I

(Rezolucje, zalecenia i opinie)

OPINIE

EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Opinia Europejskiego Inspektora Ochrony Danych na temat bieżących negocjacji Unii Europejskiej w sprawie Umowy handlowej dotyczącej zwalczania obrotu towarami podrobionymi (ACTA)

(2010/C 147/01)

EUROPEJSKI INSPEKTOR OCHRONY DANYCH,

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

uwzględniając Kartę praw podstawowych Unii Europejskiej, w szczególności jej art. 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]), w szczególności jego art. 41,

PRZYJMUJE NINIEJSZĄ OPINIĘ:

I. WPROWADZENIE

1. Unia Europejska uczestniczy w negocjacjach w sprawie Umowy handlowej dotyczącej zwalczania obrotu towarami podrobionymi (ACTA). Negocjacje rozpoczęto w 2007 r. w ramach początkowej grupy zainteresowanych stron, a następnie kontynuowano w szerszym kręgu uczestników; obecnie wśród nich znajdują się Australia, Kanada, Unia Europejska, Japonia, Korea, Meksyk, Maroko, Nowa Zelandia, Singapur, Szwajcaria i Stany Zjednoczone Ameryki Północnej. Komisja Europejska otrzymała od Rady mandat na rozpoczęcie tych negocjacji w 2008 r.

2. EIOD przyznaje, że transgraniczny obrót towarami podrobionymi i pirackimi jest coraz większym problemem odnoszącym się do zorganizowanych sieci przestępczych, który wymaga przyjęcia odpowiednich mechanizmów współpracy na poziomie międzynarodowym w celu zwalczania tej formy przestępczości.

3. EIOD podkreśla, ze negocjacje prowadzone przez Unię Europejską w sprawie wielostronnej umowy, której głównym przedmiotem jest egzekwowanie praw własności intelektualnej, poruszają ważne kwestie odnoszące się do wpływu środków podejmowanych w celu zwalczania podrabiania i piractwa na prawa podstawowe osób fizycznych, a w szczególności na ich prawo do prywatności i ochrony danych.

4. EOID z tych względów szczególnie ubolewa, że Komisja Europejska nie skonsultowała z nim treści takiej umowy. EOID z własnej inicjatywy przyjął więc niniejszą opinię w oparciu o art. 41 ust. 2 rozporządzenia (WE) nr 45/2001 w celu dostarczenia Komisji wytycznych dotyczących aspektów prywatności i ochrony danych, które należałoby uwzględnić w trakcie negocjacji ACTA.

II. STAN PRAC I PRZEWIDYWANA TREŚĆ ACTA

5. Siódma runda negocjacji odbyła się w Meksyku w dniach 26–29 stycznia 2010 r., gdzie zaplanowano zawarcie umowy do końca 2010 r. Jak dotąd nie pojawił się żaden oficjalny projekt umowy.

([1]) Dz.U. L 281 z 23.11.1995, s. 31.
([2]) Dz.U. L 201 z 31.7.2002, s. 37.
([3]) Dz.U. L 8 z 12.1.2001, s. 1.

6. Negocjacje mają na celu przyjęcie nowej wielostronnej umowy na rzecz poprawy egzekwowania praw własności intelektualnej i zwalczania podrabiania towarów i piractwa. Ta nowa umowa, gdyby została przyjęta, ustanawiałby udoskonalone międzynarodowe normy w zakresie metod działania przeciwko naruszeniom praw własności intelektualnej na szeroką skalę. DG ds. Handlu Komisji Europejskiej w szczególności podkreśliła, że „w zamyśle nastawiono się na działania z zakresu podrabiania towarów i piractwa, które w znaczący sposób wpływają na interesy handlowe, a nie na działania zwykłych obywateli" ([4]).

7. Jeśli chodzi o treść umowy, *Summary of key elements under discussion* (Streszczenie kluczowych omawianych kwestii), wydane przez DG ds. Handlu Komisji Europejskiej w listopadzie 2009 r. wskazuje, że cel ACTA, jakim jest zwalczanie piractwa i podrabiania towarów, będzie realizowany w trzech formach: (i) współpraca międzynarodowa, (ii) praktyki z zakresu egzekwowania prawa i (iii) określenie ram prawnych dla egzekwowania praw własności intelektualnej w kilku określonych obszarach, a w szczególności w środowisku cyfrowym ([5]). Przewidywane środki będą w szczególności odnosiły się do procedury prawnych (takich jak nakazy sądowe, środki tymczasowe), roli i zakresu obowiązków dostawców usług internetowych w zapobieganiu naruszania praw autorskich w Internecie oraz środków współpracy transgranicznej w celu zapobiegania przewożeniu towarów przez granicę. Ogłoszone informacje jedynie zarysowują treść umowy i nie przedstawiają precyzyjnie żadnych szczegółowych, konkretnych środków.

8. EIOD uważa, że nawet jeśli zamierzonym celem ACTA jest zwalczanie naruszeń praw własności intelektualnej jedynie na szeroką skalę, nie sposób wykluczyć, że działalność zwykłych obywateli zostanie objęta ACTA, zwłaszcza że środki egzekwowania prawa są podejmowane w środowisku cyfrowym. EIOD podkreśla, że będzie konieczne przedstawienie odpowiednich gwarancji w celu ochrony praw podstawowych osób fizycznych. Ponadto przepisy z zakresu ochrony danych obejmują wszystkie osoby fizyczne, w tym tych, którzy są potencjalnie zaangażowani w podrabianie towarów i piractwo; zwalczanie naruszeń praw na szeroką skalę będzie się bez wątpienia wiązało z przetwarzaniem danych osobowych.

9. Z tych względów EIOD usilnie zachęca Komisję Europejską do przeprowadzenia publicznego i przejrzystego dialogu na temat ACTA, jeśli to możliwe – w ramach konsultacji społecznej, co pozwoliłoby również zapewnić zgodność środków, które mają zostać przyjęte, z wymogami europejskich przepisów odnoszących się do prywatności i ochrony danych.

([4]) Zob. http://trade.ec.europa.eu/doclib/docs/2009/november/tradoc_145271.pdf, s. 2.

([5]) Zob. przypis 2 powyżej.

III. **ZAKRES UWAG EIOD**

10. EIOD usilnie wzywa UE, a w szczególności Komisję Europejską, która otrzymała mandat do zawarcia umowy, do znalezienia właściwej równowagi pomiędzy zapotrzebowaniem na ochronę praw własności intelektualnej a prawem do prywatności i ochrony danych osób fizycznych.

11. EIOD podkreśla, że prywatność i ochrona danych to podstawowe wartości Unii Europejskiej uznane w art. 8 EKPC oraz art. 7 i 8 Karty praw podstawowych UE ([6]), których należy przestrzegać we wszystkich strategiach i przepisach przyjmowanych przez UE zgodnie z art. 16 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE).

12. Ponadto EIOD podkreśla, że porozumienie osiągnięte przez Unię Europejską w sprawie ACTA, musi być zgodne z prawnymi obowiązkami nałożonymi na UE w ramach przepisów o prywatności i ochronie danych, w szczególności zawartych w dyrektywie 95/46/WE, w dyrektywie 2002/58/WE ([7]) oraz w orzecznictwie Europejskiego Trybunału Praw Człowieka ([8]) i Trybunału Sprawiedliwości ([9]).

13. Prywatność i ochrona danych musi być uwzględniana od samego początku negocjacji, a nie po określeniu i uzgodnieniu systemów i procedur, gdy jest już zbyt późno na znalezienie alternatywnych rozwiązań z poszanowaniem prywatności.

14. Ze względu na małą ilość informacji udostępnionych publicznie EIOD uważa, że nie jest w stanie przedstawić analizy poszczególnych przepisów ACTA. W niniejszej opinii EIOD skoncentruje się więc na przedstawieniu potencjalnych zagrożeń dla prywatności i ochrony danych ze strony konkretnych przepisów, które, jak poinformowano, mogą dotyczyć następujących obszarów umowy: wprowadzenie w życie praw własności intelektualnej w środowisku cyfrowym (rozdział IV) oraz mechanizmy współpracy międzynarodowej (rozdział V).

([6]) Karta praw podstawowych Unii Europejskiej, Dz.U. C 303 z 14.12.2007, s. 1.

([7]) Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa w sprawie prywatności i łączności elektronicznej), Dz. U. L 201 z 31.7.2002, s. 37,

([8]) Zawierającym wykładnię głównych pojęć i warunków zawartych w art. 8 Europejskiej konwencji o ochronie praw człowieka i podstawowych wolności (EKPC), przyjętej w Rzymie w dniu 4 listopada 1950 r., z zastosowaniem ich do różnych dziedzin. Zob. w szczególności orzecznictwo przywołane w niniejszej opinii.

([9]) Zob. w szczególności: sprawa C-275/06, *Productores de Música de España* (Promusicae), Zb.Orz. z 2008, s. I-271 oraz sprawa C-557/07, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten*, nieopublikowana dotychczas w Zbiorze.

IV. EGZEKWOWANIE PRAW WŁASNOŚCI INTELEKTUALNEJ W ŚRODOWISKU CYFROWYM

IV.1. Potrzeba przeanalizowania skutków „polityki odłączania od Internetu po trzech ostrzeżeniach"

15. Według Komisji Europejskiej ACTA stworzy prawne ramy zwalczania piractwa w środowisku cyfrowym. ([10]) Ramy te ustanowią warunki, na jakich dostawcy usług internetowych i inni pośrednicy on-line ([11]) mogą zostać pociągnięci do odpowiedzialności w związku z naruszającym prawa autorskie materiałem przewijającym się przez ich systemy. Ramy mogą również obejmować prawa i drogi ich dochodzenia, jakie będzie można zastosować wobec użytkowników Internetu w związku z wysyłaniem lub pobieraniem przez nich materiału łamiącego prawa autorskie. Choć nie dostarczono oficjalnie szczegółowych informacji na temat takich ram, w świetle informacji dostępnych z różnych źródeł można prognozować, że mogą one obejmować nałożenie na dostawców usług internetowych obowiązku przyjęcia „polityki odłączania od Internetu po trzech ostrzeżeniach", zwanej również systemem „progresywnej reakcji". System ten umożliwi właścicielom praw autorskich monitorowanie użytkowników Internetu i identyfikowanie domniemanych sprawców naruszenia praw autorskich. Po skontaktowaniu się z dostawcą usług internetowych domniemanego sprawy naruszenia, dostawca ten ostrzegałby użytkownika zidentyfikowanego jako sprawca i użytkownikowi zostałby odebrany dostęp do Internetu po trzech ostrzeżeniach.

16. Równolegle do negocjacji ACTA polityka odłączania od Internetu po trzech ostrzeżeniach jest wdrażana w niektórych państwach członkowskich, takich jak Francja. Jest ona również omawiana na różnych europejskich forach, takich jak odbywający się obecnie Dialog zainteresowanych stron na temat wysyłania i pobierania danych, moderowany przez DG MARKT, w związku z przyjęciem Komunikatu Komisji w sprawie poprawy egzekwowania praw własności intelektualnej na rynku wewnętrznym ([12]). Dyskusja na ten temat jest również prowadzona w Parlamencie Europejskim w kontekście toczącej się debaty nad projektem Rezolucji Parlamentu Europejskiego w sprawie poprawy egzekwowania praw własności intelektualnej na rynku wewnętrznym (zwanej „sprawozdaniem Gallo").

17. Takie praktyki mocno ingerują w sferę prywatną osób fizycznych. Zezwalają na uogólnione monitorowanie działań użytkowników Internetu, w tym użytkowników postępujących całkowicie zgodnie z prawem. Odnoszą się do milionów praworządnych użytkowników Internetu, w tym wielu dzieci i nastolatków. Są prowadzone przez podmioty prywatne, nie przez organy ścigania. Ponadto, obecnie Internet odgrywa kluczową rolę niemal we wszystkich aspektach współczesnego życia, skutki odebrania dostępu do Internetu mogą być ogromne – odcięcie osób fizycznych od pracy, kultury, formularzy administracji elektronicznej itp.

18. W tym kontekście ważna jest ocena zakresu, w jakim polityka ta jest zgodna z europejskimi przepisami dotyczącymi ochrony danych i prywatności, a w szczególności zbadanie, czy polityka odłączania od Internetu po trzech ostrzeżeniach stanowi konieczny środek egzekwowania praw własności intelektualnej. W tej sytuacji należy ponadto przeanalizować, czy istnieją inne, mniej inwazyjne metody.

19. Nadal nie jest jasne, czy polityka odłączania do Internetu po trzech ostrzeżeniach będzie częścią ACTA. Polityka ta jest jednak również rozważana w innych obszarach i ma potencjalnie ogromny wpływ na ochronę danych osobowych i prywatność. Z tych powodów EIOD uznaje za konieczne omówienie je w niniejszej opinii. Przed wspomnianą analizą EIOD opisze pokrótce mające zastosowanie ramy prawne ochrony danych i prywatności.

20. Warto zauważyć, że obok ochrony danych i prywatności polityka odłączania od Internetu po trzech ostrzeżeniach budzi obawy w kontekście innych wartości, takich jak prawo do rzetelnego procesu sądowego i wolność słowa. W niniejszej opinii zajęto się jednak jedynie tymi kwestiami, które odnoszą się do ochrony danych osobowych i prywatności osób fizycznych.

IV.2. Polityka odłączania od Internetu po trzech ostrzeżeniach i mające zastosowanie europejskie ramy prawne ochrony danych/prywatności

W jaki sposób można wprowadzić politykę odłączania od Internetu po trzech ostrzeżeniach

21. W skrócie, w ramach polityki odłączania od Internetu po trzech ostrzeżeniach właściciele praw autorskich korzystający z automatyzowanych środków technicznych, dostarczanych również przez strony trzecie, zidentyfikowaliby domniemane naruszenie praw autorskich, uczestnicząc

([10]) Zob. przypis 2 powyżej.

([11]) Poszczególnych pośredników on-line można zdefiniować w zależności od pełnionej przez ich funkcji. W rzeczywistości pośrednicy często pełnią kilka tych funkcji jednocześnie. Do pośredników on-line zalicza się: (a) *Dostawcy usługi dostępu*: użytkownicy łączą się z siecią, łączą się z serwerem dostawcy usługi dostępu; (b) *dostawcy sieci*: dostarczają routery, tj. urządzenia techniczne niezbędne do przesyłu danych; (c) *dostawcy hosta*: wypożyczają miejsce na serwerze, na którym użytkownicy i dostawcy treści mogą zamieszczać treści. Użytkownicy mogą wysyłać i pobierać materiały z usług on-line, takich jak BBS i sieci P2P.

([12]) Komunikat Komisji do Rady, Parlamentu Europejskiego i Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie poprawy egzekwowania praw własności intelektualnej na rynku wewnętrznym, Bruksela, dnia 11 września 2009 r., COM(2009) 467 wersja ostateczna.

w monitorowaniu działań użytkowników Internetu, na przykład poprzez nadzór forów, blogów lub podszywając się pod osoby dzielące się plikami w sieciach *peer to peer* w celu zidentyfikowania osób dzielących się plikami, które przypuszczalnie wymieniają się materiałem objętym prawami autorskimi ([13]).

22. Po zidentyfikowaniu użytkowników Internetu dokonujących domniemanego naruszenia praw autorskich poprzez zebranie ich adresów Internet Protocol (adresów IP), właściciele praw autorskich przesyłaliby adresy IP tych użytkowników do właściwych dostawców usług internetowych, którzy ostrzegliby abonenta, do którego należy adres IP, o potencjalnym naruszeniu praw autorskich, którego się dopuścił. Kilkakrotne ostrzeżenie przez dostawcę usług internetowych prowadziłoby automatycznie do zerwania lub zawieszenia przez dostawcę podłączenia abonenta do Internetu ([14]).

Mające zastosowanie europejskie ramy prawne ochrony danych/prywatności

23. Polityka odłączania od Internetu po trzech ostrzeżeniach musi być zgodna z wymogami wynikającymi z prawa do prywatności, zgodnie z art. 8 EKPC oraz art. 7 Karty praw podstawowych, a także wynikającymi z prawa do ochrony danych zgodnie z art. 8 Karty praw podstawowych i art. 16 TFUE oraz dyrektywą 95/46/WE i dyrektywą 2002/58/WE.

24. Zdaniem EIOD monitorowanie zachowania użytkowników Internetu oraz w konsekwencji gromadzenie ich adresów IP kłóci się z prawem do poszanowania ich życia prywatnego i korespondencji; innymi słowy naruszone zostaje prawo do prywatności. Pogląd ten jest zgodny z orzecznictwem Europejskiego Trybunału Praw Człowieka ([15]).

25. Dyrektywa 95/46/WE znajduje zastosowanie ([16]), ponieważ polityka odłączania od Internetu po trzech ostrzeżeniach wiąże się z przetwarzaniem adresów IP, które – w każdym przypadków w odnośnych okolicznościach – należy uznać za dane osobowe. Adresy IP to identyfikatory, które są ciągiem liczb oddzielonych kropkami, na przykład 122.41.123.45. Abonament u dostawcy Internetu zapewnia abonentowi dostęp do Internetu. Za każdym razem, gdy abonent chce wejść do Internetu, zostanie mu przypisany adres IP za pośrednictwem urządzenia, którego używa w celu połączenia z Internetem (na przykład komputera) ([17]).

26. Jeśli użytkownik przeprowadza pewne czynności, na przykład wysyła materiał do sieci, może on zostać zidentyfikowany przez osoby trzecie za pomocą adresu IP, którego używa. Na przykład użytkownik o adresie IP 122.41.123.45 wysłał rzekomo materiał naruszający prawa autorskie do systemu P2P o godz. 15.00 w dniu 1 stycznia 2010 r. Dostawca usług internetowych będzie więc w stanie połączyć taki adres IP z nazwiskiem abonenta, do którego jest on przypisany, a więc będzie w stanie ustalić jego tożsamość.

27. Jeśli spojrzeć na definicję danych osobowych, o której mowa w art. 2 dyrektywy, 95/46/WE „wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (»osoby, której dane dotyczą«); osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na numer identyfikacyjny" ([18]), można dojść do wniosku, że adresy IP i informacje o działaniach związanych z takimi adresami stanowią dane osobowe we wszystkich przypadkach, które są tu brane pod uwagę. Adres IP służy bowiem za numer identyfikacyjny, który pozwala na odnalezienie nazwiska abonenta, któremu adres ten został przypisany. Ponadto zebrane informacje na temat abonenta, który posiada taki adres IP („dana osoba wysłała pewien materiał na stronę ZS o godz. 15.00 w dniu 1 stycznia 2010 r."), „dotyczą" tego abonenta, tzn. są wyraźnie na temat działań osoby możliwej do zidentyfikowania (właściciela adresu IP), a tym samym należy je również uznać za dane osobowe.

([13]) Technologia P2P jest rozproszoną architekturą oprogramowania komputerowego, która umożliwia podłączenie się indywidualnych komputerów i bezpośrednie ich łączenie z innymi komputerami.

([14]) Przykładem alternatywnych sankcji byłoby ograniczenie funkcjonalności połączenia internetowego, na przykład szybkości połączenia, ilości danych itp.

([15]) Zob. w szczególności decyzja Europejskiego Trybunału Praw Człowieka z dnia 26 czerwca 2006 r. w sprawie *Weber i Saravi przeciwko Niemcom*, nr 54934/00 WE, pkt 77 oraz wyrok Europejskiego Trybunału Praw Człowieka z dnia 1 lipca 2008 r. w sprawie *Liberty i inni przeciwko Zjednoczonemu Królestwu* nr 58243/00 WE.

([16]) Trybunał Sprawiedliwości przyjmuje szerokie podejście do zakresu stosowania dyrektywy 95/46/WE, której przepisy należy interpretować w świetle art. 8 EKPC. W wyroku z dnia 20 maja 2003 r. w sprawach połączonych C-465/00, C-138/01 i C-139/01 *Rundfunk*, Rec. z 2003, s. I-4989, pkt 68, Trybunał orzekł, że „przepisy dyrektywy 95/46/WE w zakresie, w jakim regulują przetwarzanie danych osobowych mogących naruszyć podstawowe wolności, a w szczególności prawo do życia prywatnego, koniecznie muszą być interpretowane w świetle praw podstawowych, które – zgodnie z utrwalonym orzecznictwem – stanowią integralną część ogólnych zasad prawa, których poszanowanie zapewnia Trybunał".

([17]) Adres IP, który dostawca usług internetowych przypisuje osobie może być zawsze taki sam, za każdym razem, gdy osoba surfuje po Internecie (zwany statycznym adresem IP). Niektóre adresy IP są dynamiczne co oznacza, że dostawca usługi dostępu do Internetu przypisuje inny adres IP do klientów za każdym razem, gdy podłączają się do Internetu. W sposób oczywisty dostawca usług internetowych może połączyć adres IP z kontem abonenta, któremu został przypisany ten (dynamiczny lub statyczny) adres IP.

([18]) Motyw 26 uzupełnia tę definicję: „Zasady ochrony danych muszą odnosić się do wszelkich informacji dotyczących zidentyfikowanych lub możliwych do zidentyfikowania osób; w celu ustalenia, czy daną osobę można zidentyfikować, należy wziąć pod uwagę wszystkie sposoby, jakimi może posłużyć się administrator danych lub inna osoba w celu zidentyfikowania owej osoby; zasady ochrony danych nie mają zastosowania do danych, którym nadano anonimowy charakter w taki sposób, że podmiot danych nie będzie mógł być zidentyfikowany; (…)"

28. Poglądy te podziela w pełni grupa robocza art. 29, która w dokumencie dotyczącym kwestii ochrony danych osobowych związanych z prawami własności intelektualnej stwierdza, że adresy IP zgromadzone w celu wyegzekwowania praw własności intelektualnej, tj. w celu zidentyfikowania użytkowników Internetu, którzy rzekomo naruszyli prawa własności intelektualnej, są danymi osobowymi, o ile są wykorzystywane do egzekwowania takich praw wobec danej osoby fizycznej ([19]).

29. Dyrektywa 2002/58/WE ma również zastosowanie, ponieważ polityka odłączania od Internetu po trzech ostrzeżeniach wymaga gromadzenia danych o ruchu i komunikacji. Dyrektywa 2002/58/WE reguluje wykorzystywanie takich danych i wprowadza zasadę poufności komunikacji w odniesieniu do publicznych sieci łączności i danych charakterystycznych dla tej łączności.

IV.3. **Czy polityka odłączania od Internetu po trzech ostrzeżeniach stanowi konieczny środek**

30. Art. 8 EKPC ustanawia zasadę konieczności, zgodnie z którą każdy środek, który narusza prawo osób fizycznych do prywatności jest dozwolony tylko wtedy, gdy w demokratycznym społeczeństwie stanowi środek konieczny dla uzasadnionego celu, jaki za nim stoi ([20]). Zasadę konieczności można również odnaleźć w art. 7 i 13 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE ([21]). Zasada wymaga analizy proporcjonalności środka, którą należy ocenić w oparciu o równowagę wchodzących w grę interesów, umieszczaną w kontekście społeczeństwa demokratycznego jako całości ([22]). Wiąże się ona dalej ze sprawdzeniem, czy istnieją alternatywne, mniej inwazyjne środki.

31. Choć EIOD zgadza się co do znaczenia egzekwowania praw własności intelektualnej, jest on zdania, że polityka odłączania od Internetu po trzech ostrzeżeniach w obecnej formie – tj. zawierająca pewne elementy o ogólnym zastosowaniu – stanowi nieproporcjonalny środek i nie może tym samym zostać uznana za środek konieczny. EIOD jest ponadto przekonany, że istnieją alternatywne, mniej inwazyjne rozwiązania lub też planowana polityka może być realizowana w mniej inwazyjny sposób lub w bardziej ograniczonym zakresie. Podejście odłączania Internetu po trzech ostrzeżeniach wiąże się z problemami również na bardziej szczegółowym poziomie prawa. Wnioski te zostały przedstawione poniżej.

Podejście odłączania Internetu po trzech ostrzeżeniach jest nieproporcjonalne

32. EIOD chciałby podkreślić dalekosiężny charakter wprowadzanych środków. W tym względzie należy podnieść następujące sprawy:

(i) fakt, że (niezauważalne) monitorowanie dotyczyłoby milionów osób fizycznych i *wszystkich* użytkowników, bez względu na to, czy są o coś podejrzani;

(ii) monitorowanie wiązałoby się z systematycznym rejestrem danych, z których niektóre mogłyby prowadzić do postępowania cywilnego albo nawet karnego; ponadto niektóre zgromadzone informacje zostałyby tym samym zaklasyfikowane do danych szczególnie chronionych zgodnie z art. 8 dyrektywy 95/46/WE, które wymagają mocniejszych środków zabezpieczających;

(iii) monitorowanie prawdopodobnie będzie prowadzić do wielu fałszywie pozytywnych przypadków. Naruszenie praw autorskich to nie prosta kwestia „tak" lub „nie". Często sądy muszą przeanalizować bardzo dużą ilość technicznych i prawnych szczegółów na setkach stron w celu ustalenia, czy miało miejsce naruszenie ([23]);

([19]) Dokument roboczy grupy roboczej art. 29 w sprawie zagadnień ochrony danych związanych z prawem własności intelektualnej, WP 104, przyjęty w dniu 18 stycznia 2005 r. Grupa robocza została ustanowiona na mocy art. 29 dyrektywy 95/46/WE. Jest to niezależny europejski organ doradczy w kwestiach ochrony danych i prywatności. Jej zadania zostały opisane w art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE. Zob. również opinia grupy roboczej 4/2007 w sprawie pojęcia danych osobowych (WP 136), przyjęta w dniu 20 czerwca 2007 r., w szczególności s. 16.

([20]) Artikuł 8 EKPC w sposób wyraźny odnosi się do wymogu, by jakakolwiek ingerencja lub ograniczenie było „konieczne w demokratycznym społeczeństwie".

([21]) Artikuł 13 dyrektywy 95/46/WE zezwala na ograniczenie tylko wtedy, gdy stanowi ono „środek konieczny dla zabezpieczenia: a) bezpieczeństwa narodowego; b) obronności; c) bezpieczeństwa publicznego; d) działań prewencyjnych, prowadzonych czynności dochodzeniowo-śledczych i prokuratorskich w sprawach karnych lub sprawach o naruszenie zasad etyki w zawodach podlegających regulacji; e) ważnego interesu ekonomicznego lub finansowego państwa członkowskiego lub Unii Europejskiej, łącznie z kwestiami pieniężnymi, budżetowymi i podatkowymi; f) funkcji kontrolnych, inspekcyjnych i regulacyjnych związanych, nawet sporadycznie, z wykonywaniem władzy publicznej w przypadkach wymienionych w lit. c)–e); g) ochrony osoby, której dane dotyczą oraz praw i wolności innych osób". Artikuł 15 dyrektywy 2002/58/WE wymaga, by „takie ograniczenie stanowi[ło] środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego (i.e. bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej, jak określono w art. 13 ust. 1 dyrektywy 95/46/WE".

([22]) Zob. również wyrok Europejskiego Trybunału Praw Człowieka z dnia 2 sierpnia 1984 r. w sprawie *Malone przeciwko Zjednoczonemu Królestwu*, Seria A nr 82, pkt 81 i kolejne oraz wyrok Europejskiego Trybunału Praw Człowieka w sprawie *S. i Marper przeciwko Zjednoczonemu Królestwu* [Wielka Izba], nr 30562/04 i 30566/04, pkt 101 i kolejne.

([23]) Sądy mogą musieć ocenić, czy materiał jest rzeczywiście chroniony prawami autorskimi, jakie prawa zostały naruszone, czy wykorzystanie można uznać za przypadek uczciwego wykorzystania oraz określić właściwe prawo, szkody itp.

(iv) potencjalne *skutki* monitorowania, do których może prowadzić odłączenie od Internetu. To mogłoby kłócić się z wolnością wyrażania opinii osób fizycznych, prawem do informacji i dostępu do kultury, formularzy administracji elektronicznej, rynków, poczty elektronicznej, a w niektórych przypadkach, działań związanych z pracą. W tym kontekście szczególnie ważne jest, by zdać sobie sprawę, że skutki odczują nie tylko domniemani sprawcy naruszeń, ale również krewni, którzy korzystają z tego samego połączenia internetowego, w tym dzieci w wieku szkolnym, które wykorzystują Internet do zadań szkolnych,

(v) fakt, że podmiot dokonujący oceny i podejmujący decyzję będzie zazwyczaj prywatnym podmiotem (tj. właścicielem praw autorskich lub dostawcą usług internetowych). EIOD wyraził już w poprzedniej opinii swoje obawy odnoszące się do monitorowania osób fizycznych przez sektor prywatny (tj. dostawców usług internetowych lub właścicieli praw autorskich), w obszarach, które zasadniczo podlegają organom ścigania ([24]).

33. EIOD nie jest przekonany, że korzyści ze środków zrównoważą skutki dla praw podstawowych osób fizycznych. Ochrona praw autorskich leży w interesie właścicieli praw i społeczeństwa. Ograniczenie praw podstawowych nie wydaje się jednak uzasadnione, jeśli powagę ingerencji, tj. skalę naruszenia prywatność jak wskazują powyższe kwestie, równoważy się oczekiwanymi korzyściami, zapobiegając naruszeniom praw własności intelektualnej, które w dużej części są naruszeniami własności intelektualnej na mała skalę. Jak wskazano w opinii rzecznika generalnego Kokott w sprawie *Promusicae*: „Nie jest […] pewne, czy wymiana plików między podmiotami prywatnymi, w szczególności gdy nie odbywa się ona w celach zarobkowych, zagraża ochronie praw autorskich na tyle poważnie, by uzasadnić zastosowanie tego odstępstwa". Zakres szkody wyrządzonej w następstwie wymiany plików między podmiotami prywatnymi stanowi bowiem kwestię wzbudzającą kontrowersje ([25]).

34. W tym kontekście warto również przywołać reakcję Parlamentu Europejskiego na „systemy z trzema ostrzeżeniami" w kontekście przeglądu pakietu telekomunikacyjnego, w szczególności poprawka 138 do dyrektywy ramowej ([26]). W poprawce tej stwierdzono, że jakiekolwiek ograniczenie praw podstawowych lub wolności może mieć miejsce, jeśli jest ono odpowiednie, proporcjonalne i konieczne w społeczeństwie obywatelskim, a jej wdrożenie powinno podlegać odpowiednim gwarancjom proceduralnym zgodnym z EKPC i z ogólnymi zasadami prawa wspólnotowego, w tym z zasadą skutecznej ochrony sądowej i zasadą rzetelnego procesu ([27]).

35. W tym względzie EIOD podkreśla ponadto, że jakiekolwiek ograniczanie praw podstawowych będzie podlegać szczegółowej analizie na poziomie europejskim i krajowym. W tym kontekście można dopatrzyć się analogi z dyrektywą w sprawie zatrzymywania danych 2006/24/WE ([28]), która odstępuje od ogólnej zasady ochrony danych, jaką jest usuwanie danych, gdy nie są one już niezbędne dla celu, dla jakiego były gromadzone. Dyrektywa ta wymaga, by dane o ruchu były zatrzymywane dla celów zwalczania poważnych przestępstw. Należy zauważyć, że zatrzymywanie danych jest dopuszczalne tylko w odniesieniu do „poważnych przestępstw", że zatrzymywanie jest ograniczone do „danych o ruchu", które zasadniczo wykluczają informacje o treści komunikatów, a także że wprowadzone są mocne gwarancje. Pojawiały się jednak wątpliwości co do zgodności tego procederu ze standardami w zakresie praw podstawowych; Trybunał konstytucyjny Rumunii orzekł, że powszechne zatrzymywanie danych jest niezgodne z prawami podstawowymi ([29]), a obecnie toczy się sprawa przed trybunałem konstytucyjnym Niemiec ([30]).

Istnienie innych, mniej inwazyjnych środków

36. Powyższe wnioski wzmacnia fakt, że istnieją mniej inwazyjne środki do osiągnięcia tego samego celu. EIOD podkreśla, że takie mniej inwazyjne modele powinny zostać przeanalizowane i wypróbowane.

([24]) Opinia Europejskiego Inspektora Ochrony Danych z dnia 23 czerwca 2008 r. na temat wniosku dotyczącego decyzji Parlamentu Europejskiego i Rady w sprawie ustanowienia wieloletniego wspólnotowego programu ochrony dzieci korzystających z Internetu i z innych technologii komunikacyjnych, Dz.U. C 2 z 7.1.2009, s. 2.

([25]) Zob. sprawa, o której mowa w przypisie 8, pkt 106.

([26]) Zob. dyrektywa 2009/140/WE Parlamentu Europejskiego i Rady z dnia 25 listopada 2009 r., Dz.U. L 337 z 18.12.2009, s. 37.

([27]) Tzw. poprawka 138 otrzymała ostatecznie następujące brzmienie: „Artykuł 3a. Stosując środki związane z dostępem użytkowników końcowych – za pomocą sieci łączności elektronicznej – do usług i aplikacji lub z korzystaniem taką drogą z usług lub aplikacji, państwa członkowskie respektują podstawowe prawa i wolności osób fizycznych gwarantowane w Europejskiej konwencji o ochronie praw człowieka i podstawowych wolności oraz w ogólnych zasadach prawa wspólnotowego. Jeżeli jakikolwiek ze środków związanych z dostępem użytkowników końcowych – za pomocą sieci łączności elektronicznej – do usług i aplikacji lub z korzystaniem taką drogą z usług lub aplikacji mógłby ograniczyć wspomniane podstawowe prawa lub wolności, można go nałożyć wyłącznie wtedy, gdy jest odpowiedni, proporcjonalny i konieczny w demokratycznym społeczeństwie, a jego wdrożenie podlega odpowiednim gwarancjom proceduralnym zgodnym z Europejską konwencją o ochronie praw człowieka i podstawowych wolności i z ogólnymi zasadami prawa wspólnotowego, w tym z zasadą skutecznej ochrony sądowej i zasadą rzetelnego procesu. Środki takie można więc zastosować wyłącznie z należytym poszanowaniem zasady domniemania niewinności i prawa do prywatności. Gwarantuje się uprzednią rzetelną i bezstronną procedurę, uwzględniającą prawo zainteresowanej osoby lub zainteresowanych osób do bycia wysłuchanymi, z zastrzeżeniem potrzeby ustanowienia dla należycie ustalonych pilnych przypadków odpowiednich warunków oraz zabezpieczeń proceduralnych zgodnych z Europejską konwencją o ochronie praw człowieka i podstawowych wolności. Gwarantuje się prawo do skutecznej kontroli sądowej w rozsądnym terminie".

([28]) Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r., Dz.U. L 105 z 13.4.2006, s. 54.

([29]) http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html

([30]) http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg09-124.html

37. W tym kontekście EIOD przypomina, że zmieniona dyrektywa 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników (zwana dalej „dyrektywą o prawach obywateli"), która jest częścią zreformowanego ostatnio pakietu telekomunikacyjnego, zawiera pewne zasady i procedury ograniczające naruszanie praw autorskich wśród konsumentów na małą skalę ([31]). Takie procedury obejmują obowiązek państw członkowskich dostarczenia znormalizowanych informacji użyteczności publicznej dotyczące różnych zagadnień, w szczególności mówiące o naruszeniach praw autorskich i praw pokrewnych oraz konsekwencjach prawnych tych czynów ([32]). Państwa członkowskie mogą zwrócić się do dostawców usług informatycznych o rozpowszechnianie ich wśród swoich klientów i włączenia ich do umów.

38. System ma na celu informowanie, odwodzenie osób fizycznych od rozpowszechniania informacji objętych prawami autorskimi i uczestniczenia w działaniach naruszających takie prawa, unikając przy tym monitorowania użytkowników Internetu i związanych z tym problemów odnoszących się do prywatności i ochrony danych. Dyrektywa o prawach obywateli musi zostać wdrożona do maja 2011 r.; nie wprowadzono więc jeszcze takich procedur. Nie było jeszcze tym samym okazji, by sprawdzić płynące z nich korzyści. Pominięcie potencjalnych korzyści z tych nowych procedur i przyjęcie w zamian „polityki odłączania po trzech ostrzeżeniach", które w o wiele większym stopniu ograniczają prawa podstawowe, wydaje się przedwczesne.

39. Ponadto należy przypomnieć, że dyrektywa 2004/48/WE Parlamentu Europejskiego i Rady z dnia 28 kwietnia 2004 r. w sprawie egzekwowania praw własności intelektualnej zawiera różne narzędzia do egzekwowania praw własności intelektualnej przed sądami (omówione szerzej w pkt 43 i kolejnych) ([33]).

40. Dyrektywa w sprawie egzekwowania praw własności intelektualnej dopiero niedawno została przetransponowana do przepisów państw członkowskich. Jak dotąd nie upłynęła odpowiednia ilość czasu, by móc ocenić, czy jej przepisy są właściwe dla celu, jakim jest egzekwowanie praw własności intelektualnej. Stąd konieczność zastąpienia obecnego systemu opartego na postępowaniu sądowym, który nie został jeszcze przetestowany, jest co najmniej wątpliwa. Powyższe rozważania prowadzą w sposób nieunikniony do pytania, dlaczego istniejących naruszeń nie można odpowiednio zwalczać istniejącymi sankcjami cywilnymi i karnymi w odniesieniu do naruszenia praw autorskich. Przed zaproponowaniem takich środków polityki Komisja powinna więc dostarczyć wiarygodnych informacji pokazujących, że obecne ramy prawne nie przyniosły zamierzonych skutków.

41. Ponadto nie jest jasne, czy poważnie rozważono alternatywne modele ekonomiczne, które nie wiązałyby się z systematycznym monitorowaniem osób fizycznych. Dla przykładu, jeśli właściciele praw autorskich wykażą poniesione straty w wyniku zastosowania systemu P2P, właściciele praw i dostawcy usług internetowych mogą, na przykład, przetestować zróżnicowane abonamenty internetowe, w których część opłaty za abonament z nieograniczonym dostępem jest rozdzielana między właścicielami praw autorskich.

Możliwość prowadzenia ukierunkowanego monitorowania w mniej inwazyjny sposób

42. Abstrahując od wykorzystania całkowicie innych modeli, które jak wskazano, powinny zostać przeanalizowane i przetestowane, ukierunkowane monitorowanie można by prowadzić w mniej inwazyjny sposób.

43. Cel egzekwowania praw własności intelektualnej można również osiągnąć poprzez monitorowanie jedynie ograniczonej liczby osób fizycznych podejrzanych o udział w poważnych naruszeniach praw autorskich. Dyrektywa w sprawie egzekwowania praw własności intelektualnej dostarcza pewnych wskazówek w tym względzie. Ustanawia warunki, w których organy mogą zażądać udostępnienia danych osobowych przechowywanych przez dostawców usług internetowych w celu egzekwowania praw własności intelektualnej. Artikuł 8 tej dyrektywy stanowi, że dostawcy usług internetowych mogą zostać poproszeni przez właściwe organy prawne o dostarczenie danych osobowych, które przechowują na temat domniemanych sprawców naruszeń (np. informacji o pochodzeniu i sieciach dystrybucji towarów lub usług, które naruszają prawo własności intelektualnej) w odpowiedzi na uzasadniony i proporcjonalny wniosek w przypadkach naruszenia na skalę handlową ([34]).

44. Kryterium „skali handlowej" jest zatem decydujące. Zgodnie z tym kryterium monitorowanie może być proporcjonalne w kontekście ograniczonych, szczególnych doraźny sytuacji, w których istnieją w pełni uzasadnione podejrzenia

([31]) Zob. dyrektywa 2009/136/WE Parlamentu Europejskiego i Rady z dnia 25 listopada 2009 r., Dz.U. L 337 z 18.12.2009, s. 11.

([32]) W szczególności art. 21 ust. 4 dyrektywy 2009/136/WE stanowi, że „Państwa członkowskie mogą wymagać, aby przedsiębiorstwa, o których mowa w ust. 3, w odpowiednich przypadkach nieodpłatnie rozpowszechniały informacje użyteczności publicznej wśród aktualnych i nowych abonentów za pomocą tych samych środków, jakie zwykle wykorzystują one w komunikacji z abonentami. W takim przypadku informacje te są dostarczane w znormalizowanej formie przez właściwe organy publiczne i dotyczą między innymi następujących zagadnień: a) najpowszechniejszych sposobów wykorzystywania usług łączności elektronicznej do działań niezgodnych z prawem lub do rozpowszechniania szkodliwych treści – zwłaszcza w przypadku gdy może to naruszać prawa i wolności innych osób – w tym przypadków naruszania praw autorskich i praw pokrewnych oraz konsekwencji prawnych tych czynów (…)." Ponadto zgodnie z art. 20 ust. 2 „Państwa członkowskie mogą także wymagać, aby umowa zawierała wszelkie informacje, które mogą zostać dostarczone w tym celu przez właściwe organy publiczne, o wykorzystywaniu sieci i usług łączności elektronicznej do działań niezgodnych z prawem lub do rozpowszechniania szkodliwych treści oraz o sposobach ochrony bezpieczeństwa, prywatności i danych osobowych, o których mowa w art. 21 ust. 4 i które mają związek ze świadczoną usługą."

([33]) Dz.U. L 157 z 30.4.2004, s. 45 (zwana dalej dyrektywą w sprawie egzekwowania praw własności intelektualnej).

([34]) Potwierdzono to w motywie 14 dyrektywy w sprawie egzekwowania praw własności intelektualnej.

naruszenia praw autorskich na skalę handlową. Kryterium to mogłoby obejmować sytuacje wyraźnego naruszenia praw autorskich przez prywatne osoby w celu osiągnięcia bezpośrednich lub pośrednich korzyści handlowych.

45. W praktyce, aby powyższa metoda było skuteczna, właściciele praw autorskich mogliby podjąć się ukierunkowanego monitorowania niektórych adresów IP w celu sprawdzenia skali naruszenia praw autorskich. To oznaczałoby, że właściciele prawa autorskich mogliby również śledzić doniesienia o naruszeniu do tych samych celów. Takie informacje powinny być wykorzystywane wyłącznie po sprawdzeniu zakresu naruszenia – dla przykładu jasne przypadki większych naruszeń oraz niewielkie, ale ciągłe naruszenia, trwające przez pewien czas, w celu osiągnięcia korzyści handlowej lub finansowej. Poniżej podkreślono i objaśniono szczegółowo, przy omawianiu zasady przechowywania danych, konieczność ciągłości w pewnych okresach.

46. Oznaczałoby to, że w takich przypadkach gromadzenie danych w celu wykazania domniemanego naruszenia w Internecie może zostać uznane za proporcjonalne i konieczne w celu przygotowania postępowania prawnego, w tym sądowego.

47. EIOD uważa, że w ramach dodatkowej gwarancji operacje przetwarzania danych mające na celu zbieranie tego typu dowodów powinny najpierw zostać sprawdzone i uwierzytelnione przez krajowe organy ochrony danych. Opinia ta jest oparta na fakcie, że operacje przetwarzania danych wiązałyby się ze szczególnymi zagrożeniami dla praw i wolności osób fizycznych w świetle przyświecających im celów, tj. prowadzenia działań z zakresu egzekwowania prawa, które mogą być w końcu przestępcze, a także w świetle szczególnie chronionego charakteru gromadzonych danych. Fakt, że przetwarzanie danych wiąże się z monitorowaniem elektronicznych komunikatów jest dodatkowym czynnikiem, który wskazuje na potrzebę zwiększonego nadzoru.

48. EIOD uważa, że „skala handlowa" włączona do dyrektywy w sprawie egzekwowania praw własności intelektualnej wyjątkowo nadaje się do wyznaczenia granic monitorowania w celu przestrzegania zasady proporcjonalności. Ponadto nie wydaje się, by istniał wiarygodny dowód wskazujący w ramach kryteriów określonych w dyrektywie w sprawie egzekwowania praw własności intelektualnej, że wystąpienie na drogę sądową przeciwko naruszeniu praw autorskich okazuje się niemożliwe i nieskuteczne. Dla przykładu takie raporty jak z Niemiec, gdzie od 2008 r., po transpozycji dyrektywy w sprawie egzekwowania praw własności intelektualnej, odnotowano około 3 000 nakazów sądowych, w wyniku których dostawcy usług internetowych udostępnili sądom informacje abonenckie 300 000 abonentów, wydają się wskazywać odwrotnie.

49. Podsumowując, ponieważ dyrektywa w sprawie egzekwowania praw własności intelektualnej obowiązuje dopiero od dwóch lat, trudno zrozumieć, dlaczego ustawodawcy przeszliby od kryteriów zawartych w tej dyrektywie do bardziej inwazyjnych metod, kiedy UE dopiero wypróbowuje środki przyjęte przez nią ostatnio. Z tych samych względów trudno również zrozumieć konieczność zastąpienia obecnego systemu opartego na sądownictwie innym rodzajem środków (obok pojawiających się kwestii prawo do rzetelnego procesu sądowego, których tutaj nie omówiono).

IV.4. **Zgodność polityki odłączania od Internetu po trzech ostrzeżeniach z bardziej szczegółowymi przepisami dotyczącymi ochrony danych**

50. Istnieją inne, bardzie szczegółowe powody prawne, dla których podejście z trzema ostrzeżeniami jest problematyczne z punktu widzenia ochrony danych. EIOD chciałby podkreślić wątpliwą podstawę prawną przetwarzania danych, której wymaga dyrektywa 95/46/WE oraz wymóg zawarty w dyrektywie 2002/58/WE usuwania plików dziennika systemowego.

Podstawa prawna przetwarzania danych

51. Systemy z trzema ostrzeżeniami wiążą się z przetwarzaniem danych osobowych, z których niektóre będą wykorzystywane w postępowaniu sądowym lub administracyjnym zmierzającym do odcięcia od Internetu osób nagminnie dopuszczających się naruszeń. Z tej perspektywy dane takie są zaliczane do szczególnie chronionych zgodnie z art. 8 dyrektywy 95/46/WE. Artikuł 8 ust. 5 stanowi, że „przetwarzanie danych dotyczących przestępstw, wyroków skazujących lub środków bezpieczeństwa może być dokonywane jedynie pod kontrolą władz publicznych, lub też, jeżeli zgodnie z prawem krajowym ustanowiono określone środki zabezpieczające".

52. W tym kontekście warto przypomnieć przytoczony powyżej dokument grupy roboczej art. 29, w którym omówiono kwestię przetwarzania danych sądowych ([35]). Grupa robocza stwierdza, że „pojedyncze osoby mają oczywiście prawo przetwarzać dane sądowe w związku ze swoją sprawą sądową, jednak zasada ta nie umożliwia dogłębnego śledzenia, gromadzenia ani centralizacji danych osobowych przez strony trzecie, w tym zwłaszcza systematycznych badań na szeroka skalę, takich jak przeszukiwanie Internetu (…)." Takie poszukiwania należą do zadań organów sądowych ([36]). O ile gromadzenie ukierunkowanych, konkretnych dowodów, w szczególności w sprawach o poważne naruszenia, może być konieczne w celu złożenia skargi i prowadzenia sporu, EIOD w pełni podziela opinię grupy roboczej art. 29 na temat braku uzasadnienia dla zakrojonych na szeroką skalę poszukiwań wiążących się z przetwarzaniem masowych ilości danych użytkowników Internetu.

53. Powyższe omówienie zasady proporcjonalności i kryterium „skali handlowej" są ważne dla ustalenia, w jakich warunkach gromadzenie adresów IP i powiązanych informacji będzie uzasadnione.

([35]) Zob. pkt 28 niniejszej opinii.
([36]) Podkreślenia własne.

54. Dostawcy usług internetowych mogą próbować uzasadniać przetwarzanie danych przez właścicieli praw autorskich, zamieszczając w umowach klientów klauzule pozwalające na monitorowanie ich danych i unieważnianie abonamentu. Uznawałoby, że klienci, zawierając takie umowy, wyrazili zgodę na monitorowanie. Praktyka ta wiąże się, po pierwsze, z podstawowym pytaniem, czy osoby fizyczne mogą wyrazić zgodę dostawcom usług internetowych na przetwarzanie danych, którego dokonają nie dostawcy a osoby trzecie „niepodlegające" tym dostawcom.

55. Po drugie pojawia się kwestia ważności zgody. Artikuł 2 lit. h) dyrektywy 95/46/WE definiuje zgodę jako „konkretne i świadome, dobrowolne wskazanie przez osobę, której dane dotyczą na to, że wyraża przyzwolenie na przetwarzanie odnoszących się do niej danych osobowych." Ważne jest to, że by zgoda była ważna, bez względu na okoliczności, w których jest udzielana, musi być konkretnym, świadomym i dobrowolnym wskazaniem przyzwolenia przez osobę, które dane dotyczą, zgodnie z art. 2 lit. h) dyrektywy. EIOD ma poważne wątpliwości, czy osoby fizyczne poproszone o wyrażenie zgody na monitorowanie swoich działań w Internecie będą miały szansę dokonać rzeczywistego wyboru – zwłaszcza że alternatywą będzie brak dostępu do Internetu, co potencjalnie wpłynęłoby negatywnie na wiele innych obszarów ich życia.

56. Po trzecie, bardzo wątpliwe, czy takie monitorowanie mogłoby kiedykolwiek uznane za *konieczne* do wykonania umowy, której stroną jest osoba, której dane dotyczą, czego wymaga art. 7 lit. b) dyrektywy 95/46/WE, ponieważ monitorowanie nie jest w sposób oczywisty przedmiotem umowy zawartej z osobą, której dane dotyczą, a jedynie środkiem dostawców usług internetowych do innych celów.

Usuwanie plików dziennika systemowego

57. Zgodnie z dyrektywą 2002/58/WE, a w szczególności jej art. 6, dane o ruchu, takie jak adresy IP, mogą być gromadzone i przechowywane wyłącznie ze względów bezpośrednio związanych z samym komunikatem, w tym w celu naliczania opłat, zarządzania ruchem i zapobiegania oszustwom. Następnie dane należy usunąć. Dzieje się tak bez uszczerbku dla wymogów zawartych w dyrektywie w sprawie zatrzymywania danych, która, jak wskazano, wymaga zachowania danych o ruchu i udostępnienia ich policji i prokuratorom w ramach wspierania ścigania **wyłącznie poważnych przestępstw** ([37]).

([37]) Zob. pkt 35 niniejszej opinii.

58. Zgodnie z powyższym dostawcy usług internetowych powinni usuwać pliki dziennika systemowego zawierające informacje o działaniach użytkowników Internetu, które nie są już niezbędne dla powyższych celów. Biorąc pod uwagę, że pliki dziennika systemowego nie są niezbędne dla naliczania opłat, wydaje się, że trzy lub cztery tygodnie powinny być wystarczające dla dostawców usług internetowych do zarządzania ruchem ([38]).

59. To oznacza, że jeśli właściciele praw autorskich kontaktują się z dostawcami usług internetowych, o ile kontakt taki nie wystąpi w krótkim, wskazanym powyżej okresie, dostawcy nie powinni być w posiadaniu plików dziennika systemowego, łączących adresy IP z odpowiednimi abonentami. Przechowanie plików dziennika systemowego po tym okresie powinno mieć miejsce tylko z uzasadnionych względów, w ramach celów określonych w prawie.

60. W praktyce oznacza to, że prośby właściciela praw autorskich kierowane do dostawców usług internetowych, o ile nie nastąpią bardzo szybko, nie będą mogły zostać spełnione, zwyczajnie, dlatego że dostawcy nie będą już posiadali takich informacji. To samo w sobie wyznacza granice tego, co kryje się pod dopuszczalnymi praktykami monitorowania opisanymi w powyższej części.

Ryzyko skutków ubocznych

61. EIOD niepokoi nie tylko wpływ polityki odłączania od Internetu po trzech ostrzeżeniach na prywatność i ochronę danych, ale również jej skutki uboczne. Zezwolenie na politykę odłączania od Internetu po trzech ostrzeżeniach jest na prostej drodze do zalegalizowania bardziej masowego nadzoru działań użytkowników Internetu, w różnych dziedzinach i dla różnych celów.

62. EDPS zaleca Komisji dopilnowanie, by ACTA nie wychodziła poza i przeciwko obecnemu europejskiemu systemowi egzekwowania praw własności intelektualnej, który przestrzega praw podstawowych, wolności i swobód obywatelskich, takich jak ochrona danych osobowych.

V. **KWESTIE OCHRONY DANYCH W ODNIESIENIU DO MECHANIZMÓW WSPÓŁPRACY MIĘDZYNARODOWEJ**

63. Jednym ze środków zaproponowanych przez uczestników ACTA w celu rozwiązania kwestii egzekwowania praw własności intelektualnej jest wzmocnienie współpracy

([38]) Zarządzanie ruchem obejmuje analizę ruchu w sieci komputerowej w celu zoptymalizowania lub zagwarantowania jej wydajnego funkcjonowania, zmniejszenia opóźnienia lub zwiększenia przepustowości łącza.

międzynarodowej, z wieloma środkami, które umożliwiłyby skuteczne egzekwowanie takich praw w sądach sygnatariuszy ACTA.

64. W świetle dostępnych informacji można spodziewać się, że wiele środków planowanych w celu zapewnienia egzekwowania praw własności intelektualnej będzie wiązało się z międzynarodową wymianą informacji na temat domniemanych naruszeń praw własności intelektualnych pomiędzy organami publicznymi (takimi jak organy celne, policja i sądy), ale również pomiędzy podmiotami publicznymi i prywatnymi (takimi jak dostawcy usług internetowych, organizacje właścicieli praw własności intelektualnej). Takie przekazywanie danych budzi wiele wątpliwości z punktu widzenia ochrony danych.

V.1. **Czy wymiana danych rozważana w kontekście ACTA jest uzasadniona, konieczna i proporcjonalna?**

65. Na obecnym etapie negocjacji, na którym wielu konkretnych kwestii przetwarzania danych nadal nie określono albo nie omówiono, nie sposób sprawdzić, czy zaproponowane ramy środków są zgodne z podstawowymi zasadami ochrony danych i europejskimi przepisami dotyczącymi ochrony danych.

66. Na wstępie można zastanawiać się, czy przekazywanie danych do państw trzecich w kontekście ACTA jest uzasadnione. Zasadność przyjmowania środków na poziomie międzynarodowym w tej dziedzinie wydaje się dyskusyjna, biorąc pod uwagę, że w obrębie państw członkowskich UE brak porozumienia co do ujednolicenia środków egzekwowania praw w środowisku cyfrowym i rodzajów sankcji karnych, jakie należy stosować ([39]).

67. W związku z powyższym wydaje się, że zasady konieczności i proporcjonalności przekazywania danych w ramach ACTA byłyby łatwiejsze do przestrzegania, gdyby umowa ograniczała się w sposób wyraźny do zwalczania jedynie najbardziej poważnych przestępstw naruszających prawa własności intelektualnej, zamiast zezwalać na masowe przekazywanie danych odnoszących się do każdego podejrzenia o naruszenie praw własności intelektualnej. Będzie to wymagać precyzyjnego zdefiniowana zakresu tego, co stanowi „najbardziej poważne przestępstwa naruszające prawa własności intelektualnej", przy których możliwe będzie przekazanie danych.

68. Ponadto wyjątkowo należy potraktować osoby uczestniczące w wymianie danych, a także szczególną uwagę zwrócić na to, czy dane będą wymieniane tylko pomiędzy organami publicznymi, czy też będę również wymieniane pomiędzy podmiotami prywatnymi a organami publicznymi. Jak podkreślono wcześniej w niniejszej opinii, zaangażowanie prywatnych podmiotów w dziedzinę, która zasadniczo podlega organom ścigania, budzi wiele wątpliwości ([40]). Warunki, na jakich podmioty prywatne będą zaangażowane w gromadzenie i wymianę z organami publicznymi danych osobowych odnoszących się do naruszeń praw własności intelektualnej, powinny być ściśle ograniczone do specyficznych okoliczności, wraz z odpowiednimi gwarancjami.

V.2. **Mające zastosowanie przepisy dotyczące ochrony danych, regulujące przekazywanie danych w kontekście ACTA**

Ogólny system przekazywania danych

69. Ogólne ramy ochrony danych mające zastosowanie w UE zostały określone w dyrektywie 95/46/WE. Artikuł 25 i 26 dyrektywy 95/46/WE definiuje system mający zastosowanie do przekazywania danych do państw trzecich. Art. 25 wymaga, by dane były przekazywane tylko do państw trzecich, które zapewnią odpowiedni stopień ochrony, w innych przypadkach takie przekazywanie jest zasadniczo zakazane.

70. Stopień odpowiedniej ochrony zapewniany przez państwa trzecie ocenia na zasadzie indywidualnego przypadku Komisja Europejska, która wydała szereg decyzji uznających wielu państwom odpowiedni charakter ochrony, w wyniku szczegółowej analizy przeprowadzonej przez grupę roboczą art. 29 ([41]).

71. EIOD podkreśla, że większość uczestników ACTA nie znajduje się na liście państw zapewniających odpowiednią ochronę danych, sporządzonej przez Komisję. Z wyjątkiem Szwajcarii i w szczególnych okolicznościach Kanady i USA, wszyscy pozostali uczestnicy ACTA nie zostali uznani za państwa zapewniające odpowiedni stopień ochrony. To oznacza, że aby dane zostały przekazane z UE do tych państw musi zostać spełniony jeden z warunków określonych w art. 26 ust. 1 dyrektywy 95/46/WE lub strony muszą wprowadzić odpowiednie środki zabezpieczające w stosunku do przekazywania danych, zgodnie z art. 26 ust. 2 dyrektywy.

Szczegółowy system przekazywania danych w dziedzinie egzekwowania prawa karnego

72. Podczas gdy dyrektywa 95/46/WE stanowi główny instrument ochrony danych w UE, jej zakres jest obecnie ograniczony, ponieważ w sposób wyraźny wyklucza ona, między innymi, działalność państwa w obszarach prawa karnego (art. 3). Wymiana danych dla celów egzekwowania prawa karnego nie będzie się więc mieściła w zakresie dyrektywy 95/46/WE i będzie podlegać ogólnym zasadom ochrony

([39]) Wniosek w sprawie sankcji karnych jest obecnie omawiany w Radzie, COM(2006) 168 z dnia 26 kwietnia 2006 r.

([40]) Zob. pkt 32 i 52 niniejszej opinii. Zob. również Opinia Europejskiego Inspektora Ochrony Danych w sprawie sprawozdania końcowego grupy kontaktowej wysokiego szczebla UE–USA ds. wymiany informacji oraz ochrony prywatności i danych osobowych, Dz.U. C 128 z 6.6.2009, s. 1.

([41]) Zob. decyzje o odpowiednim stopniu ochrony wydane przez Komisję Europejską dla Argentyny, Kanady, Szwajcarii, USA – bezpieczny transfer danych osobowych i PNR – Guernsey, wyspy Man i Jersey, dostępne pod adresem http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

danych określonym w Konwencji Rady Europy nr 108 i jej Protokole dodatkowym, których stroną są wszystkie państwa członkowskie UE ([42]). Ponadto zastosowanie znajdą zasady przyjęte przez UE w odniesieniu do współpracy policji i sądów w sprawach karnych, które określono w decyzji ramowej Rady 2008/877/JHA ([43]).

73. Instrumenty te również zawierają zasadę, zgodnie z którą w państwach trzecich, do których przekazywane są dane, musi istnieć odpowiedni stopień ochrony danych Wprowadzono kilka odstępstw, w szczególności gdy państwo trzecie zapewnia odpowiednie środki zabezpieczające. Podobnie jak w wymianie danych w ramach dyrektywy 95/46/WE, wymiana danych w dziedzinie egzekwowania prawa karnego będzie tym samym wymagała wprowadzenia odpowiednich środków zabezpieczających pomiędzy stronami, między którymi przekazywane są dane, by takie przekazanie miało miejsce.

W kierunku nowego systemu przekazywania danych

74. W najbliższej przyszłości można spodziewać się przyjęcia przez UE, w oparciu o art. 16 TFUE, nowych wspólnych zasad ochrony danych mających zastosowanie do wszystkich dziedzin działalności UE. To oznacza, że za kilka lat mogą powstać globalne ramy ochrony danych UE, które określą spójne zasady ochrony danych we wszystkich dziedzinach działalności UE, wymagające tego samego stopnia środków zabezpieczających i gwarancji dla wszystkich działań z zakresu przetwarzania danych. Jak stwierdziła Viviane Reding ([44]), komisarz ds. sprawiedliwości, praw podstawowych i obywatelstwa, te nowe ramy powinny funkcjonować jako „nowoczesny i kompleksowy instrument prawny" ochrony danych w UE. Takie ramy są tym bardziej pożądane, że wprowadziłyby więcej porządku i spójności do mających zastosowanie w UE zasad w zakresie ochrony danych.

75. W kontekście międzynarodowym EIOD wskazuje na Rezolucję w sprawie międzynarodowych norm ochrony danych osobowych i prywatności przyjętą niedawno przez organy ochrony danych, która jest pierwszym krokiem w kierunku ustanowienia ogólnoświatowych norm ochrony danych ([45]). Międzynarodowe normy obejmują kilka środków zabezpieczających ochronę danych. podobnych do tych, o których mowa w dyrektywie 95/46/WE i Konwencji nr 108. Choć międzynarodowe normy nie mają jeszcze mocy wiążącej, są użytecznymi wytycznymi w zakresie zasad ochrony danych, które mogą być dobrowolnie stosowane przez państwa trzecie, dzięki czemu ich ramy prawne stają się zgodne z normami europejskimi. EIOD uważa, że sygnatariusze ACTA powinni również wziąć pod uwagę zasady określone w międzynarodowych normach przy przetwarzaniu danych osobowych z UE.

V.3. **Konieczność wdrożenia odpowiednich środków zabezpieczających w celu ochrony przekazywanych danych z UE do państw trzecich**

Jaką formę powinny przyjąć środki zabezpieczające w celu skutecznej ochrony danych przekazywanych do państw trzecich?

76. EIOD podkreśla, że jeśli wykazano konieczność przekazania danych osobowych do państw trzecich, Unia Europejska powinna negocjować z państwami trzecimi będącymi odbiorcą – obok samej umowy ACTA – szczegółowe instrumenty zawierające odpowiednie gwarancje ochrony danych w celu uregulowania ochrony danych.

77. Odpowiednie środki zabezpieczające ochronę danych powinny zazwyczaj zostać wprowadzone do wiążącej umowy pomiędzy UE a państwem trzecim będącym odbiorcą, za pośrednictwem której strona odbierająca dane zobowiązuje się do przestrzegania europejskich przepisów dotyczących ochrony danych i zapewnienia osobom fizycznym takich samych praw i możliwości ich dochodzenia, jakie gwarantuje prawo europejskie. Konieczność wiążącej umowy wynika z art. 26 ust. 2 dyrektywy 95/46/WE i art. 13 ust. 3 lit. b) decyzji ramowej i jest ponadto uzasadniona bieżącą praktyką UE zawierania szczegółowych umów w celu umożliwienia konkretnego przesyłania danych do państw trzecich ([46]).

78. Podobnie, w ramach międzynarodowych norm, odbiorca może zostać poproszony o zagwarantowanie, że zapewni wymagany stopień ochrony, w celu przesłania danych. Gwarancje te mogłyby również przyjąć formę zobowiązania umownego.

Treść środków zabezpieczających, jakie sygnatariusze ACTA powinni wprowadzić w odniesieniu do przekazywania danych osobowych

79. EIOD szczególnie podkreśla, że międzynarodowa wymiana informacji w celu egzekwowania prawa jest szczególnie chroniona w ramach ochrony danych, w związku z tym ramy mogłyby zalegalizować masowe przekazywanie

([42]) Konwencja o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, przyjęta w Strasburgu dnia 28 stycznia 1981 r. oraz Protokół dodatkowych Rady Europy do Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych dotyczący organów nadzoru i transgranicznych przepływów danych, Strasburg, dnia 8 listopada 2001 r.

([43]) Decyzja ramowa Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych, Dz.U. L 350 z 30.12.2008, s. 60.

([44]) Zob. odpowiedzi na kwestionariusz Parlamentu Europejskiego dla kandydatki na komisarza Viviane Reding, s. 5, http://www.europarl.europa.eu/hearings/static/commissioners/answers/reding_replies_en.pdf

([45]) Rezolucję przyjęto w Madrycie w listopadzie 2009 r.

([46]) Dla przykładu umowy Europol i Eurojust z USA, umowa o PNR, umowa SWIFT, umowa pomiędzy UE a Australią w sprawie przetwarzania danych dotyczących przelotu pasażera (PNR) pochodzących z Unii Europejskiej i przekazywania tych danych przez przewoźników lotniczych australijskim organom celnym.

danych w dziedzinie, w której wpływ na osoby fizyczne jest szczególnie duży oraz w której zasadnicze i niezawodne środki zabezpieczające są tym bardziej niezbędne.

80. EIOD podkreśla, że szczegółowe warunki i środki zabezpieczające można zdefiniować wyłącznie indywidualnie, po uwzględnieniu wszystkich wskaźników wymiany danych. Jako wskazówki EIOD wyszczególnia poniżej niektóre z zasad i środków zabezpieczających, które osoby trzecie będące odbiorcami danych muszą wprowadzić w celu umożliwienia przekazania danych:

— należy sprawdzić, jakie jest prawne uzasadnienie, w ramach którego mają miejsce działania z zakresu przetwarzania danych (tj. czy operacje przetwarzania są oparte na wymogu prawnym, na zgodzie osób, których dane dotyczą, czy innym ważnym uzasadnieniu?) oraz czy przekazywanie danych jest zgodne z pierwotnym celem gromadzenia danych. Przekazywanie danych nie powinno wychodzić poza zakres określonego celu,

— ilość i rodzaje danych osobowych, które mają podlegać wymianie, powinny zostać jasno określone i zminimalizowane do tego, co niezbędne w celu osiągnięcia celu przekazania danych. Dane osobowe zgromadzone i przekazane mogą w szczególności zawierać adresy IP użytkowników Internetu, datę i czas domniemanego przestępstwa i rodzaj przestępstwa. EIOD zaleca, by dane nie były wiązane z konkretną osobą fizyczną na etapie ścigania i przypomina, że identyfikacja podejrzanej osoby musi nastąpić zgodnie z prawem i pod nadzorem sądu. W tym względzie EIOD podkreśla, że dane odnoszące się do naruszeń praw własności intelektualnej i podejrzeń o naruszenia są specjalną kategorią danych, których przetwarzanie jest zazwyczaj zarezerwowane dla organów ścigania i wymaga zastosowania dodatkowych środków zabezpieczających. Osoby upoważnione do przetwarzania danych odnoszących się do naruszeń praw własności intelektualnej i podejrzeń o naruszenia oraz warunki przetwarzania tych danych muszą zatem zostać szczegółowo określone zgodnie z istniejącymi przepisami w zakresie ochrony danych,

— osoby, wśród których dane mogą być wymieniane, muszą zostać wyraźnie wskazane i następnie przekazywanie danych innym odbiorcom powinno być zasadniczo zakazane, chyba że takie przekazywanie jest niezbędne dla konkretnego przypadku ścigania. Ograniczenie to ma szczególne znaczenie, ponieważ wyznaczeni odbiory nie powinni bezpodstawnie dzielić się informacjami z nieupoważnionymi odbiorcami,

— EIOD spodziewa się, że ACTA nie tylko określi współpracę pomiędzy organami publicznymi, ale również powierzy zadania z zakresu egzekwowania prawa prywatnym organizacjom (takim jak dostawcy usług internetowych, organizacje właścicieli praw autorskich itp.). W tym ostatnim przypadku warunki i stopień zaangażowania prywatnych organizacji w egzekwowanie praw własności intelektualnej muszą zostać ostrożnie ocenione, w tym sensie, że postanowienia ACTA nie powinny de facto nadawać dostawcom usług internetowych i organizacjom właścicieli praw własności intelektualnej prawa do monitorowania działań użytkowników on-line. Ponadto przetwarzanie danych osobowych przez prywatne organizacje w kontekście egzekwowania prawa powinno mieć miejsce wyłącznie w oparciu o właściwą podstawę prawną. Ważne również, by wyraźnie określić, czy prywatne organizacje będą zobowiązane do współpracy z policją oraz zdefiniować zakres takiej współpracy. We wszystkich przypadkach powinno się to ograniczać do „poważnych przestępstw", których precyzyjna definicja również będzie niezbędna, ponieważ nie wszystkie naruszenia praw własności intelektualnej uznaje się za poważne przestępstwa,

— metoda wykorzystywana do wymiany danych osobowych musi zostać doprecyzowana, w szczególności należy określić, czy wymiana będzie przebiegać w ramach systemu pchającego – np. dostawcy usług internetowych i organizacje właścicieli praw intelektualnych przekazywaliby w ramach pełnionej kontroli dane osobom trzecim, takim jak policja i organy ścigania, znajdującym się za granicą – lub system ssący – np. policja i organy ścigania miałyby bezpośredni dostęp do baz danych prywatnych podmiotów lub baz danych, w których informacje byłyby scentralizowane. Jak już przedstawiono w kontekście danych PNR, system pchający jest jedyną opcją zgodną z zasadami ochrony danych z punktu widzenia ochrony danych w UE, ponieważ upoważnia nadawcę z UE, którym najczęściej jest administrator danych, do pełnienia kontroli nad przesyłaniem danych ([47]).

— należy określić czas, na jaki dane osobowe będą zatrzymywane oraz cel, dla którego takie zatrzymywanie jest konieczne. Ten okres zatrzymywania danych powinien być proporcjonalny do obranego celu, co oznacza, że dane powinny zostać usunięte/skasowane, gdy nie są już potrzebne do osiągnięcia tego celu,

— należy wyraźnie określić obowiązki spoczywające na administratorach danych w państwach trzecich. Należy zagwarantować mechanizmy nadzoru lub mechanizmy pociągania do odpowiedzialności tak, by istniały skuteczne środki zaradcze i sankcje wobec administratorów danych w przypadku bezpodstawnego przetwarzania danych lub innych tego rodzaju zdarzeń.

([47]) Zob. Artykuł 29 opinii grupy roboczej 4/2003 w sprawie poziomu ochrony zapewnianej przez Stany Zjednoczone przekazywaniu danych pasażerów, WP 78, 13.6.2003 r.

Ponadto należy prowadzić mechanizmy odwoławcze, by osoby fizyczne mogły złożyć skargę do niezależnego organu ochrony danych i by mogły domagać się swoich praw przed niezawisłym i bezstronnym sądem ([48]),

— instrument wprowadzony pomiędzy stronami powinien jasno określać prawa osób, których dane dotyczą, w odniesieniu do ich danych osobowych, jeśli dane takie są przetwarzane przez osobę trzecią będącą odbiorcą, by zagwarantować im skuteczne środki egzekwowania swoich praw w odniesieniu do przetwarzania odbywającego się za granicą,

— ponadto przejrzystość ma zasadnicze znaczenie i strony instrumentu ochrony danych muszą uzgodnić, w jaki sposób będą informować osoby, których dane dotyczą, o mającym miejsce przetwarzaniu danych oraz o ich prawach i sposobach ich wykonywania.

VI. **WNIOSKI**

81. EIOD usilnie zachęca Komisję Europejską do przeprowadzenia publicznego i przejrzystego dialogu na temat ACTA, jeśli to możliwe – w ramach konsultacji społecznej, co pozwoliłoby również zapewnić zgodność środków, które mają zostać przyjęte, z wymogami europejskich przepisów odnoszących się do prywatności i ochrony danych.

82. W trakcie toczących się negocjacji w sprawie ACTA EIOD wzywa Komisję Europejską do odnalezienia złotego środka pomiędzy zapotrzebowaniem na ochronę praw własności intelektualnej a prawem do prywatności i ochrony danych osób fizycznych. EIOD podkreśla, że podstawowe znaczenie ma uwzględnienie prywatności i ochrony danych od samego początku negocjacji, przed uzgodnieniem jakichkolwiek postanowień, gdy jest jeszcze czas na znalezienie alternatywnych rozwiązań z poszanowaniem prywatności.

83. Własność intelektualna jest ważna dla społeczeństwa i należy ją chronić, nie należy jej jednak stawiać wyżej niż prawa podstawowe osób fizycznych do prywatności, ochrony danych i inne prawa, takie jak domniemanie niewinności, skuteczna ochrona sądowa i wolność wyrażania opinii.

84. Ponieważ obecny projekt ACTA popiera politykę odłączania Internetu po trzech ostrzeżeniach lub przynajmniej pośrednio do niej nawołuje, ACTA w ogromnej mierze może ograniczać prawa podstawowe i wolności europejskich obywateli, w szczególności ochronę danych osobowych i prywatność.

85. EIOD jest zadania, że polityka odłączania Internetu po trzech ostrzeżeniach nie jest konieczna do osiągnięcia celu, jakim jest egzekwowanie praw własności intelektualnej. EIOD jest przekonany, że istnieją alternatywne, mniej inwazyjne rozwiązania albo przynajmniej planowana polityka może być realizowana w mniej inwazyjny sposób lub w bardziej ograniczonym zakresie, w szczególności poprzez formy ukierunkowanego doraźnego monitorowania.

86. Polityka odłączania Internetu po trzech ostrzeżeniach jest również problematyczna na bardziej szczegółowym poziomie prawa, w szczególności dlatego że przetwarzanie danych sądowych, w szczególności przez organizacje prawne, musi mieć właściwą podstawę prawną. Operacje systemów trzech ostrzeżeń mogą wiązać się ponadto z przechowywaniem plików dziennika systemowego w długim okresie, co byłoby sprzeczne z istniejącymi przepisami.

87. Ponadto, ponieważ ACTA wiąże się z wymianą danych osobowych pomiędzy organami lub prywatnymi organizacjami znajdującymi się u sygnatariuszy, EIOD wzywa Unię Europejską do wdrożenia odpowiednich środków zabezpieczających. Te środki zabezpieczające powinny mieć zastosowanie do wszystkich przypadków przekazywania danych w kontekście ACTA – czy to w ramach egzekwowania prawa cywilnego, karnego lub przepisów dotyczących środowiska cyfrowego – i powinny być zgodne z zasadami ochrony danych określonymi w Konwencji nr 108 i dyrektywie 95/46/WE. EIOD zaleca, by takie środki zabezpieczające przybrały formę wiążących umów między nadawcami z UE a państwami trzecimi będącymi odbiorcami.

88. EIOD chciałby, aby skonsultowano się z nim w sprawie środków wdrażanych w odniesieniu do przekazywania danych, wprowadzanych w ramach ACTA, w celu umożliwienia analizy ich proporcjonalności i sprawdzenia, czy gwarantują one odpowiedni stopień ochrony danych.

Sporządzono w Brukseli dnia 22 lutego 2010 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych

([48]) Opinia Europejskiego Inspektora Ochrony Danych w sprawie sprawozdania końcowego grupy kontaktowej wysokiego szczebla UE–USA ds. wymiany informacji oraz ochrony prywatności i danych osobowych, 11.11.2008 r.