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r., Dz.U. L 337 z 18.12.2009, s. 11.
([3]) Dz.U. L 8 z 12.1.2001, s. 1.
([4]) COM(2011) 225 wersja ostateczna.
([5]) Dyrektywa w sprawie zatrzymywania danych (dyrektywa 2006/24/WE) została przyjęta w dniu 15 marca 2006 r. i opublikowana w Dz.U. L 105 z 13.4.2006, s. 54. Termin wydania raportu określono na dzień 15 września 2010 r., zob. art. 14 ust. 1 dyrektywy w sprawie zatrzymywania danych.
([6]) Zob. s. 1 sprawozdania z oceny.

6. Zatrzymywanie danych telekomunikacyjnych stanowi w jasny sposób ingerencję w prawo do poszanowania prywatności zainteresowanych osób zgodnie z art. 8 Europejskiej Konwencji Praw Człowieka (zwanej dalej „Konwencją") oraz art. 7 Karty praw podstawowych UE.

7. Europejski Trybunał Praw Człowieka wielokrotnie stwierdzał, że „samo zatrzymywanie danych dotyczących prywatnego życia poszczególnych osób stanowi ingerencję w rozumieniu art. 8 [Konwencji]" ([7]). W szczególności w odniesieniu do danych telefonicznych Europejski Trybunał Praw Człowieka stwierdził, że „ujawnianie tych informacji policji bez zgody abonenta stanowi […] ingerencję w prawo gwarantowane przez art. 8 [Konwencji]" ([8]).

8. Z art. 8 ust. 2 Konwencji i art. 52 ust. 1 Karty praw podstawowych UE wynika, że ingerencja może być uzasadniona, o ile stanowi tak prawo, służy to uzasadnionemu celowi oraz jest niezbędne w społeczeństwie demokratycznym do osiągnięcia celu zgodnego z prawem.

9. EIOD potwierdza, że dostępność pewnych danych dotyczących ruchu i lokalizacji może być kluczowa dla organów wymiaru sprawiedliwości w zwalczaniu terroryzmu i innych poważnych przestępstw. Równocześnie jednak EIOD wielokrotnie wyrażał wątpliwości, co do uzasadnienia zatrzymywania danych na taką skalę w świetle prawa do poszanowania prywatności i ochrony danych ([9]). Te wątpliwości podziela wiele organizacji społeczeństwa obywatelskiego ([10]).

10. EIOD z bliska przyglądał się na różne sposoby opracowywaniu, wdrażaniu i ocenie dyrektywy od 2005 r. W 2005 r. EIOD wydał krytyczną opinię po tym, jak Komisja opublikowała swój wniosek w sprawie dyrektywy ([11]). Po przyjęciu dyrektywy EIOD został członkiem grupy ekspertów ds. zachowywania danych, o której mowa w motywie 14 dyrektywy w sprawie zatrzymywania danych ([12]). Ponadto EIOD uczestniczy w pracach grupy roboczej powołanej na mocy art. 29, która opublikowała wiele dokumentów w tej sprawie, ostatnio w lipcu 2010 r. – sprawozdanie na temat stosowania dyrektywy w praktyce ([13]). EIOD działał również w charakterze interwenienta w sprawie przed Europejskim Trybunałem Sprawiedliwości, w której podnoszono kwestię ważności dyrektywy ([14]).

11. Nie można przeceniać znaczenia sprawozdania z oceny i procesu oceny ([15]). Dyrektywa w sprawie zatrzymywania danych stanowi doskonały przykład środka UE mającego na celu zapewnienie dostępności danych generowanych i przetwarzanych w kontekście komunikacji elektronicznej do egzekwowania prawa. Ponieważ środek istnieje już od kilku lat, ocena jego praktycznego stosowania powinna wykazać niezbędność i proporcjonalność środka w świetle prawa do poszanowania prywatności i ochrony danych. W tym kontekście EIOD nazwał ocenę „chwilą prawdy" dla dyrektywy w sprawie zatrzymywania danych ([16]).

12. Obecny proces oceny ma również implikacje dla innych instrumentów regulujących zarządzanie informacjami, w tym przetwarzanie olbrzymich ilości danych osobowych w obszarze wolności, bezpieczeństwa i sprawiedliwości. W komunikacie z 2010 r. Komisja stwierdziła, że mechanizmy oceny różnych instrumentów wskazują na duże zróżnicowanie ([17]). EIOD jest zdania, że obecną procedurę oceny należy wykorzystać do ustalenia standardu oceny innych instrumentów UE i zapewnienia pozostawienia wyłącznie w pełni uzasadnionych środków.

13. W związku z tym EIOD pragnie podzielić się w upublicznionej opinii uwagami w sprawie ustaleń przedstawionych w sprawozdaniu z oceny. Dzieje się to na wczesnym etapie procesu w celu wniesienia rzeczywistego i konstruktywnego wkładu w przyszłe dyskusje, prawdopodobnie w kontekście nowego wniosku legislacyjnego, o którym mowa w sprawozdaniu z oceny Komisji ([18]).

I.3. **Struktura opinii**

14. W niniejszej opinii zostanie przeanalizowana i omówiona treść sprawozdania z oceny z punktu widzenia poszanowania prywatności i ochrony danych. Analiza skupi się na tym, czy obecna dyrektywa w sprawie zatrzymywania danych spełnia wymagania określone przez te dwa prawa podstawowe. Obejmuje to analizę tego, czy konieczność zatrzymywania danych regulowana w dyrektywie została wystarczająco wykazana.

15. Niniejsza opinia zorganizowana jest w następujący sposób: część II zawiera opis najważniejszych przepisów dyrektywy

([7]) Zob. np. Europejska Konwencja Praw Człowieka, wyrok z dnia 4 grudnia 2008 r. w sprawie *S. i Marper* v. *UK*, 30562/04 i 30566/04, pkt 67.

([8]) Zob. Europejska Konwencja Praw Człowieka, wyrok z dnia 2 sierpnia 1984 r. w sprawie *Malone* v. *UK*, A-82, pkt 84.

([9]) Zob. opinia EIOD z dnia 26 września 2005 r., Dz.U. C 298 z 29.11.2005, s. 1. Podczas konferencji zorganizowanej przez Komisję w grudniu 2010 r. EIOD odniósł się do instrumentu jako do „najsilniej ingerującego instrumentu kiedykolwiek przyjętego przez UE, jeśli chodzi o zakres i liczbę osób, których dotyczy", zob. wystąpienie z dnia 3 grudnia 2010 r., które znajduje się na stronie internetowej EIOD (http://www.edps.europa.eu) w zakładce „Publications" >> „Speeches & Articles" >> „2010".

([10]) Te wątpliwości podziela wiele organizacji społeczeństwa obywatelskiego (http://www.vorratsdatenspeicherung.de/images/DRletter_Malmstroem.pdf).

([11]) Zob. opinia EIOD, o której mowa w przypisie 9.

([12]) Zob. również decyzję Komisji z dnia 25 marca 2008 r., Dz.U. L 111 z 23.4.2008, s. 11.

([13]) Zob. grupa robocza 172 z dnia 13 lipca 2010 r., sprawozdanie 1/2010 w sprawie drugiego wspólnego egzekwowania.

([14]) Zob. ETS, wyrok z dnia 10 lutego 2009 r. w sprawie *Irlandia* przeciwko *Parlamentowi i Radzie*, C-301/06. W tej sprawie zob. również pkt 29 poniżej.

([15]) EIOD już podkreślał w swojej opinii z 2005 r. znaczenie obowiązku dokonania oceny instrumentu (zob. przypis 9, pkt 72–73).

([16]) Zob. wystąpienie z dnia 3 grudnia 2010 r., o którym mowa w przypisie 9.

([17]) COM(2010) 385 z dnia 20 lipca 2010 r., Przegląd zarządzania informacjami w przestrzeni wolności, bezpieczeństwa i sprawiedliwości, s. 24. W sprawie tego komunikatu zob. opinię EIOD z dnia 30 września 2010 r., która znajduje się na stronie internetowej EIOD (http://www.edps.europa.eu) w zakładce „Consultation" >> „Opinions" >> „2010".

([18]) Zob. s. 32 sprawozdania z oceny.

w sprawie zatrzymywania danych oraz jej związków z dyrektywą 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dalej: „dyrektywa o prywatności i łączności elektronicznej") ([19]). W części III krótko zostaną przedstawione zmiany wprowadzone przez traktat lizboński, gdyż odnoszą się one w szczególności do bieżącej sprawy i mają bezpośrednie konsekwencje dla sposobu, w jaki należy postrzegać, oceniać i – ewentualnie – zmieniać przepisy UE w sprawie zatrzymywania danych. Najdłuższa część opinii, część IV, zawiera analizę ważności dyrektywy w sprawie zatrzymywania danych w świetle prawa do poszanowania prywatności i ochrony danych oraz z myślą o ustaleniach przedstawionych w sprawozdaniu z oceny. W części V omówione zostaną możliwe dalsze działania. Opinię kończą wnioski zawarte w części VI.

II. **PRZEPISY UE W ZAKRESIE ZATRZYMYWANIA DANYCH**

16. W kontekście niniejszej opinii zatrzymywanie danych odnosi się do obowiązku nałożonego na dostawców powszechnie dostępnych usług komunikacji elektronicznej lub publicznych sieci komunikacyjnych do zatrzymywania danych dotyczących ruchu i danych, a także powiązanych danych niezbędnych do zidentyfikowania abonenta lub użytkownika, przez określony okres. Obowiązek ten wprowadza dyrektywa w sprawie zatrzymywania danych, w której w art. 5 ust. 1 określono kategorie zatrzymywanych danych. Zgodnie z art. 6 dyrektywy w sprawie zatrzymywania danych państwa członkowskie gwarantują, że dane są zatrzymywane na okresy nie krótsze niż sześć miesięcy oraz nie dłuższe niż dwa lata od daty połączenia.

17. Dane są zatrzymywane, o ile dane te są generowane lub przetwarzane przez dostawców w procesie dostarczania przedmiotowych usług łączności. Obejmuje to również dane związane z nieskutecznymi próbami połączenia. Zgodnie z dyrektywą (art. 5 ust. 1) nie można zatrzymywać żadnych danych ujawniających treść komunikacji.

18. Dane są zatrzymywane w celu zapewnienia ich dostępności do celu „dochodzenia, wykrywania i ścigania poważnych przestępstw, określonych w ustawodawstwie każdego państwa członkowskiego" (art. 1 ust. 1).

19. Dyrektywa w sprawie zatrzymywania danych nie zawiera dalszych przepisów w sprawie warunków, na jakich właściwe władze krajowe mogą mieć dostęp do zatrzymywanych danych. Leży to w gestii państw członkowskich i wykracza poza zakres dyrektywy. W art. 4 dyrektywy podkreślono, że przepisy krajowe powinny być zgodne z wymogami niezbędności i proporcjonalności, określonymi w szczególności w Konwencji.

20. Dyrektywa w sprawie zatrzymywania danych jest ściśle powiązana z dyrektywą o prywatności elektronicznej. Dyrektywa ta, uszczegółowiająca i uzupełniająca ogólną dyrektywę w sprawie ochrony danych 95/46/WE, określa, że państwa członkowskie zapewniają poufność łączności i powiązanych danych o ruchu ([20]). Dyrektywa o prywatności elektronicznej wymaga, by dane o ruchu i lokalizacji wygenerowane w wyniku korzystania z usług komunikacji elektronicznej były usuwane lub uczynione anonimowymi, gdy nie będą już potrzebne do celów przesyłu w ramach komunikacji, chyba że są one niezbędne w celu naliczania opłat i tylko tak długo, jak będzie to niezbędne ([21]). Niektóre dane mogą być przetwarzane przez okres niezbędny do świadczenia usług o wartości dodanej, pod warunkiem uzyskania zgody.

21. Na podstawie art. 15 ust. 1 dyrektywy o prywatności elektronicznej państwa członkowskie mają możliwość przyjmowania środków prawnych ograniczających zakres wspomnianych wyżej zobowiązań, jeżeli „takie ograniczenia stanowią środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego (np. bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych […]". Ta kwestia zatrzymywania danych jest przywołana *explicite* w art. 15 ust. 1 dyrektywy o prywatności elektronicznej. Państwa członkowskie mogą „uchwalić środki ustawodawcze przewidujące przechowywanie danych przez określony czas" uzasadnione we wspomniany sposób.

22. Dyrektywa w sprawie zatrzymywania danych miała na celu dostosowanie inicjatyw państw członkowskich na mocy art. 15 ust. 1 w zakresie zatrzymywania danych do celów dochodzenia, wykrywania i ścigania poważnych przestępstw. Należy podkreślić, że dyrektywa w sprawie zatrzymywania danych stanowi wyjątek od ogólnego obowiązku wynikającego z dyrektywy o prywatności elektronicznej, zgodnie z którym dane należy usunąć, gdy nie są już potrzebne ([22]).

23. Wraz z przyjęciem dyrektywy w sprawie zatrzymywania danych dodano dodatkowy ustęp 1a w art. 15 dyrektywy o prywatności elektronicznej, w którym stwierdza się, że art. 15 ust. 1 nie ma zastosowania do danych, które w sposób szczególny na mocy dyrektywy w sprawie zatrzymywania danych mają być zatrzymywane do celów określonych w art. 1 ust. 1 tej dyrektywy.

24. W sprawozdaniu z oceny stwierdzono, że art. 15 ust. 1 i art. 15 ust. 1b są stosowane przez niektóre państwa członkowskie w celu wykorzystania danych zatrzymywanych na mocy dyrektywy o zatrzymywaniu danych również do innych celów, co zostanie dalej omówione w części IV.3 poniżej ([23]). EIOD odniósł się do tej kwestii jako do „luki prawnej" w przepisach, która uniemożliwia osiągnięcie celu dyrektywy w sprawie zatrzymywania danych, którym jest stworzenie takich samych warunków działania dla całego sektora ([24]).

([19]) Porównaj: przypis 2.

([20]) Zob. art. 5 dyrektywy o prywatności elektronicznej.

([21]) Zob. art. 6 dyrektywy o prywatności elektronicznej.

([22]) Zob. również grupa robocza 29 w sprawozdaniu z dnia 13 lipca 2010 r., o którym mowa w przypisie 13, s. 1.

([23]) Zob. s. 4 sprawozdania z oceny. Zob. również w tym kontekście motyw 12 dyrektywy w sprawie zatrzymywania danych.

([24]) Zob. wystąpienie z dnia 3 grudnia 2010 r., o którym mowa w przypisie 9, s. 4.

III. **PO LIZBONIE ZMIENIŁ SIĘ OGÓLNY KONTEKST PRAWNY UE**

25. Ogólny kontekst prawny UE w odniesieniu do dyrektywy w sprawie zatrzymywania danych zmienił się w znaczący sposób z wejściem w życie traktatu lizbońskiego. Istotną zmianą było zniesienie struktury opartej na filarach, która ustanawiała różne procedury legislacyjne i mechanizmy przeglądu dla różnych obszarów kompetencji UE.

26. Wcześniejsza struktura oparta na filarach wywoływała dyskusje dotyczące właściwej podstawy prawnej instrumentu UE, jeżeli dana kwestia leżała w kompetencjach UE należących do różnych filarów. Wybór podstawy prawnej nie był bez znaczenia, ponieważ prowadził do różnych procedur legislacyjnych w odniesieniu do, przykładowo, wymogu głosowania w Radzie (większość kwalifikowana lub jednomyślność) lub udziału Parlamentu Europejskiego.

27. Dyskusje te odnosiły się ściśle do zatrzymywania danych. Ponieważ celem dyrektywy w sprawie zatrzymywania danych była harmonizacja obowiązków dla operatorów i tym samym wyeliminowanie przeszkód dla rynku wewnętrznego, podstawę prawną można było znaleźć w art. 95 poprzedniego Traktatu WE (stary pierwszy filar). Do kwestii można jednak było podejść od strony egzekwowania prawa, argumentując, że celem przechowywania danych było zwalczanie poważnych przestępstw w ramach współpracy policyjnej i sądowej w sprawach karnych zgodnie ze starym Traktatem UE (poprzednio trzeci filar) ([25]).

28. Ostatecznie dyrektywa w sprawie zatrzymywania danych została przyjęta w oparciu o art. 95 poprzedniego Traktatu WE, regulując jedynie obowiązki operatorów. Dyrektywa nie określała zasad dostępu ani wykorzystywania zatrzymywanych danych przez wymiar sprawiedliwości.

29. Ważność dyrektywy po jej przyjęciu była badana przez Trybunał Sprawiedliwości. Twierdzono, że dyrektywę należało oprzeć na trzecim filarze zamiast na pierwszym, ponieważ cel, dla którego dane miały być zatrzymywane (dochodzenie, wykrywanie oraz ściganie poważnych przestępstw), leżał w zakresie kompetencji UE w ramach trzeciego filaru ([26]). Ponieważ jednak działania właściwych organów *explicite* znalazły się poza zakresem dyrektywy, Trybunał Sprawiedliwości stwierdził, że dyrektywa słusznie oparta jest na Traktacie WE ([27]).

30. Od początku EIOD twierdził, że jeżeli UE przyjęłaby instrument w sprawie zatrzymywania danych, powinien on regulować obowiązek operatorów, a także dostęp i przyszłe wykorzystanie danych przez organy wymiaru sprawiedliwości. W opinii z 2005 r. w sprawie wniosku Komisji EIOD podkreślał, że dostęp i dalsze wykorzystanie danych przez właściwe władze krajowe stanowiły kluczową i niemożliwą do wyodrębnienia część przedmiotowej kwestii ([28]).

31. Negatywny wpływ uregulowania przez UE jedynie połowy kwestii potwierdza przedmiotowe sprawozdanie z oceny, co zostanie rozwinięte w dalszej części opinii. Komisja stwierdza, że różnice w prawie krajowym w zakresie dostępu i dalszego wykorzystania przez właściwe władze krajowe doprowadziły do „znacznych trudności" dla operatorów ([29]).

32. Wraz ze zniesieniem struktury opartej na filarach po wejściu w życie traktatu lizbońskiego w TFUE dwa przedmiotowe obszary kompetencji UE zostały połączone, co pozwala na przyjmowanie przepisów prawa UE w oparciu o tę samą procedurę legislacyjną. Ten nowy kontekst umożliwia przyjęcie nowego wspólnego instrumentu w sprawie zatrzymywania danych, regulującego obowiązki operatorów oraz warunki dostępu i dalszego wykorzystania przez organy wymiaru sprawiedliwości. Prawo do poszanowania prywatności i ochrony danych, jak wyjaśniono w części IV.3 poniżej, wymaga uregulowania tej kwestii w całości, o ile rozważany byłby zmieniony środek UE w sprawie zatrzymywania danych.

33. Traktat lizboński nie tylko zniósł strukturę opartą na filarach, ale również nadał Karcie praw podstawowych, dotychczas niewiążącej, zawierającej prawo do poszanowania prywatności i ochrony danych w art. 7 i 8, taką samą wartość prawną jak traktatom ([30]). Podmiotowe prawo do ochrony danych zostało również zawarte w art. 16 TFUE, tworząc odrębną podstawę prawną dla instrumentów UE o ochronie danych osobowych.

34. Ochrona praw podstawowych od dawna stanowi podstawę polityki UE, a traktat lizboński doprowadził do jeszcze silniejszego zaangażowania w poszanowanie tych praw w kontekście UE. Zmiany wynikające z traktatu lizbońskiego zachęciły Komisję w październiku 2010 r. do ogłoszenia promowania „kultury praw podstawowych" na wszystkich etapach procesu legislacyjnego oraz do stwierdzenia, że postanowienia Karty praw podstawowych UE „powinny przyświecać […] politykom Unii" ([31]). EIOD jest zdania, że obecny proces oceny stanowi dla Komisji doskonałą okazję potwierdzenia zaangażowania w realizację tego zobowiązania.

([25]) Pierwszy wniosek w sprawie zasad zatrzymywania danych w UE (decyzja ramowa) opierał się na poprzednim Traktacie UE i został wniesiony przez Irlandię, Francję Szwecję i Zjednoczone Królestwo. Zob. dokument Rady 8958/04 z dnia 28 kwietnia 2004 r. Po tym wniosku powstał wniosek Komisji oparty na Traktacie WE. Zob. COM(2005) 438 z dnia 21 września 2005 r.

([26]) Argument ten opierał się na wyroku Trybunału Sprawiedliwości w „sprawach PNR", zob. ETS, wyrok z dnia 30 maja 2006 r. w sprawie *Parlament* przeciwko *Radzie i Komisji,* C-317/05 i C-318/04.

([27]) Zob. ETS, wyrok z dnia 10 lutego 2009 r. w sprawie *Irlandia* przeciwko *Parlamentowi i Radzie,* C-301/06, pkt 82–83.

([28]) Zob. opinię z 2005 r., pkt 80. Zob. również w tej kwestii część IV.3 niniejszej opinii.

([29]) Zob. s. 31 sprawozdania z oceny.

([30]) Zob. art. 6 ust. 1 TUE.

([31]) COM(2010) 573 z dnia 19 października 2010 r., Strategia skutecznego wprowadzania w życie Karty praw podstawowych przez Unię Europejską, s. 4.

IV. **CZY DYREKTYWA W SPRAWIE ZATRZYMYWANIA DANYCH SPEŁNIA WYMOGI DOTYCZĄCE POSZANOWANIA PRYWATNOŚCI I OCHRONY DANYCH?**

35. Sprawozdanie z oceny wskazuje na pewne słabości obecnej dyrektywy w sprawie zatrzymywania informacji. Przedstawione informacje wskazują, że dyrektywa nie osiągnęła swojego głównego celu, jakim jest harmonizacja ustawodawstw krajowych dotyczących zatrzymywania danych. Komisja zauważa, że istnieją „znaczące" różnice w transpozycji przepisów w obszarze ograniczenia celu, dostępu do danych, okresów zatrzymywania, ochrony danych, bezpieczeństwa danych i danych statystycznych ([32]). Według Komisji różnice wynikają częściowo z różnorodności wprowadzonej *explicite* przez dyrektywę. Komisja stwierdza jednak, że nawet poza tą kwestią „różnice w krajowym stosowaniu zatrzymywania danych stanowią poważną trudność dla operatorów" oraz „sektorowi nadal brakuje pewności prawnej" ([33]). Oczywiste jest, że taki brak harmonizacji działa na niekorzyść wszystkich zainteresowanych stron: obywateli, przedsiębiorców oraz organów wymiaru sprawiedliwości.

36. Z punktu widzenia poszanowania prywatności i ochrony danych sprawozdanie z oceny uzasadnia wniosek, że dyrektywa w sprawie zatrzymywania danych nie spełnia wymogów wypływających z prawa do poszanowania prywatności i ochrony danych. Istnieje wiele braków: konieczność zatrzymywania danych zgodnie z dyrektywą w sprawie zatrzymywania danych nie została wystarczająco wykazana, zatrzymywanie danych mogło być regulowane w sposób mniej ingerujący w prywatność, a dyrektywie w sprawie zatrzymywania danych brakuje przewidywalności. Te trzy kwestie zostaną omówione bardziej szczegółowo poniżej.

IV.1. **Konieczność zatrzymywania danych, o której mowa w dyrektywie w sprawie zatrzymywania danych, nie została wystarczająco wykazana**

37. Ingerencja w prawo do poszanowania prywatności i ochrony danych jest dopuszczalna jedynie wówczas, jeżeli środek jest niezbędny do osiągnięcia zgodnego z prawem celu. Konieczność zatrzymywania danych jako środek egzekwowania prawa stale jest przedmiotem dyskusji ([34]). We wniosku w sprawie dyrektywy stwierdzono, że ograniczenie prawa do poszanowania prywatności i ochrony danych jest „proporcjonalne i niezbędne do osiągnięcia ogólnie uznanych celów, jakimi są zapobieganie i zwalczanie przestępczości i terroryzmu" ([35]). W opinii z 2005 r. EIOD wskazywał jednak, że to stwierdzenie go nie przekonuje, gdyż niezbędne są dalsze dowody ([36]). Tym niemniej bez dostarczenia żadnych dodatkowych dowodów w motywie 9 dyrektywy w sprawie zatrzymywania danych stwierdzono, że „zatrzymywanie danych okazało się niezbędnym i skutecznym narzędziem egzekwowania prawa […] w niektórych państwach członkowskich".

38. W związku z brakiem wystarczających dowodów EIOD stwierdził, że dyrektywa w sprawie zatrzymywania danych była wyłącznie oparta na założeniu, że tak rozwinięte zatrzymywanie danych, jak przewiduje dyrektywa w sprawie zatrzymywania danych, stanowiło środek konieczny ([37]). EIOD zwrócił się więc do Komisji i do państw członkowskich o wykorzystanie sprawozdania z oceny do przedstawienia dodatkowych dowodów potwierdzających, że założenie konieczności środka zatrzymywania danych i sposób jego uregulowania w dyrektywie w sprawie zatrzymywania danych jest właściwy.

39. W tej kwestii Komisja stwierdza w sprawozdaniu z oceny, że „większość państw członkowskich przyjmuje stanowisko, że przepisy UE w sprawie zatrzymywania danych pozostają konieczne jako narzędzie egzekwowania prawa, ochrony ofiar i systemów wymiaru sprawiedliwości". Zatrzymywanie danych opisywane jest również jako odgrywające „bardzo ważną rolę" w dochodzeniach w sprawach karnych oraz jako „cenne, a w niektórych sprawach niezbędne". Stwierdza się również, że bez zatrzymywania danych niektóre sprawy karne „mogłyby nigdy nie zostać rozwiązane" ([38]). Komisja stwierdza, że UE powinna w związku z tym „wspierać i regulować zatrzymywanie danych jako środek bezpieczeństwa" ([39]).

40. Wątpliwe jest jednak, czy Komisja może też stwierdzić, że większość państw członkowskich uznaje zatrzymywanie danych za narzędzie konieczne. Nie wskazuje się, które państwa członkowskie tworzą większość, którą w UE 27 państw członkowskich powinno stanowić co najmniej 14 z nich, by można było mówić o większości państw członkowskich. W rozdziale 5, na którym oparte są wnioski, konkretne odwołania dotyczą co najwyżej dziewięciu państw członkowskich ([40]).

41. Ponadto wydaje się, że Komisja opiera się przede wszystkim na stwierdzeniach państw członkowskich dotyczących tego, czy zatrzymywanie danych jest narzędziem niezbędnym do egzekwowania prawa. Stwierdzenia te wskazują jednak, czy poszczególne państwa członkowskie chcą mieć przepisy w sprawie zatrzymywania danych, ale nie mogą jako takie stwierdzić zapotrzebowania na zatrzymywanie danych jako środka egzekwowania prawa, wspieranego i regulowanego przez UE. Stwierdzenia o konieczności wymagają poparcia wystarczającymi dowodami.

42. Wykazanie konieczności środka ingerującego w prywatność nie jest na pewno łatwym zadaniem. W szczególności nie jest to łatwe dla Komisji, która w dużej mierze uzależniona jest od informacji dostarczonych przez państwa członkowskie.

43. Jeżeli środek już istnieje, tak jak dyrektywa w sprawie zatrzymywania danych, i zebrano już doświadczenie praktyczne, powinny istnieć wystarczające informacje

([32]) Zob. s. 31 sprawozdania z oceny.
([33]) Zob. s. 31 sprawozdania z oceny.
([34]) Zob. opinia EIOD z 2005 r. Zob. również pismo z dnia 22 czerwca 2010 r. od dużej grupy organizacji społeczeństwa obywatelskiego, o którym mowa w przypisie 10.
([35]) COM(2005) 438 z dnia 21 września 2005 r., s. 3.
([36]) Zob. opinia z 2005 r., pkt 17–22.
([37]) Zob. wystąpienie z dnia 3 grudnia 2010 r., o którym mowa w przypisie 9.
([38]) Wszystkie cytaty ze s. 23 lub s. 31 sprawozdania z oceny.
([39]) Zob. s. 31 sprawozdania z oceny.
([40]) Republika Czeska, Niemcy, Irlandia, Węgry, Niderlandy, Polska, Słowenia, Finlandia i Zjednoczone Królestwo.

jakościowe i ilościowe pozwalające na ocenę, czy środek rzeczywiście działa oraz czy porównywalne wyniki można by było osiągnąć bez tego instrumentu lub za pomocą środka alternatywnego, mniej ingerującego w prywatność. Takie informacje powinny stanowić niezbywalny dowód i pokazywać związek pomiędzy wykorzystaniem a wynikiem ([41]). Ponieważ dotyczy to dyrektywy UE, informacje powinny przedstawiać praktykę co najmniej większości państw członkowskich UE.

44. Po uważnej analizie EIOD uważa, że mimo iż Komisja włożyła znaczne wysiłki w zebranie informacji od rządów państw członkowskich, informacje ilościowe i jakościowe dostarczone przez państwa członkowskie nie są wystarczające, by potwierdzić konieczność zatrzymywania danych w sposób określony w dyrektywie w sprawie zatrzymywania danych. Przedstawiono ciekawe przykłady zastosowań, jest jednak zbyt wiele braków w przedstawionych w sprawozdaniu informacjach, by móc wyciągnąć ogólne wnioski o konieczności instrumentu. Ponadto nadal należy dokładniej przeanalizować alternatywne środki. Te dwie kwestie zostaną omówione bardziej szczegółowo poniżej.

Informacje ilościowe i jakościowe przedstawione w sprawozdaniu z oceny

45. W odniesieniu do aspektu ilościowego informacje statystyczne przedstawiono przede wszystkim w rozdziale 5 i w załączniku do sprawozdania z oceny, brakuje jednak kluczowych informacji. Na przykład przedstawione dane nie wskazują celów, do których dane były potrzebne. Ponadto dane liczbowe nie pokazują, czy wszystkie dane, co do których wnoszono o dostęp, były danymi przechowywanymi w wyniku obowiązku prawnego zatrzymywania danych, czy były to dane przechowywane do celów komercyjnych. Nie ma również informacji o wynikach wykorzystania danych. W kontekście wyciągania wniosków problematyczna jest również kwestia niepełnej porównywalności informacji z różnych państw członkowskich, a w wielu przypadkach wykresy pokazują jedynie dziewięć państw członkowskich.

46. Przykłady jakościowe zawarte w sprawozdaniu służą lepszemu zobrazowaniu ważnej roli, jaką odegrały zatrzymywane dane w konkretnych sytuacjach oraz potencjalnych korzyści płynących z systemu zatrzymywania danych. Nie we wszystkich przypadkach jest jednak jasne, czy wykorzystanie zatrzymywanych danych było jedynym sposobem rozwiązania sprawy danego przestępstwa.

47. Niektóre przykłady ilustrują niezbędność środka polegającego na zatrzymywaniu danych do zwalczania cyberprzestępczości. W tej kwestii należy zauważyć, że główny międzynarodowy instrument w tym zakresie – Konwencja Rady Europy w sprawie cyberprzestępczości – nie przewiduje zatrzymywania danych jako środka zwalczania cyberprzestępczości, a odwołuje się jedynie do zachowywania danych jako narzędzia śledczego ([42]).

48. Komisja wydaje się przywiązywać dużą wagę do przykładów przedstawionych przez państwa członkowskie, w których zatrzymywane dane były wykorzystywane do wykluczenia podejrzanych o przestępstwo i do sprawdzania alibi ([43]). Mimo że są to ciekawe przykłady wykorzystywania danych przez wymiar sprawiedliwości, nie można ich wykorzystywać jako potwierdzenia potrzeby zatrzymywania danych. Argument ten należy wykorzystywać ostrożnie, ponieważ może zostać źle zrozumiany, sugerując, że zatrzymywanie danych jest niezbędne do udowodnienia niewinności obywateli, co trudno byłoby pogodzić z domniemaniem niewinności.

49. Sprawozdanie z oceny zawiera jedynie krótką informację na temat wartości zatrzymywania danych w powiązaniu z rozwiązaniami technologicznymi, a w szczególności wykorzystaniem przedpłaconych kart SIM ([44]). EIOD podkreśla, że większa ilość informacji ilościowych i jakościowych dotyczących nowych technologii nieobjętych dyrektywą (na przykład VoIP i sieci społecznościowe) pomogłaby dokonać oceny skuteczności dyrektywy.

50. Sprawozdanie z oceny jest ograniczone, ponieważ skupiono się w nim przede wszystkim na danych ilościowych i jakościowych dostarczonych przez państwa członkowskie, które wdrożyły dyrektywę w sprawie zatrzymywania danych. Ciekawe byłoby jednak przyjrzeć się, czy pomiędzy tymi państwami członkowskimi a państwami, które nie wdrożyły dyrektywy, pojawiły się znaczące różnice. W szczególności w odniesieniu do tych państw członkowskich, w których unieważniono przepisy wykonujące (Republika Czeska, Niemcy i Rumunia), ciekawe byłoby sprawdzenie, czy są jakiekolwiek dowody na sukces lub niepowodzenie dochodzeń przed unieważnieniem lub po nim.

51. Komisja przyznaje, że dane statystyczne i przykłady zawarte w sprawozdaniu z oceny są „w niektórych aspektach ograniczone", ale stwierdza jednak, że dowody potwierdzają „bardzo istotną rolę zatrzymywanych danych w śledztwach w sprawach karnych" ([45]).

52. EIOD jest zdania, że Komisja powinna być bardziej krytyczna wobec państw członkowskich. Jak wyjaśniono, same deklaracje polityczne niektórych państw członkowskich w sprawie potrzeby takiego środka nie mogą uzasadniać działania UE. Komisja powinna była naciskać na państwa członkowskie, by dostarczyły wystarczających dowodów potwierdzających konieczność środka. Według EIOD Komisja powinna była przynajmniej uzależnić swoje poparcie dla środka bezpieczeństwa w postaci zatrzymywania danych (zob. s. 31 sprawozdania z oceny) od dostarczenia przez państwa członkowskie dodatkowych dowodów podczas oceny wpływu.

Środki alternatywne

53. Konieczność zatrzymywania danych w sposób określony w dyrektywie w sprawie zatrzymywania danych zależy również od tego, czy istnieje środek mniej ingerujący w prywatność prowadzący do porównywalnych wyników. Zostało to potwierdzone przez Trybunał Sprawiedliwości w wyroku w sprawie *Schecke* w listopadzie 2010 r.,

([41]) W kwestii konieczności i proporcjonalności zob. również opinię EIOD z dnia 25 marca 2011 r. w sprawie wniosku UE PNR, która znajduje się na stronie internetowej EIOD (http://www.edps.europa.eu) w zakładce „Consultation" >> „Opinions" >> „2011".

([42]) Zob. s. 5 sprawozdania z oceny.

([43]) Zob. s. 24 sprawozdania z oceny.

([44]) Zob. s. 25 sprawozdania z oceny.

([45]) Zob. s. 31 sprawozdania z oceny.

w którym Trybunał stwierdził nieważność przepisów UE dotyczących publikacji nazwisk beneficjentów funduszy rolniczych ([46]). Jedną z przyczyn unieważnienia był fakt, że Rada i Komisja nie rozważyły alternatywnych środków, które byłyby spójne z celem publikacji, a równocześnie powodowałyby mniej ingerencji w prawo do poszanowania prywatności i ochrony danych zainteresowanych osób ([47]).

54. Najważniejsza alternatywa pojawiająca się w dyskusjach wokół dyrektywy w sprawie zatrzymywania danych to metoda zachowywania danych („szybkie zamrożenie" i „szybkie zamrożenie plus") ([48]). Polega ona na czasowym zabezpieczeniu, czyli „zamrożeniu", niektórych danych dotyczących ruchu telekomunikacyjnego i lokalizacji, wyłącznie w odniesieniu do konkretnych osób podejrzanych o działalność przestępczą, a które to dane mogą być dalej udostępnione organom wymiaru sprawiedliwości na mocy zezwolenia sądu.

55. W sprawozdaniu z oceny zachowywanie danych jest wspomniane w kontekście wspomnianej już Konwencji w sprawie cyberprzestępczości, ale jest uznane za niewłaściwe, ponieważ „nie gwarantuje zdolności do ustalenia ścieżek dowodowych przed nakazem zachowania oraz nie pozwala prowadzić dochodzenia, jeżeli nie jest znany cel, a także nie pozwala na zbieranie dowodów o ruchach np. ofiar lub świadków przestępstwa" ([49]).

56. EIOD przyznaje, że jeżeli zamiast szerokiego systemu zatrzymywania danych wykorzystywany jest system zachowywania danych, dostępnych jest mniej informacji. Jednak to właśnie z powodu bardziej ukierunkowanego charakteru zachowywanie danych stanowi instrument mniej ingerujący w prywatność, jeśli chodzi o skalę i liczbę osób, których dotyka. Ocena powinna skupić się nie tylko na dostępnych danych, ale też na różnych wynikach uzyskiwanych z obu systemów. EIOD jest zdania, że uzasadniona i niezbędna jest bardziej pogłębiona analiza tego środka. Mogłoby to zostać wykonane podczas oceny wpływu w najbliższych miesiącach.

57. W tej kwestii niefortunne jest stwierdzenie we wnioskach sprawozdania, że Komisja zobowiązuje się do przeanalizowania, czy – a jeżeli tak, to w jaki sposób – podejście UE do zachowywania danych mogłoby uzupełnić (czyli nie zastąpić) zatrzymywanie danych ([50]). Możliwość połączenia jednego z systemów zatrzymywania danych z gwarancjami proceduralnymi dotyczącymi różnych sposobów zachowywania danych rzeczywiście wymaga dalszej analizy. EIOD zaleca jednak, by Komisja podczas oceny wpływu rozważyła również, czy system zachowywania danych lub inny alternatywny środek mógłby w całości lub w części zastąpić obecny system zatrzymywania danych.

([46]) ETS, wyrok z dnia 9 listopada 2010 r. w sprawie *Volker und Markus Schecke*, C-92/09 i C-93/09.
([47]) ETS, wyrok w sprawie *Schecke*, pkt 81.
([48]) „Szybkie zamrożenie" dotyczy „zamrożenia" danych dotyczących ruchu i lokalizacji w odniesieniu do konkretnego podejrzanego od dnia zezwolenia sądu. „Szybie zamrożenie plus" również obejmuje „zamrożenie" danych już będących w posiadaniu operatorów do celów naliczania opłat i przesyłu.
([49]) Zob. s. 5 sprawozdania z oceny.
([50]) Zob. s. 32 sprawozdania z oceny.

IV.2. **Zatrzymywanie danych zgodnie z dyrektywą w sprawie zatrzymywania danych jednoznacznie wykracza poza to, co niezbędne**

58. Według EIOD informacje w sprawozdaniu z oceny nie zawierają wystarczającego potwierdzenia konieczności istnienia środka zatrzymywania danych w postaci przyjętej w dyrektywie w sprawie zatrzymywania danych. Sprawozdanie z oceny pozwala jednak na stwierdzenie, że dyrektywa w sprawie zatrzymywania danych reguluje zatrzymywanie danych w sposób wykraczający poza to, co niezbędne, lub co najmniej nie zapewnia niewykorzystywania zatrzymywania danych w taki sposób. W tej kwestii można podkreślić cztery elementy.

59. Po pierwsze, niejasny cel środka i szerokie pojęcie „właściwych władz krajowych" prowadzi do wykorzystania zatrzymywanych danych w zdecydowanie zbyt szerokim zakresie celów i przez zdecydowanie zbyt wiele organów. Ponadto brakuje konsekwencji w obostrzeniach i warunkach dostępu do danych. Na przykład do uzyskania dostępu nie we wszystkich państwach członkowskich konieczne jest uzyskanie wcześniejszego zatwierdzenia przez organy sądowe lub inne niezależne organy.

60. Po drugie, maksymalny okres zatrzymywania wynoszący dwa lata wydaje się wykraczać poza to, co konieczne. Dane statystyczne z wielu państw członkowskich w sprawozdaniu z oceny wskazują, że zdecydowana większość wniosków o dostęp dotyczy danych z ostatnich sześciu miesięcy: jest to 86 % ([51]). Ponadto szesnaście państw członkowskich w swoich przepisach zdecydowało się na okres zatrzymywania wynoszący jeden rok lub krótszy ([52]). To wyraźnie sugeruje, że maksymalny okres wynoszący dwa lata zdecydowanie wykracza poza to, co uznano za niezbędne w większości państw członkowskich.

61. Ponadto brak ustalonego wspólnego okresu zatrzymywania dla wszystkich państw członkowskich spowodował przyjęcie rozbieżnych przepisów krajowych, co może rodzić komplikacje, gdyż nie zawsze jest jasne, które prawo krajowe – zarówno w odniesieniu do zatrzymywania danych, jak i do ochrony danych – ma zastosowanie, jeżeli operatorzy przechowują dane w państwie członkowskim innym niż to, w którym dane są zbierane.

62. Po trzecie, poziom bezpieczeństwa nie jest wystarczająco zharmonizowany. Jeden z głównych wniosków grupy roboczej powołanej na mocy art. 29 zawartego w jej sprawozdaniu z lipca 2010 r. jest taki, że istnieje duża różnorodność środków bezpieczeństwa istniejących w poszczególnych państwach członkowskich. Komisja wydaje się uważać, że środki bezpieczeństwa w obecnej dyrektywie są wystarczające, ponieważ „nie ma konkretnych przykładów poważnego łamania prywatności" ([53]). Wydaje się jednak, że Komisja zwróciła się o informacje w tej kwestii wyłącznie do rządów państw członkowskich. W celu dokonania oceny przydatności obecnych przepisów i środków bezpieczeństwa potrzebne są szersze konsultacje

([51]) Zob. s. 22 sprawozdania z oceny. 12 % dotyczy danych z okresu sprzed 6 do 12 miesięcy, a 2 % – danych starszych niż rok.
([52]) Zob. s. 14 sprawozdania z oceny.
([53]) Zob. s. 30 sprawozdania z oceny.

i bardziej konkretne zbadanie przypadków nadużyć. Mimo że w tym kontekście nie mówi się o konkretnych przypadkach złamania zasad bezpieczeństwa, przypadki łamania bezpieczeństwa danych i skandale w obszarze danych przesyłowych i komunikacji elektronicznej w niektórych państwach członkowskich stanowią również czytelne ostrzeżenia. Do kwestii tej nie można podchodzić lekko, gdyż bezpieczeństwo zatrzymywanych danych ma kluczowe znaczenie dla samego systemu zatrzymywania danych, ponieważ zapewnia ona przestrzeganie wszystkich innych obostrzeń ([54]).

63. Po czwarte, ze sprawozdania nie wynika jasno, czy wszystkie kategorie zatrzymywanych danych rzeczywiście są niezbędne. Rozróżnia się tylko w sposób ogólny dane telefoniczne i internetowe. Niektóre państwa członkowskie zdecydowały się na wprowadzenie krótszego okresu zatrzymywania w odniesieniu do danych internetowych ([55]). Nie można jednak wyciągnąć z tego ogólnych wniosków.

IV.3. **Dyrektywie w sprawie zatrzymywania danych brakuje przewidywalności**

64. Kolejna słabość dyrektywy w sprawie zatrzymywania danych dotyczy jej braku przewidywalności. Wymóg przewidywalności wynika z ogólnego wymogu określonego w art. 8 ust. 2 Konwencji oraz art. 52 ust. 1 Karty praw podstawowych UE, zgodnie z którymi ingerencja powinna być określona w przepisach. Według Europejskiego Trybunału Praw Człowieka oznacza to, że środek powinien mieć podstawę prawną i być spójny z zasadą praworządności. Oznacza to, że prawo jest odpowiednio dostępne i przewidywalne ([56]). Trybunał Sprawiedliwości podkreślił w wyroku w sprawie *Österreichischer Rundfunk*, że przepisy należy formułować wystarczająco precyzyjnie, by obywatele mogli odpowiednio dostosować swoje postępowanie ([57]). Przepisy muszą wskazywać wystarczająco jasno zakres swobody właściwych władz i sposób jej wykonywania ([58]).

65. Również w liście sprawdzającej określonej w komunikacie Komisji w sprawie Karty praw podstawowych UE jedno z pytań, na które należy odpowiedzieć, dotyczy tego, czy wszelkie ograniczenie praw podstawowych jest sformułowane „w sposób jasny i przewidywalny" ([59]). W komunikacie poświęconym przeglądowi zarządzania informacjami w przestrzeni wolności, bezpieczeństwa i sprawiedliwości Komisja stwierdziła również, że obywatele „mają prawo wiedzieć, które z ich danych osobowych są przetwarzane i wymieniane, przez kogo i z jakiego powodu" ([60]).

66. W przypadku dyrektywy UE odpowiedzialność za zgodność z prawami podstawowymi, w tym z wymogiem przewidywalności, leży przede wszystkim w gestii państw członkowskich wdrażających dyrektywę do swojego prawa krajowego. Powszechnie znany jest wymóg, zgodnie z którym taka implementacja musi być zgodna z prawami podstawowymi ([61]).

67. Również w sprawozdaniu z oceny Komisja podkreśla, że dyrektywa „jako taka nie gwarantuje, że zatrzymywane dane są przechowywane, pozyskiwane i wykorzystywane z pełnym poszanowaniem prawa do prywatności i ochrony danych osobowych". Powołuje się na „odpowiedzialność państw członkowskich za zapewnienie przestrzegania tych praw" ([62]).

68. EIOD jest jednak zdania, że sama dyrektywa powinna w pewnym zakresie również spełniać wymóg przewidywalności. Reformułując wyrok Trybunału Sprawiedliwości w sprawie *Lindqvist*, systemowi określanemu w dyrektywie nie powinno „brakować przewidywalności" ([63]). Dotyczy to w szczególności środka UE, na mocy którego państwa członkowskie ingerują na szeroką skalę w prawo do prywatności i ochronę danych obywateli. EIOD jest zdania, że UE odpowiada za zapewnienie co najmniej jasnego określenia celu i tego, kto może uzyskać dostęp do danych oraz na jakich warunkach.

69. Takie stanowisko potwierdza nowy kontekst prawny wynikający z traktatu lizbońskiego, który, jak wyjaśniono, zwiększa kompetencje UE w zakresie współpracy policyjnej i sądowej w sprawach karnych i ustanawia silniejsze zobowiązanie UE do przestrzegania praw podstawowych.

70. EIOD pragnie przypomnieć, że wymóg określonego celu i wynikający z tego zakaz przetwarzania danych w sposób niezgodny z tym celem („zasada ograniczenia celu") mają podstawowe znaczenie dla ochrony danych osobowych, co potwierdza art. 8 Karty praw podstawowych UE ([64]).

71. Sprawozdanie z oceny pokazuje, że wybór pozostawienia państwom członkowskim precyzyjnego zdefiniowania, czym jest „poważne przestępstwo", a w konsekwencji, co należy uznać za „właściwe władze", doprowadził do wykorzystywania danych do wielu różnych celów ([65]).

72. Komisja stwierdza, że „większość państw członkowskich dokonujących transpozycji zgodnie z przepisami krajowymi umożliwia dostęp i wykorzystanie zatrzymywanych danych do celów wykraczających poza te określone w dyrektywie, w tym do ogólnego zapobiegania i zwalczania przestępczości oraz w sytuacjach zagrożenia życia" ([66]). Państwa członkowskie wykorzystają „lukę prawną" wynikającą z art. 15 ust. 1 dyrektywy o prywatności elektronicznej ([67]). Komisja uważa, że ta sytuacja może nie zapewniać

([54]) Zob. również w tej kwestii opinię EIOD z 2005 r., pkt 29–37. Zob. również wystąpienie zastępcy inspektora z dnia 4 maja 2011 r., które znajduje się na stronie internetowej EIOD (http://www.edps.europa.eu) w zakładce „Publications" >> „Speeches & Articles" >> „2011".
([55]) Zob. s. 14 sprawozdania z oceny.
([56]) Zob. Europejski Trybunał Praw Człowieka, wyrok w sprawie *S. i Marper*, o którym mowa w przypisie 7, pkt 151.
([57]) ETS, dnia 20 maja 2003 r., wyrok w sprawie *Österreichischer Rundfunk*, C-465/00, pkt 77 oraz Europejski Trybunał Praw Człowieka, wyrok w sprawie *S. i Marper*, o którym mowa w przypisie 7, pkt 95.
([58]) Zob. Europejski Trybunał Praw Człowieka, wyrok w sprawie *Malone*, o którym mowa w przypisie 8, pkt 66–68.
([59]) COM(2010) 573, o którym mowa w przypisie 31, s. 5.
([60]) COM(2010) 385, o którym mowa w przypisie 17, s. 3.
([61]) Zob. np. ETS, wyrok z dnia 6 listopada 2003 r. w sprawie *Lindqvist*, pkt 87.
([62]) Zob. s. 31 sprawozdania z oceny.
([63]) ETS, wyrok w sprawie *Lindqvist*, pkt 84.
([64]) Zob. również art. 6 dyrektywy 95/46/WE.
([65]) Zob. s. 8 sprawozdania z oceny.
([66]) Zob. s. 8 sprawozdania z oceny.
([67]) Zgodnie z omówieniem w pkt 24 powyżej.

wystarczającej „przewidywalności stanowiącej wymóg dla wszystkich środków prawnych ograniczających prawo do prywatności" ([68]).

73. W tych okolicznościach nie można stwierdzić, że sama dyrektywa w sprawie zatrzymywania danych, czytana w szczególności w połączeniu z dyrektywą o prywatności elektronicznej, zapewnia jasność niezbędną do spełnienia zasady przewidywalności na poziomie UE.

V. **ROZWIĄZANIA NA PRZYSZŁOŚĆ: NALEŻY ROZWAŻYĆ WSZYSTKIE OPCJE**

74. Analiza w poprzednich częściach uzasadnia wniosek, że dyrektywa w sprawie zatrzymywania danych nie spełnia wymogów ustalonych w prawie do poszanowania prywatności i ochrony danych. Jest więc oczywiste, że dyrektywa w sprawie zatrzymywania danych nie może dalej istnieć w obecnej formie. W związku z tym Komisja słusznie proponuje przegląd obecnych ram dla zatrzymywania danych ([69]).

75. Przed zaproponowaniem jednak zmienionej wersji dyrektywy:

a) Komisja powinna, podczas oceny wpływu, zaangażować się w zebranie większej liczby dowodów praktycznych z państw członkowskich, w celu wykazania niezbędności zatrzymywania danych jako środka w ramach prawa UE;

b) jeżeli większość państw członkowskich uważa, że zatrzymywanie danych jest konieczne, państwa te powinny dostarczyć Komisji dowody ilościowe i jakościowe, które to potwierdzą;

c) państwa członkowskie, które sprzeciwiają się takiemu środkowi zatrzymywania danych, powinny dostarczyć Komisji informacje umożliwiające dokonanie szerszej oceny tej kwestii.

76. W ocenie wpływu należałoby dodatkowo przeanalizować, czy alternatywne, mniej ingerujące w prywatność środki mogłyby prowadzić w przeszłości lub obecnie do porównywalnych wyników. Komisja powinna podjąć w tej kwestii inicjatywę, korzystając w razie potrzeby z zewnętrznego wsparcia ekspertów.

77. EIOD z radością przyjmuje fakt, że Komisja ogłosiła konsultacje obejmujące wszystkie zainteresowane strony podczas oceny wpływu ([70]). W związku z tym EIOD zachęca Komisję do znalezienia sposobów bezpośrednio angażujących obywateli w to zadanie.

78. Należy podkreślić, że ocena konieczności i analiza alternatywnych, mniej ingerujących w prywatność środków, może zostać przeprowadzona w uczciwy sposób wyłącznie wówczas, jeżeli wszystkie opcje dla przyszłej dyrektywy pozostaną otwarte. W związku z tym Komisja wydaje się wykluczać możliwość uchylenia dyrektywy, albo jako takiej, albo w połączeniu z wnioskiem w sprawie alternatywnego, bardziej ukierunkowanego środka UE. EIOD zwraca się więc do Komisji o poważne rozważenie również tych opcji w ocenie wpływu.

79. Przyszła dyrektywa w sprawie zatrzymywania danych może być rozważana wyłącznie w przypadku porozumienia, że potrzebne są przepisy UE z perspektywy rynku wewnętrznego oraz współpracy w sprawach karnych i sądowych oraz jeżeli, podczas oceny wpływu, można by wystarczająco wykazać konieczność zatrzymywania danych, popieraną i regulowaną przez UE, co obejmuje uważne przeanalizowanie środków alternatywnych.

80. EIOD nie podważa dużej wartości zatrzymywanych danych dla celów egzekwowania prawa oraz kluczowego znaczenia, jakie mogą one odegrać w konkretnych przypadkach. Podobnie jak niemiecki Bundesverfassungsgericht EIOD nie wyklucza, że dobrze zdefiniowany obowiązek zatrzymywania danych telekomunikacyjnych mógłby być uzasadniony w niektórych, bardzo ograniczonych, okolicznościach ([71]).

81. Każdy przyszły instrument UE w zakresie zatrzymywania danych powinien więc spełniać następujące podstawowe wymogi:

— być zrozumiały i w pełni harmonizować przepisy w zakresie obowiązku zatrzymywania danych oraz w sprawie dostępu i przyszłego wykorzystywania danych przez właściwe władze,

— być wyczerpujący, co oznacza, że ma jasny i precyzyjny cel oraz likwiduje lukę prawną, która istnieje w związku z art. 15 ust. 1 dyrektywy o prywatności elektronicznej,

— być proporcjonalny i nie wykraczać poza niezbędny zakres (zob. w tej kwestii uwagi zawarte w części IV.2 powyżej).

82. EIOD oczywiście szczegółowo przeanalizuje każdy przyszły wniosek w sprawie zatrzymywania danych w świetle tych podstawowych warunków.

VI. **WNIOSKI**

83. EIOD z zadowoleniem stwierdza, iż mimo że nie jest to ściśle wymagane zgodnie z art. 14 dyrektywy w sprawie zatrzymywania danych, Komisja uwzględniła również w sprawozdaniu z oceny implikacje dyrektywy dla praw podstawowych.

84. Sprawozdanie z oceny wskazuje, że dyrektywa nie osiągnęła swojego głównego celu, jakim jest harmonizacja ustawodawstw krajowych dotyczących zatrzymywania danych. Taki brak harmonizacji działa na niekorzyść wszystkich zainteresowanych stron: obywateli, przedsiębiorców oraz organów egzekwowania prawa.

85. Na podstawie sprawozdania z oceny można wnioskować, że dyrektywa w sprawie zatrzymywania danych nie spełnia wymogów wynikających z prawa do poszanowania prywatności i ochrony danych z następujących powodów:

— konieczność zatrzymywania danych, o której mowa w dyrektywie w sprawie zatrzymywania danych, nie została wystarczająco wykazana,

— zatrzymywanie danych mogłoby być regulowane w sposób mniej ingerujący w prywatność,

([68]) Zob. s. 9 i s. 15 sprawozdania z oceny.
([69]) Zob. s. 32–33 sprawozdania z oceny.
([70]) Zob. s. 32–33 sprawozdania z oceny.
([71]) Zob. Bundesverfasssungsgericht, 1 BvR 256/08.

— dyrektywie w sprawie zatrzymywania danych brakuje przewidywalności.

86. EIOD zwraca się do Komisji o poważne rozważenie wszystkich możliwości w ocenie wpływu, w tym możliwości samego uchylenia dyrektywy, albo jej uchylenia z wnioskiem w sprawie alternatywnego, bardziej ukierunkowanego środka UE.

87. Przyszła dyrektywa w sprawie zatrzymywania danych powinna być rozważana wyłącznie w przypadku porozumienia, że potrzebne są przepisy UE z perspektywy rynku wewnętrznego oraz współpracy w sprawach karnych i sądowych oraz jeżeli, podczas oceny wpływu, można by wystarczająco wykazać konieczność zatrzymywania danych, popieraną i regulowaną przez UE, co obejmuje uważne przeanalizowanie środków alternatywnych. Taki instrument powinien spełniać poniższe podstawowe wymagania:

— być zrozumiały i w pełni harmonizować przepisy w zakresie obowiązku zatrzymywania danych oraz w sprawie dostępu i przyszłego wykorzystywania danych przez właściwe władze,

— być wyczerpujący, co oznacza, że ma jasny i precyzyjny cel oraz likwiduje lukę prawną, która istnieje w związku z art. 15 ust. 1 dyrektywy o prywatności elektronicznej,

— być proporcjonalny i nie wykraczać poza niezbędny zakres.

Sporządzono w Brukseli dnia 31 maja 2011 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych