I

(Rezolucje, zalecenia i opinie)

OPINIE

EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Opinia Europejskiego Inspektora Ochrony Danych w sprawie komunikatu Komisji dla Parlamentu Europejskiego i Rady w sprawie kontynuacji programu prac na rzecz skuteczniejszego wdrażania dyrektywy o ochronie danych

(2007/C 255/01)

EUROPEJSKI INSPEKTOR OCHRONY DANYCH,

uwzględniając Traktat ustanawiający Wspólnotę Europejską, w szczególności jego art. 286,

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 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 ([2]), w szczególności jego art. 41,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

I. WPROWADZENIE

1. W dniu 7 marca 2007 r. Komisja przesłała EIOD komunikat dla Parlamentu Europejskiego i Rady w sprawie kontynuacji programu prac na rzecz skuteczniejszego wdrażania dyrektywy o ochronie danych ([3]). Zgodnie z art. 41 rozporządzenia (WE) nr 45/2001 EIOD przedstawia niniejszą opinię.

2. Komunikat potwierdza znaczenie dyrektywy 95/46/WE ([4]) jako kamienia milowego w dziedzinie ochrony danych osobowych i omawia dyrektywę oraz jej stosowanie w trzech rozdziałach poświęconych przeszłości, sytuacji obecnej i przyszłości. Głównym przesłaniem komunikatu jest to, że dyrektywy nie należy zmieniać. Należy dalej usprawniać jej wdrażanie za pomocą innych narzędzi politycznych, w większości o charakterze niewiążącym prawnie.

3. Struktura niniejszej opinii EIOD jest analogiczna do struktury komunikatu. Co ważniejsze, EIOD podziela główny wniosek Komisji, że dyrektywy nie należy zmieniać.

4. EIOD przyjął takie stanowisko jednak również z przyczyn pragmatycznych, wychodząc od następujących przesłanek:

— w perspektywie krótkoterminowej najlepiej nakierować działania na skuteczniejsze wdrażanie dyrektywy. Jak wykazuje komunikat, ciągle jest możliwe znaczne usprawnienie wdrażania;

— w dalszej perspektywie zmiany w dyrektywie — z zachowaniem jej podstawowych zasad — wydają się nieuchronne;

— należy już teraz określić konkretny termin przeglądu, by przygotować wnioski dotyczące zmian. Taki termin byłby wyraźnym bodźcem do niezwłocznego rozpoczęcia refleksji nad przyszłymi zmianami.

([1]) Dz.U. L 281 z 23.11.1995, str. 31.
([2]) Dz.U. L 8 z 12.1.2001, str. 1.
([3]) Zwany dalej „komunikatem”.
([4]) Zwana dalej „dyrektywą”.

5. Te przesłanki mają fundamentalne znaczenie, gdyż należy pamiętać, że dyrektywa działa w zmieniającym się kontekście. Po pierwsze, zmienia się Unia Europejska: wzrosło znaczenie swobodnego przepływu informacji między państwami członkowskimi — oraz między państwami członkowskimi a państwami trzecimi — i będzie ono nadal wzrastać. Po drugie, zmienia się społeczeństwo. Społeczeństwo informacyjne ewoluuje i przyjmuje coraz więcej cech społeczeństwa kontrolowanego ([5]). Implikuje to rosnącą potrzebę skutecznej ochrony danych osobowych, by w sposób w pełni zadowalający stawiać czoła nowej rzeczywistości.

II. PUNKTY WIDZENIA PRZEDSTAWIONE W NINIEJSZEJ OPINII

6. W swej ocenie komunikatu EIOD zajmie się w szczególności następującymi zagadnieniami, które są istotne w odniesieniu do wspomnianych wcześniej zmian:

— skuteczniejsze wdrażanie samej dyrektywy: w jaki sposób uczynić ochronę danych skuteczniejszą? Do usprawnienia wdrażania konieczny jest zestaw narzędzi politycznych, poczynając od lepszej komunikacji ze społeczeństwem, a kończąc na ściślejszym przestrzeganiu praw związanych z ochroną danych;

— interakcje z technologią: nowe osiągnięcia techniki, takie jak rozwój wspólnego dostępu do danych, systemy RFID, biometria i systemy zarządzania tożsamością mają wyraźny wpływ na wymagania dotyczące skutecznych ram prawnych ochrony danych. Ponadto potrzeba skutecznej ochrony danych osobowych poszczególnych osób może nałożyć ograniczenia na wykorzystywanie tych nowych technologii. Interakcja jest więc obustronna: technologia wpływa na prawodawstwo, a prawodawstwo wpływa na technologię;

— globalne zagadnienia dotyczące prywatności i jurysdykcji, mające związek z granicami zewnętrznymi Unii Europejskiej. Podczas gdy jurysdykcja prawodawcy wspólnotowego jest ograniczona do terytorium Unii Europejskiej, granice zewnętrzne tracą na znaczeniu dla przepływu danych. Gospodarka jest coraz bardziej uzależniona od sieci globalnych. Przedsiębiorstwa mające siedzibę w Unii Europejskiej coraz częściej podzlecają różne zadania, w tym przetwarzanie danych osobowych, państwom trzecim. Ponadto niedawne sprawy dotyczące SWIFT i PNR potwierdzają, że inne jurysdykcje są zainteresowane „danymi pochodzącymi z UE". Ogólnie rzecz biorąc, faktyczne miejsce przetwarzania danych jest mniej istotne;

— ochrona danych i egzekwowanie prawa: ostatnie zagrożenia społeczne, związane z terroryzmem lub nie, doprowadziły do (wymagają) stworzenia organom ścigania większych możliwości gromadzenia, przechowywania i wymiany danych osobowych. W niektórych przypadkach — jak niedawno zaobserwowano — aktywnie angażują się strony prywatne. Linia oddzielająca trzeci filar Traktatu o UE (w obrębie którego dyrektywa nie ma zastosowania) z jednej strony zyskuje na znaczeniu, a z drugiej staje się coraz płynniejsza. Istnieje nawet ryzyko, że w niektórych przypadkach dane osobowe nie będą chronione ani przez instrumenty należące do pierwszego, ani do trzeciego filaru (luka prawna).

— Takie są konsekwencje — przynajmniej w tym, co się tyczy ochrony danych i egzekwowania prawa — wejścia w życie traktatu reformującego, które jest obecnie przewidziane na rok 2009.

III. PRZESZŁOŚĆ I STAN OBECNY

7. Pierwsze sprawozdanie z wdrażania dyrektywy o ochronie danych z dnia 15 maja 2003 r. zawierało program prac na rzecz skuteczniejszego wdrażania dyrektywy o ochronie danych wraz z wykazem 10 inicjatyw, które miały zostać przeprowadzone w latach 2003-2004. Komunikat opisuje sposób przeprowadzenia każdego z tych działań.

8. Komunikat zawiera pozytywną ocenę osiągnięć we wdrażaniu dyrektywy sporządzoną na podstawie analizy działań przeprowadzonych w ramach wspomnianego programu prac. W przeprowadzonej przez Komisję ocenie, streszczonej w podtytułach rozdziału II („dzień dzisiejszy") komunikatu, zasadniczo stwierdzono, że: skuteczność wdrażania dyrektywy wzrosła, jednak niektóre państwa pozostają w tyle; nadal pojawiają się pewne rozbieżności, które jednak leżą głównie w obrębie marginesu swobody przewidzianego w dyrektywie, a ponadto nie stanowią zagrożenia dla rynku wewnętrznego. Rozwiązania prawne określone w dyrektywie okazały się w zasadzie właściwe, by zagwarantować fundamentalne prawo do ochrony danych, radząc sobie również z postępem technicznym i wymaganiami nakładanymi ze względu na interes publiczny.

9. EIOD podziela główne punkty tej pozytywnej opinii. Uznaje zwłaszcza znaczne wysiłki dokonane w dziedzinie transgranicznych przepływów danych: ustalenia dotyczące właściwej ochrony danych w odniesieniu do państw trzecich, nowe standardowe klauzule umowne, przyjęcie wiążących zasad dla przedsiębiorstw, refleksje nad bardziej jednolitą wykładnią przepisów art. 26 ust. 1 dyrektywy oraz usprawnienie powiadamiania na mocy art. 26 ust. 2 mają na celu ułatwienie międzynarodowego transferu danych osobowych. Orzecznictwo Trybunału Sprawiedliwości ([6]) pokazało jednak, że w tej zasadniczej dziedzinie pozostały jeszcze do wykonania prace mające na celu dostosowanie do postępu technicznego oraz postępu w zakresie egzekwowania prawa.

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

([6]) Zwłaszcza orzeczenia Trybunału w sprawie „Lindqvist" (zob. przypis 15) i „PNR" (zob. przypis 17).

10. Komunikat pokazuje również, że egzekwowanie i podnoszenie świadomości stanowią kwestie kluczowe dla promowania lepszego wdrażania i że należy nadal kłaść na nie nacisk. Ponadto wymiana wzorców postępowania i harmonizacja przepisów dotyczących powiadamiania i informowania stanowią ważne precedensy dla zmniejszenia biurokracji i redukcji kosztów ponoszonych przez przedsiębiorstwa.

11. Należy dodać, że analiza sytuacji w przeszłości potwierdza, iż nie da się osiągnąć postępów bez zaangażowania wielu różnych stron. Komisja, organy ochrony danych i państwa członkowskie są głównymi motorami większości prowadzonych działań. Rola stron prywatnych jednak znacznie wzrasta, szczególnie w zakresie propagowania samoregulacji i europejskich kodeksów postępowania lub postępów w dziedzinie technologii ochrony prywatności.

IV. **PRZYSZŁOŚĆ**

A. **Wniosek: rezygnacja ze zmiany dyrektywy na obecnym etapie.**

12. Jest kilka powodów dla poparcia wniosku Komisji głoszącego, że w obecnej sytuacji i w perspektywie krótkoterminowej nie należy przewidywać żadnej propozycji zmian w dyrektywie.

13. Komisja w zasadzie popiera swój wniosek dwoma argumentami. Po pierwsze, dotąd nie wykorzystano w pełni potencjału dyrektywy. Ciągle jest możliwe znaczne usprawnienie wdrażania dyrektywy w obrębie jurysdykcji poszczególnych państw członkowskich. Po drugie, Komisja stwierdza, że choć dyrektywa pozostawia państwom członkowskim margines swobody, nie ma dowodów na to, by mieszczące się w tym marginesie rozbieżności stanowiły zagrożenie dla rynku wewnętrznego.

14. Na podstawie tych dwóch argumentów Komisja sformułowała swój wniosek w następujący sposób. Wyjaśnia ona, czego powinna dokonać dyrektywa, z naciskiem na zapewnienie zaufania, po czym stwierdza, że stanowi ona punkt odniesienia, jest neutralna z technicznego punktu widzenia i nadal pozostaje źródłem trwałych i stosownych rozwiązań ([7]).

15. EIOD z zadowoleniem przyjmuje sposób sformułowania tego wniosku, jest jednak zdania, że powinien on zostać poparty dwoma dodatkowymi argumentami:

— po pierwsze, charakterem samej dyrektywy;

— po drugie, polityką prawodawczą Unii.

Charakter dyrektywy

16. Podstawowe prawo osób fizycznych do ochrony swoich danych osobowych zostało uznane w art. 8 Karty praw podstawowych Unii oraz, między innymi, objęte konwencją 108 Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych. Zasadniczo dyrektywa stanowi ramy obejmujące główne elementy ochrony tego podstawowego prawa poprzez nadanie mu treści oraz powiększanie praw i swobód wyrażonych w konwencji ([8]).

17. Prawa podstawowe mają na celu ochronę obywateli demokratycznego społeczeństwa we wszystkich sytuacjach. Zasadnicze elementy takiego prawa podstawowego nie powinny łatwo ulegać zmianom ze względu na rozwój społeczeństwa lub preferencje polityczne kolejnych rządów. Przykładowo, zagrożenie społeczeństwa przez organizacje terrorystyczne może prowadzić w konkretnych przypadkach do różnych rezultatów, gdyż mogą być konieczne istotniejsze ingerencje w prawa podstawowe osób, ale ingerencje te mogą w ogóle nie wpływać na zasadnicze elementy samego prawa ani nie uniemożliwiać osobie prywatnej korzystania z tego prawa lub niewłaściwie ograniczać takie korzystanie.

18. Drugą cechą charakterystyczną dyrektywy jest to, że przewiduje ona propagowanie swobodnego przepływu informacji w obrębie rynku wewnętrznego. Również ten drugi cel może być uznany za podstawowy w coraz bardziej rozwijającym się rynku wewnętrznym pozbawionym wewnętrznych granic. Harmonizacja najważniejszych przepisów prawa krajowego jest jednym z głównych narzędzi mających na celu ustanowienie i funkcjonowanie tego rynku wewnętrznego. Stanowi ona realizację wzajemnego zaufania państw członkowskich do swoich krajowych systemów prawnych. Również dlatego należy właściwie rozważyć wszelkie zmiany. Zmiany mogą wpływać na wzajemne zaufanie.

19. Trzecią cechą charakterystyczną dyrektywy jest to, że musi być postrzegana jako ogólne ramy, na których budowane są szczegółowe instrumenty prawne. Te szczegółowe instrumenty obejmują środki wykonawcze do ogólnych ram oraz szczegółowe ramy dla poszczególnych sektorów. Dyrektywa o prywatności i łączności elektronicznej, 2002/58/WE ([9]), stanowi takie właśnie szczegółowe ramy. W miarę możliwości zmiany zachodzące w społeczeństwie powinny prowadzić do zmian środków wykonawczych lub szczegółowych ram prawnych, nie zaś do zmian ram ogólnych, na których się one zasadzają.

Polityka prawodawcza Unii

20. W opinii EIOD wniosek, by obecnie nie zmieniać dyrektywy, jest również logiczną konsekwencją ogólnych zasad dobrej administracji i polityki prawodawczej. Wnioski prawodawcze — niezależnie od tego, czy oznaczają nowe obszary działania Wspólnoty lub też zmieniają istniejące normy prawodawcze — należy składać wyłącznie, jeżeli dostatecznie dowiedziono konieczności i proporcjonalności nowego uregulowania. Nie należy składać wniosku prawodawczego, jeżeli ten sam wynik mógłby zostać osiągnięty z użyciem innych, nie sięgających tak daleko narzędzi.

([7]) Str. 9, pierwszy pełny akapit komunikatu.

([8]) Motyw 11 dyrektywy.

([9]) 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 o prywatności i łączności elektronicznej) (Dz.U. L 201 z 31.7.2002, str. 37).

21. W obecnych warunkach konieczności i proporcjonalności zmiany dyrektywy nie dowiedziono. EIOD przypomina, że dyrektywa stwarza ogólne ramy ochrony danych na mocy prawa wspólnotowego. Musi ona zapewnić — z jednej strony — ochronę praw i swobód poszczególnych osób, zwłaszcza prawa do prywatności, w odniesieniu do przetwarzania danych osobowych, a z drugiej strony swobodny przepływ tych danych w obrębie rynku wewnętrznego.

22. Takie ogólne ramy nie powinny być zmieniane, póki nie zostaną w pełni wdrożone w państwach członkowskich, chyba że są jasne wskazania, iż cele dyrektywy przy obecnych ramach nie mogą być spełnione. Zdaniem EIOD Komisja w obecnej sytuacji właściwie oceniła, że potencjał dyrektywy nie został jeszcze w pełni wykorzystany (zob. rozdział III niniejszej opinii). Nie ma także dowodów na to, że w obecnych ramach niemożliwe jest osiągnięcie wyznaczonych celów.

B. **W dalszej perspektywie zmiany w dyrektywie wydają się nieuchronne**

23. Również w przyszłości należy zapewnić osobom fizycznym skuteczną ochronę dzięki zasadom ochrony danych, uwzględniając zmieniający się kontekst, w jakim działa dyrektywa (zob. pkt 5 niniejszej opinii) oraz perspektywy przedstawione w pkt 6 niniejszej opinii: usprawnienie wdrażania dyrektywy, interakcje z technologią, globalne zagadnienia dotyczące prywatności i jurysdykcji, ochronę danych i egzekwowanie prawa oraz traktat reformujący. Ta potrzeba pełnego zastosowania zasad ochrony danych ustanawia normy przyszłych zmian w dyrektywie. EIOD po raz kolejny przypomina, że w dalszej perspektywie zmiany w dyrektywie wydają się nieuchronne.

24. Co się tyczy treści wszelkich przyszłych środków, EIOD już na obecnym etapie jest w stanie podać pewne elementy, które uważa za zasadnicze w jakimkolwiek przyszłym systemie ochrony danych w Unii Europejskiej. Oto one:

— nie ma konieczności ustalania nowych zasad, ale istnieje oczywista potrzeba wprowadzenia innych rozwiązań administracyjnych, z jednej strony skutecznych i właściwych dla społeczeństwa operującego w sieci, a z drugiej strony minimalizujących koszty administracyjne;

— szeroki zakres praw o ochronie danych nie powinien ulec zmianie. Powinien mieć zastosowanie do wszystkich sposobów wykorzystania danych osobowych i nie powinien być limitowany do danych wrażliwych lub w inny sposób ograniczony do szczególnych interesów lub zagrożeń. Innymi słowy, EIOD odrzuca podejście *„de minimis”* w odniesieniu do zakresu zastosowania ochrony danych. Zapewni to osobom, których dotyczą dane, możliwość korzystania ze swoich praw we wszystkich sytuacjach;

— prawo o ochronie danych powinno nadal obejmować szeroki wachlarz sytuacji, pozwalając zarazem w konkretnych przypadkach na wyważone podejście, z uwzględnieniem innych uzasadnionych interesów (publicznych lub prywatnych) oraz potrzeby zminimalizowania konsekwencji biurokratycznych. Ten system powinien również umożliwić organom ochrony danych określanie priorytetów i skupienie się na obszarach lub zagadnieniach szczególnej wagi lub związanych ze szczególnymi zagrożeniami;

— system powinien mieć w pełni zastosowanie do wykorzystywania danych osobowych do celów egzekwowania prawa, choć mogą być konieczne odpowiednie środki dodatkowe, by rozwiązać szczególne problemy w tej dziedzinie;

— należy dokonać stosownych ustaleń dotyczących przepływu danych z państwami trzecimi, w miarę wykonalności opartych na światowych standardach ochrony danych.

25. W komunikacie wspomina się — w związku z wyzwaniami stawianymi przez nowe technologie — o toczącym się przeglądzie dyrektywy 2002/58/WE oraz ewentualnej potrzebie wprowadzenia specyficznych zasad w celu rozwiązania problemów wynikających z wykorzystania technologii takich jak Internet i RFID ([10]). EIOD z zadowoleniem przyjmuje ten przegląd i dalsze działania, choć jego zdaniem powinny one nie tylko być związane z postępem technicznym, lecz także uwzględniać zmieniający się kontekst w sposób całościowy, a w dalszej perspektywie objąć również dyrektywę 95/46/WE. Ponadto w tym kontekście konieczne jest większe skupienie. Niestety komunikat pozostawia pewne otwarte kwestie:

— brak harmonogramu realizacji różnych działań wspomnianych w rozdziale 3 komunikatu;

— brak terminu przedstawienia kolejnego sprawozdania z wdrażania dyrektywy. Artykuł 33 dyrektywy wymaga „regularnego” składania przez Komisję sprawozdań, lecz nie określa ich częstotliwości;

— brak zakresu zadań: komunikat nie pozwala na ocenę realizacji przewidzianych działań. Po prostu odnosi się do programu prac przedstawionego w roku 2003.

— nie ma wskazówek co do sposobu postępowania w dalszej perspektywie.

EIOD sugeruje, by Komisja szczegółowo opracowała te elementy.

([10]) Str. 11 komunikatu.

V. **PERSPEKTYWY PRZYSZŁYCH ZMIAN**

A. **Pełne wdrożenie**

26. Jakiekolwiek przyszłe zmiany muszą być poprzedzone pełnym wdrożeniem obecnych przepisów dyrektywy. Pełne wdrożenie rozpoczyna się od zgodności z wymogami prawnymi określonymi w dyrektywie. W komunikacie wspomniano ([11]), że niektóre państwa członkowskie nie dokonały transpozycji wielu istotnych przepisów dyrektywy i wskazano w związku z tym w szczególności przepisy dotyczące niezależności organów nadzoru. Zadaniem Komisji jest nadzorowanie zgodności oraz, gdy uzna to za stosowne, wykorzystanie uprawnień nadanych jej na mocy art. 226 TWE.

27. Komunikat przewiduje wydanie komunikatu wyjaśniającego dotyczącego niektórych przepisów, zwłaszcza tych, które mogą prowadzić do formalnych postępowań o naruszenie przepisów zgodnie z art. 226 TWE.

28. Ponadto dyrektywa wprowadza inne mechanizmy usprawniające jej wdrażanie. W szczególności mając to na względzie, określono w art. 30 dyrektywy zadania grupy roboczej art. 29. Zadania te mają stymulować wdrażanie w państwach członkowskich wysokiego i zharmonizowanego poziomu ochrony danych, wykraczając poza to, co ściśle niezbędne do wypełnienia obowiązków nałożonych dyrektywą. Realizując swoje zadania, wspomniane grupa robocza przez lata sporządziła znaczną liczbę opinii i innych dokumentów.

29. W opinii EIOD pełne wdrożenie dyrektywy obejmuje następujące dwa elementy:

— należy zapewnić całkowite wypełnianie przez państwa członkowskie swoich obowiązków wynikających z prawa europejskiego. Oznacza to, że przepisy dyrektywy powinny zostać przetransponowane do prawa krajowego, a w praktyce należy osiągnąć rezultaty przewidziane w dyrektywie;

— należy w pełni wykorzystywać inne, niewiążące narzędzia, które mogłyby przyczynić się do osiągnięcia wysokiego i zharmonizowanego poziomu ochrony danych.

EIOD podkreśla, że należy jasno rozróżnić te dwa elementy ze względu na ich różne skutki prawne oraz związane z nimi zobowiązania. Podstawowa zasada jest następująca: Komisja powinna ponosić całkowitą odpowiedzialność za pierwszy element, a grupa robocza powinna odgrywać rolę przewodnią w tym, co się tyczy drugiego elementu.

30. Inne, bardziej szczegółowe rozróżnienie należy poczynić w związku z dostępnymi narzędziami mającymi usprawnić wdrażanie dyrektywy. Obejmują one:

— środki wykonawcze. Środki te — przedsiębrane przez Komisję za pomocą procedury komitologii — przewidziano w rozdziale IV poświęconym przekazywaniu danych osobowych do państw trzecich (zob. art. 25 ust. 6 i art. 26 ust. 3);

— prawodawstwo branżowe;

— postępowania o naruszenie przepisów na mocy art. 226 TWE;

— komunikaty wyjaśniające. Takie komunikaty powinny skupiać się na przepisach, które mogą prowadzić do postępowań o naruszenie przepisów lub które przewidziano głównie jako wytyczne dla ochrony danych w praktyce (zob. także pkt 57-62) ([12]);

— inne komunikaty. Przykładem może służyć komunikat Komisji dla Parlamentu Europejskiego i Rady w sprawie technologii na rzecz ochrony prywatności;

— promowanie wzorców postępowania. To narzędzie może być wykorzystywane do wielu zagadnień, takich jak upraszczanie procedur administracyjnych, audyty, egzekwowanie prawa i kary itd. (zob. także pkt 63-67).

31. EIOD sugeruje Komisji, by jasno wskazała, w jaki sposób będzie korzystać z tych narzędzi podczas opracowywania swojej polityki na bazie omawianego komunikatu. Komisja w tym kontekście powinna również dokonać jasnego rozróżnienia własnych obowiązków od obowiązków grupy roboczej. Poza tym nie trzeba przypominać, że warunkiem sukcesu jest dobra współpraca między Komisją a grupą roboczą w każdej sytuacji.

B. **Interakcje z technologią**

32. Punktem wyjścia jest fakt, że przepisy dyrektywy zostały sformułowane w sposób neutralny z technicznego punktu widzenia. Komunikat łączy nacisk na techniczną neutralność z pewną liczbą osiągnięć technicznych, takich jak Internet, usługi dostępu świadczone w państwach trzecich, RFID oraz połączenie danych dźwiękowych i obrazowych z automatycznym rozpoznawaniem. Rozróżniono w nim dwa typy działań. Po pierwsze, konkretne wskazówki dotyczące stosowania zasad ochrony danych w zmieniającym się otoczeniu technicznym; istotną rolę odgrywa grupa robocza i wchodząca w jej skład grupa zadaniowa ds. Internetu ([13]). Po drugie, Komisja mogłaby przedstawiać wnioski dotyczące prawodawstwa branżowego.

33. EIOD z zadowoleniem przyjmuje to podejście jako jeden z istotnych pierwszych kroków. W dalszej perspektywie konieczne mogą być jednak inne, bardziej zasadnicze kroki. Wydanie omawianego komunikatu może być wykorzystane jako początek podejścia długoterminowego. EIOD sugeruje — w ramach działań wynikających z omawianego komunikatu — rozpoczęcie dyskusji nad tym podejściem. Jako ewentualne elementy takiego podejścia można wskazać przedstawione poniżej punkty.

([11]) Str. 6 komunikatu, przedostatni akapit.

([12]) Zob. np. opinię (WE) nr 4/2007 w sprawie pojęcia danych osobowych (WP 137) wydaną przez grupę roboczą i przyjętą dnia 20 czerwca 2007 r.

([13]) Grupa zadaniowa ds. Internetu jest częścią grupy roboczej art. 29.

34. Po pierwsze, interakcje z technologią są dwukierunkowe. Z jednej strony, nowe, dopiero rozwijające się technologie mogą wymagać modyfikacji ram prawnych ochrony danych. Z drugiej strony, potrzeba skutecznej ochrony danych osobowych poszczeglnych osób może wymagać nowych ograniczeń lub stosownych zabezpieczeń związanych z wykorzystaniem pewnych technologii, co jest bardziej dalekosiężnym skutkiem. Nowe technologie jednak mogą również być skutecznie wykorzystywane do ochrony prywatności i można je spożytkować.

35. Po drugie, mogą okazać się niezbędne określone limity, jeżeli nowe technologie będą stosowane przez instytucje rządowe podczas wykonywania zadań publicznych. Dyskusje nad interoperacyjnością i dostępem w przestrzeni wolności, bezpieczeństwa i sprawiedliwości związane z realizacją programu haskiego są tego dobrym przykładem ([14]).

36. Po trzecie, istnieje tendencja do coraz szerszego wykorzystywania materiału biometrycznego, takiego jak materiał genetyczny, choć nie tylko. Konkretne wyzwania związane z wykorzystywaniem danych osobowych ustalonych na bazie takiego materiału mogą mieć konsekwencje dla praw dotyczących ochrony danych.

37. Po czwarte, należy uznać, że samo społeczeństwo ulega zmianom i przybiera coraz więcej cech społeczeństwa kontrolowanego ([15]). Zmiany te wymagają debaty dotyczącej podstawowych zasad. Głównymi punktami tej debaty byłoby stwierdzenie, czy zmiany te są nieuniknione, czy jest zadaniem prawodawcy europejskiego ingerowanie w te zmiany oraz ograniczanie ich zasięgu oraz czy i w jaki sposób prawodawca europejski mógłby przedsiębrać skuteczne środki itd.

C. **Globalne zagadnienia dotyczące prywatności i jurysdykcji**

38. Globalne zagadnienia dotyczące prywatności i jurysdykcji odgrywają w komunikacie ograniczoną rolę. W tym kontekście jedynym zamiarem Komisji jest dalsze monitorowanie forów międzynarodowych i dalsze w nich uczestnictwo, by zapewnić zgodność zobowiązań państw członkowskich z ich obowiązkami wynikającymi z dyrektywy. Poza tym w komunikacie wymieniono pewną liczbę działań przeprowadzonych na rzecz uproszczenia wymogów dotyczących międzynarodowego transferu danych (zob. rozdział III niniejszej opinii).

39. EIOD wyraża ubolewanie, że temu zagadnieniu nie przyznano w komunikacie ważniejszej roli.

40. Obecnie rozdział IV dyrektywy (art. 25 i 26) wprowadza szczególne zasady przekazywania danych osobowych do państw trzecich, niezależnie od ogólnych zasad ochrony danych. Te szczególne zasady były opracowywane przez wiele lat z zamiarem osiągnięcia równowagi między ochroną osób, których dane mają zostać przekazane do państw trzecich, a m.in. wymaganiami handlu międzynarodowego i rzeczywistym funkcjonowaniem globalnych sieci telekomunikacyjnych. Komisja i grupa robocza ([16]), ale także np. Międzynarodowa Izba Handlowa, włożyły wiele wysiłku w uruchomienie tego systemu poprzez określanie odpowiedniego poziomu ochrony, standardowe klauzule umowne, zastosowanie wiążących zasad dla przedsiębiorstw itd.

41. Jeżeli chodzi o zastosowanie tego systemu do Internetu, szczególne znaczenie ma wyrok Trybunału Sprawiedliwości w sprawie *Lindqvist* ([17]). Trybunał zaznaczył wszechobecny charakter informacji w Internecie i zadecydował, że samo ładowanie danych na stronę internetową, nawet jeżeli te dane są w ten sposób udostępniane osobom w państwach trzecich posiadającym środki techniczne umożliwiające dostęp do nich, nie jest uznawane za przekazywanie danych do państwa trzeciego.

42. Ten system, stanowiący logiczną i konieczną konsekwencję ograniczeń terytorialnych Unii Europejskiej, nie zapewni pełnej ochrony obywatelowi UE, którego dotyczą dane, w społeczeństwie operującym w sieci, dla którego fizyczne granice tracą na znaczeniu (zob. przykłady w pkt 6 niniejszej opinii): informacje w Internecie są wszechobecne, lecz jurysdykcja prawodawcy europejskiego jest ograniczona terytorialnie.

43. Wyzwaniem będzie opracowanie praktycznych rozwiązań, które pogodziłyby potrzebę ochrony obywateli UE, których dotyczą dane, z ograniczeniami terytorialnymi Unii Europejskiej i jej państw członkowskich. EIOD — w swoich uwagach do komunikatu Komisji w sprawie strategii zewnętrznego wymiaru przestrzeni wolności, bezpieczeństwa i sprawiedliwości — zachęcał już Komisję do aktywnego zajęcia się propagowaniem ochrony danych osobowych na szczeblu międzynarodowym poprzez wspieranie dwu- i wielostronnych podejść z udziałem państw trzecich oraz współpracę z organizacjami międzynarodowymi ([18]).

([14]) Zob. np. uwagi do komunikatu Komisji w sprawie interoperacyjności między europejskimi bazami danych, z dnia 10 marca 2006 r., opublikowane na stronie internetowej EIOD.

([15]) Zob.: „Raport w sprawie społeczeństwa kontrolowanego" (*Report on the Surveillance Society*) przygotowany przez Surveillance Studies Network dla brytyjskiego komisarza ds. informacji (UK Information Commissioner) i przedstawiony na 28. Międzynarodowej Konferencji Komisarzy ds. Ochrony Danych i Prywatności w Londynie w dniach 2-3 listopada 2006 r. (zob.: www.privacyconference2006.co.uk (sekcja Documents [Dokumenty])).

([16]) Zob. np. dokument roboczy dotyczący jednolitej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z dnia 24 października 1995 r., przyjęty dnia 25 listopada 2005 r. (WP114); dokument roboczy ustanawiający procedurę współpracy na rzecz wydawania wspólnych opinii dotyczących odpowiednich środków zabezpieczających wynikających z wiążących zasad dla przedsiębiorstw, przyjęty dnia 14 kwietnia 2005 r. (WP107) oraz opinia 8/2003 w sprawie projektu standardowych klauzul umownych przedłożonego przez grupę stowarzyszeń przedsiębiorstw („alternatywny model umowy") przyjęta dnia 17 grudnia 2003 r. (WP84).

([17]) Wyrok Trybunału z dnia 6 listopada 2003 r., sprawa C-101/01, Zb. Orz. [2003], s. I-12971, pkt 56-71.

([18]) Zob. pismo do dyrektora generalnego Dyrekcji Sprawiedliwości, Wolności i Bezpieczeństwa Komisji Europejskiej w sprawie komunikatu „Strategia zewnętrznego wymiaru przestrzeni wolności, bezpieczeństwa i sprawiedliwości" z dnia 28 listopada 2005 r., dostępne na stronie internetowej EIOD.

44. Takie praktyczne rozwiązania obejmują:

— dalszy rozwój globalnych ram ochrony danych. Jako bazę można wykorzystać szerzej akceptowane normy, takie jak wytyczne OECD dla ochrony danych (1980) oraz wytyczne ONZ;

— dalszy rozwój szczególnych zasad przekazywania danych do państw trzecich, zawartych w rozdziale IV dyrektywy (art. 25 i 26);

— międzynarodowe porozumienia w sprawie jurysdykcji lub podobne porozumienia z państwami trzecimi;

— inwestycje w mechanizmy zgodności na szczeblu globalnym, takie jak stosowanie zasad wiążących dla przedsiębiorstw przez firmy międzynarodowe, niezależnie od miejsca przetwarzania przez nie danych osobowych.

45. Żadne z tych rozwiązań nie jest nowe. Konieczna jest jednak pewna wizja tego, w jaki sposób najskuteczniej wykorzystywać te metody i jak zapewnić, by standardy ochrony danych — które w Unii Europejskiej zaliczane są do praw podstawowych — były równie skuteczne w globalnym społeczeństwie operującym w sieci. EIOD zachęca Komisję do rozpoczęcia opracowywania takiej wizji we współpracy z najważniejszymi zainteresowanymi stronami.

D. **Egzekwowanie prawa**

46. W komunikacie poświęcono wiele uwagi wymogom wynikającym z interesu publicznego, szczególnie w zakresie bezpieczeństwa. Wyjaśniono w nim art. 3 ust. 2 dyrektywy oraz wykładnię tego przepisu wyrażoną przez Trybunał Sprawiedliwości w wyroku w sprawie PNR ([19]), a także art. 13 dyrektywy, związany m.in. z orzecznictwem Europejskiego Trybunału Praw Człowieka. W komunikacie ponadto podkreśla się, że gdy Komisja osiąga równowagę między środkami zapewniającymi bezpieczeństwo oraz niekwestionowanymi prawami podstawowymi, upewnia się, że dane osobowe są chronione zgodnie z art. 8 europejskiej konwencji o ochronie praw człowieka (EKOPC). Ten punkt wyjścia ma zastosowanie również do dialogu ze Stanami Zjednoczonymi Ameryki.

47. Zdaniem EIOD ważne jest, że Komisja w tak jasny sposób potwierdza wynikające z art. 6 TUE zobowiązania Unii do poszanowania praw podstawowych gwarantowanych przez EKOPC. Jest to tym istotniejsze teraz, gdy Rada Europejska zadecydowała, że na mocy traktatu reformującego Karta praw podstawowych Unii Europejskiej stanie się prawnie wiążąca. Artykuł 8 karty określa prawo każdej osoby do ochrony dotyczących jej danych osobowych.

48. Jest sprawą ogólnie znaną, że żądania organów ścigania dotyczące coraz szerszego wykorzystywania danych osobowych do walki z przestępczością — by nie wspomnieć zwalczania terroryzmu — wiążą się z ryzykiem obniżenia poziomu ochrony obywateli, nawet poniżej poziomu gwarantowanego art. 8 EKOPC lub konwencją Rady Europy nr 108 ([20]). Te obawy stanowiły trzon trzeciej opinii EIOD w sprawie wniosku dotyczącego decyzji ramowej Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych, wydanej dnia 27 kwietnia 2007 r.

49. W tym kontekście ma fundamentalne znaczenie, by standardy ochrony zapewniane przez dyrektywę zostały uznane za podstawę ochrony obywateli, także w związku z żądaniami organów ścigania. EKOPC i konwencja 108 zapewniają minimalny poziom ochrony, ale nie są wystarczająco precyzyjne. Konieczne były więc dodatkowe środki zapewniające obywatelom właściwą ochronę. Ta potrzeba była jednym z bodźców do przyjęcia dyrektywy ([21]) w 1995 r.

50. Równie zasadniczą kwestią jest skuteczne zagwarantowanie tego standardu ochrony we wszystkich sytuacjach, w których dane osobowe są przetwarzane do celów egzekwowania prawa. Choć omawiany komunikat nie omawia przetwarzania danych w obrębie trzeciego filaru, słusznie odnosi się do sytuacji, w której dane gromadzone (i przetwarzane) do celów handlowych są wykorzystywane do celów egzekwowania prawa. Sytuacja taka staje się coraz powszechniejsza, od kiedy policja coraz częściej polega na dostępności informacji posiadanych przez strony trzecie. Dyrektywę 2006/24/WE ([22]) można uznać za najlepszą ilustrację tej tendencji: dyrektywa ta zobowiązuje dostawców usług łączności elektronicznej do (dłuższego) przechowywania danych, które zgromadzili (i przechowują) do celów handlowych, by służyły one celom egzekwowania prawa. Zdaniem EIOD należy w pełni zagwarantować właściwą ochronę danych osobowych gromadzonych i przetwarzanych w ramach zakresu zastosowania dyrektywy, gdy są one wykorzystywane do celów interesu publicznego, w szczególności do celów związanych z bezpieczeństwem lub zwalczaniem terroryzmu. W niektórych przypadkach jednak te ostatnie cele mogą wykraczać poza zakres zastosowania dyrektywy.

([19]) Wyrok Trybunału z 30 maja 2006 r., Parlament Europejski przeciwko Radzie Unii Europejskiej (C-317/04) i Komisji (C-318/04), sprawy połączone C-317/04 i C-318/04, Zb. Orz. 2006, str. I-4721.

([20]) Konwencja Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych z dnia 28 stycznia 1981 r.

([21]) Brak precyzji w konwencji nr 108 został wspomniany przez EIOD w kilku opiniach w związku z potrzebą przyjęcia decyzji ramowej Rady.

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

51. Te obserwacje prowadzą do następujących sugestii skierowanych do Komisji:

— konieczna jest dalsza refleksja nad implikacjami, jakie ma dla ochrony danych zaangażowanie przedsiębiorstw prywatnych w działania w zakresie egzekwowania prawa; służyłaby ona zapewnieniu pełnego stosowania do tych sytuacji zasad zawartych w dyrektywie 95/46/WE oraz zapewnieniu tego, że żadne luki prawne nie zagrożą podstawowemu prawu obywateli do ochrony ich danych. Należy zwłaszcza zagwarantować właściwą i stałą ochronę danych osobowych zgromadzonych w ramach zakresu zastosowania dyrektywy także wtedy, gdy są one dalej przetwarzane do celów interesu publicznego, w ramach zakresu zastosowania dyrektywy lub poza nim;

— refleksja ta powinna w każdym wypadku obejmować niedociągnięcia obecnych ram prawnych, w których granica między pierwszym a trzecim filarem jest niejasna i w których mogą nawet wystąpić sytuacje całkowitego braku właściwej podstawy instrumentu prawnego dotyczącego ochrony danych ([23]);

— artykuł 13 dyrektywy, umożliwiający wyjątki od zasad ochrony danych i ograniczenia tych zasad, gdy są one konieczne m.in. ze względu na interes publiczny, należy przeredagować w taki sposób, by zachować jego skuteczność jako zasadniczej płaszczyzny wzajemnego oddziaływania i gwarancji dla danych osobowych gromadzonych w ramach zakresu zastosowania dyrektywy, zgodnie z wyrokiem Trybunału Sprawiedliwości w sprawie *Österreichischer Rundfunk* ([24]) i orzecznictwem Europejskiego Trybunału Praw Człowieka;

— należy rozważyć możliwość złożenia wniosków prawodawczych mających na celu harmonizację warunków stosowania wyjątków od art. 13 i związanych z nimi zabezpieczeń.

E. **Możliwa sytuacja po wejściu w życie traktatu reformującego**

52. W komunikacie Komisja porusza kwestię (ogromnego) wpływu traktatu konstytucyjnego na dziedzinę ochrony danych. Rzeczywiście traktat ten — obecnie zaś traktat reformujący — będzie miał fundamentalne znaczenie. Traktat oznacza koniec struktury filarowej, przepisy dotyczące ochrony danych (obecnie art. 286 TWE) zostaną wyjaśnione, a Karta praw podstawowych Unii Europejskiej, w której art. 8 znajduje się przepis o ochronie danych, stanie się instrumentem prawnie wiążącym.

53. W mandacie Konferencji Międzyrządowej zwrócono szczególną uwagę na ochronę danych. Pkt 19 ppkt f) zasadniczo zawiera trzy twierdzenia. Po pierwsze, ogólne zasady ochrony danych będą pozostawać bez uszczerbku dla szczególnych zasad przyjętych w tytule o WPZiB (obecny drugi filar); po drugie, zostanie przyjęte oświadczenie dotyczące ochrony danych w obszarach współpracy policyjnej i sądowej w sprawach karnych (obecny trzeci filar) i po trzecie, zostaną przyjęte konkretne zapisy w stosownych protokołach dotyczące stanowisk poszczególnych państw członkowskich (ten element jest związany przede wszystkim ze stanowiskiem Zjednoczonego Królestwa wobec współpracy policyjnej i sądowej w sprawach karnych).

54. Ten drugi element (oświadczenie) będzie wymagał objaśnienia w ramach Konferencji Międzyrządowej. Należy starannie rozważyć skutki zniesienia struktury filarowej oraz możliwości zastosowania dyrektywy o współpracy policyjnej i sądowej w sprawach karnych, by zapewnić jak najszersze możliwe stosowanie zasad ochrony danych zawartych w dyrektywie 95/46/WE. W niniejszej opinii nie ma miejsca na bardziej szczegółowe omówienie tego zagadnienia. EIOD przedstawił swoje propozycje dotyczące oświadczenia w piśmie skierowanym do przewodniczącego Konferencji Międzyrządowej ([25]).

VI. **NARZĘDZIA SŁUŻĄCE LEPSZEMU WDRAŻANIU DYREKTYWY**

A. **Uwaga ogólna**

55. Komunikat odnosi się do licznych narzędzi i działań, które można wykorzystać w przyszłości w celu lepszego wdrażania dyrektywy. EIOD pragnie przedstawić swoje uwagi do nich, wraz z analizą dodatkowych instrumentów, które nie zostały wspomniane w komunikacie.

B. **Prawodawstwo branżowe**

56. W niektórych przypadkach może okazać się niezbędne konkretne działanie prawodawcze na szczeblu UE. Zwłaszcza konieczne może się okazać prawodawstwo branżowe, pozwalające dostosować zasady zawarte w dyrektywie do problemów związanych z pewnymi technologiami, jak w przypadku dyrektyw o ochronie prywatności w sektorze telekomunikacyjnym. Należy szczegółowo rozważyć zastosowanie szczególnego prawodawstwa w takich dziedzinach, jak wykorzystanie technologii RFID.

C. **Postępowanie o naruszenie przepisów**

57. Najważniejszym instrumentem wspomnianym w komunikacie jest postępowanie o naruszenie przepisów. Komunikat określa jeden obszar wymagający szczególnej uwagi, tj. niezależność organów ochrony danych i ich uprawnienia; innym obszarom poświęcono tylko ogólny komentarz. EIOD podziela opinię, że postępowania o naruszenie przepisów stanowią podstawowe i nieuniknione narzędzie, jeżeli państwa członkowskie nie zapewnią pełnego wdrożenia dyrektywy, zwłaszcza biorąc pod uwagę fakt, że minęło niemal dziewięć lat od terminu wdrożenia dyrektywy i że odbył się już zorganizowany dialog określony w programie prac. Do dnia dzisiejszego jednak do Trybunału Sprawiedliwości nie wpłynęła żadna sprawa o naruszenie przepisów dyrektywy 95/46/WE.

([23]) Kwestia „luki prawnej", kilkakrotnie poruszona przez EIOD, głównie w związku z wyrokiem w sprawie PNR (zob. np. sprawozdanie roczne za 2006 r., s. 47).

([24]) Wyrok Trybunału z dnia 20 maja 2003 r., sprawy połączone C-465/00, C-138/01 i C-139/01, Zb. Orz. 2003, str. I-4989.

([25]) Zob. pismo EIOD z dnia 23 lipca 2007 r. do przewodniczącego Konferencji Międzyrządowej w sprawie ochrony danych na mocy traktatu reformującego, dostępne na stronie internetowej EIOD.

58. Analiza porównawcza wszystkich przypadków, w których podejrzewa się niewłaściwą lub niepełną transpozycję przepisów ([26]), oraz komunikat wyjaśniający mogą z pewnością zwiększyć spójność roli Komisji jako strażnika Traktatów. Przygotowanie tych instrumentów, które może wymagać pewnego czasu i wysiłku, nie powinno jednak opóźniać postępowań o naruszenie przepisów w tych dziedzinach, w których Komisja jednoznacznie stwierdziła niewłaściwą transpozycję lub błędne praktyki.

59. EIOD zachęca zatem Komisję do starania się o lepsze wdrażanie dyrektywy za pomocą — o ile to konieczne — postępowań o naruszenie przepisów. W tym kontekście EIOD skorzysta ze swoich uprawnień do interwencji przed Trybunałem Sprawiedliwości, by wziąć udział — w stosownych przypadkach — w postępowaniach o naruszenie przepisów związanych z wdrażaniem dyrektywy 95/46/WE lub z innymi instrumentami prawnymi w obszarze ochrony danych osobowych.

D. **Komunikat wyjaśniający**

60. Komunikat również zawiera odniesienie do komunikatu wyjaśniającego niektóre przepisy, w którym Komisja objaśni swoją interpretację tych przepisów dyrektywy, których wdrażanie okazało się problematyczne i może w konsekwencji prowadzić do postępowań o naruszenie przepisów. EIOD z zadowoleniem przyjmuje fakt, że w tym kontekście Komisja uwzględni prace nad interpretacją przeprowadzone przez grupę roboczą. Należyte uwzględnienie stanowiska grupy roboczej podczas redagowania tego komunikatu wyjaśniającego oraz właściwe przeprowadzenie konsultacji z grupą roboczą mają fundamentalne znaczenie dla wykorzystania doświadczenia tej grupy w zakresie wdrażania dyrektywy na szczeblu krajowym.

61. Ponadto EIOD potwierdza, że jest gotowy doradzać Komisji we wszystkich kwestiach związanych z ochroną danych osobowych. Dotyczy to również tych instrumentów — takich jak komunikat Komisji — które nie są wiążące, ale mają na celu określenie polityki Komisji w dziedzinie ochrony danych osobowych. By EIOD mógł skutecznie prowadzić działania doradcze, w przypadku komunikatów konsultacje z nim powinny mieć miejsce przed przyjęciem komunikatu wyjaśniającego ([27]). Rola zarówno grupy roboczej art. 29, jak i EIOD jako doradców wniesie do tego komunikatu dodatkowe wartości, nie naruszając niezależności Komisji w samodzielnym podejmowaniu decyzji o formalnym rozpoczęciu postępowań o naruszenie przepisów związanych z wdrażaniem dyrektywy.

62. EIOD z zadowoleniem przyjmuje fakt, że komunikat będzie się odnosił jedynie do ograniczonej liczby artykułów, umożliwiając w ten sposób skupienie się na trudniejszych kwestiach. Z tego punktu widzenia EIOD zwraca uwagę Komisji na następujące zagadnienia, które zasługują na szczególną uwagę w komunikacie wyjaśniającym:

— pojęcie danych osobowych ([28]);

— definicja roli administratora danych lub przetwarzającego;

— określenie prawa właściwego;

— zasada ograniczenia celu i niezgodne z nią wykorzystanie danych;

— podstawa prawna przetwarzania danych, szczególnie w odniesieniu do jednoznacznego wyrażenia zgody oraz do wyważenia interesów.

E. **Inne, niewiążące instrumenty**

63. Inne, niewiążące instrumenty powinny pomagać w osiąganiu zgodności z zasadami ochrony danych, szczególnie w nowych otoczeniach technicznych. Środki te powinny być oparte na zasadzie „prywatności wynikającej z projektu" (ang. *privacy by design*) i zapewniać opracowywanie i tworzenie struktur nowych technologii z właściwym uwzględnieniem zasad ochrony danych. Zasadniczy tego element powinna stanowić promocja produktów technologicznych zgodnych z zasadami poszanowania prywatności w kontekście szybko wzrastającego wszechobecnego użycia komputerów.

64. Ściśle powiązana z powyższym jest potrzeba zwiększenia liczby stron zainteresowanych egzekwowaniem prawa o ochronie danych. Z jednej strony, EIOD zdecydowanie popiera zasadniczą rolę organów ochrony danych w egzekwowaniu realizacji zasad zawartych w dyrektywie przy pełnym wykorzystaniu swoich uprawnień oraz zakresu koordynacji w ramach grupy roboczej art. 29. Skuteczniejsze wdrażanie dyrektywy jest również jednym z celów „inicjatywy londyńskiej".

65. Z drugiej strony, EIOD podkreśla, że pożądane jest propagowanie wdrażania zasad ochrony danych w przedsiębiorstwach prywatnych poprzez samoregulację i konkurencyjność. Należy zachęcać przemysł do wdrażania zasad ochrony danych i konkurowania w opracowywaniu produktów i usług zgodnych z zasadami poszanowania prywatności jako sposobu zwiększania swego udziału w rynku poprzez lepsze dostosowanie się do oczekiwań konsumentów świadomych kwestii związanych z prywatnością. Dobrym przykładem mogą być etykiety dotyczące ochrony prywatności, które można dołączać do produktów i usług po uprzednim przeprowadzeniu certyfikacji ([29]).

([26]) Zob. komunikat, str. 6.

([27]) ob. dokument strategiczny EIOD „EIOD doradza instytucjom Wspólnoty w sprawie wniosków legislacyjnych i związanych z nimi dokumentów", dostępny na stronie internetowej EIOD (pkt 5.2 tego dokumentu).

([28]) To zagadnienie zostało również omówione w opinii nr 4/2007 grupy roboczej, wspomnianej w przypisie 9.

([29]) Warto wspomnieć o projekcie „EuroPriSe", promowanym przez Organ Ochrony Danych Landu Schleswig-Holstein w ramach projektu „Eten" Komisji Europejskiej.

66. EIOD pragnie również zwrócić uwagę Komisji na inne narzędzia, które — choć nie zostały wspomniane w komunikacie — mogłyby okazać się użyteczne w lepszym wdrażaniu dyrektywy. Przykładami takich narzędzi, które mogłyby pomóc organom ochrony danych w lepszym wdrażaniu prawa dotyczącego ochrony danych, są:

— analiza porównawcza;

— propagowanie wzorców postępowania i dzielenie się nimi;

— przeprowadzane przez strony trzecie kontrole zachowywania prywatności.

F. **Inne instrumenty w dalszej perspektywie**

67. Na koniec EIOD odnosi się do innych instrumentów, które nie zostały wspomniane w komunikacie, ale mogłyby zostać rozważone w związku z przyszłymi zmianami w dyrektywie lub włączone do innych horyzontalnych aktów prawnych; w szczególności:

— działania uprawniające grupy obywateli do wspólnego wszczynania postępowań spornych w sprawach dotyczących ochrony danych osobowych mogłyby stanowić bardzo istotne narzędzie ułatwiające wdrażanie dyrektywy;

— działania zapoczątkowane przez osoby prawne, takie jak stowarzyszenia konsumentów i związki zawodowe, których działalność ma na celu ochronę pewnych kategorii osób, mogłyby przynieść podobne efekty;

— zobowiązanie administratorów danych do powiadamiania osób, których dotyczą dane, o naruszeniu bezpieczeństwa tych danych stanowiłoby nie tylko wartościowe zabezpieczenie, lecz także sposób lepszego informowania obywateli;

— przepisy ułatwiające stosowanie etykiet dotyczących ochrony prywatności lub przeprowadzanych przez strony trzecie kontroli zachowywania prywatności (zob. pkt 65 i 66) w sprawach międzynarodowych.

G. **Lepsze określenie obowiązków zainteresowanych instytucji, zwłaszcza grupy roboczej**

68. Różne instytucje mają obowiązki związane z wdrażaniem dyrektywy. Organy nadzorcze w państwach członkowskich na mocy art. 28 dyrektywy ponoszą odpowiedzialność za kontrolę stosowania na ich terytorium przepisów przyjętych przez państwa członkowskie na mocy tej dyrektywy. Artykuł 29 wprowadza grupę roboczą złożoną z organów nadzorczych, a w art. 30 wymieniono zadania tej grupy. Na mocy art. 31 komitet składający się z przedstawicieli rządów państw członkowskich wspiera Komisję w związku z przedsiębraniem środków na szczeblu wspólnotowym (komitet działający w ramach procedury komitologii).

69. Potrzeba lepszego określenia obowiązków tych różnych instytucji jest szczególnie widoczna w przypadku (działań) grupy roboczej. W art. 30 ust. 1 wymieniono cztery zadania grupy roboczej, które można podsumować jako badanie wdrażania dyrektywy na szczeblu krajowym, pod kątem jego jednolitości, oraz wyrażanie opinii na temat zmian na szczeblu wspólnotowym: poziom ochrony, wnioski legislacyjne i kodeksy postępowania. Ten wykaz pokazuje, jak daleko sięga odpowiedzialność grupy roboczej w dziedzinie ochrony danych, czego ilustracją są dokumenty sporządzone przez tę grupę na przestrzeni lat.

70. Zgodnie z tekstem komunikatu grupa robocza „odgrywa kluczową rolę w zapewnianiu skuteczniejszego i bardziej spójnego wdrażania dyrektywy". EIOD w pełni przychyla się do tej opinii, lecz uważa również za konieczne wyjaśnienie pewnych konkretnych elementów obowiązków grupy roboczej.

71. Po pierwsze, komunikat wzywa do zwiększenia wkładu grupy roboczej, gdyż organy krajowe powinny starać się o dostosowanie praktyk krajowych do wspólnej linii postępowania ([30]). EIOD z zadowoleniem przyjmuje zamiar, jaki przyświeca temu stwierdzeniu, ale ostrzega przed nakładaniem się na siebie obowiązków. Zgodnie z art. 211 TWE zadaniem Komisji jest czuwanie nad stosowaniem postanowień Traktatu przez państwa członkowskie, w tym również przez ich organy nadzorcze. Grupa robocza jako niezależny organ doradczy nie może być pociągana do odpowiedzialności za stosowanie się organów krajowych do jej opinii.

72. Po drugie, Komisja musi być świadoma swoich różnych ról w ramach grupy roboczej, gdyż jest ona nie tylko członkiem tej grupy, lecz także organizuje jej sekretariat. Odgrywając rolę sekretariatu musi wspierać grupę roboczą w taki sposób, by mogła ona wykonywać swoją pracę w sposób niezawisły. Zasadniczo oznacza to dwie rzeczy: Komisja musi zapewnić niezbędne środki, a sekretariat musi pracować zgodnie z instrukcjami grupy roboczej i jej przewodniczącego w tym, co się tyczy treści i zakresu działalności grupy roboczej oraz charakteru wyników jej prac. Ogólniej rzecz biorąc, działania Komisji w ramach wypełniania jej pozostałych obowiązków wynikających z prawa WE nie powinny negatywnie wpływać na jej dostępność jako sekretariatu.

73. Po trzecie, chociaż określenie priorytetów grupy roboczej zależy od jej własnego uznania, Komisja mogłaby wskazywać, czego oczekuje od grupy roboczej i jak — w jej opinii — można najlepiej wykorzystać dostępne środki.

74. Po czwarte, EIOD wyraża ubolewanie, że w komunikacie nie zawarto jasnych wskazówek dotyczących podziału ról pomiędzy Komisję i grupę roboczą. Zachęca Komisję do przedłożenia grupie roboczej dokumentu, który zawierałby takie wskazówki. EIOD proponuje, by w dokumencie tym ująć następujące kwestie:

— Komisja mogłaby zwrócić się do grupy roboczej o podjęcie prac nad kilkoma konkretnymi zagadnieniami. Wnioski Komisji powinny być oparte na jasnej strategii zadań i priorytetów grupy roboczej;

([30]) Zob. str. 11 komunikatu.

— grupa robocza sama ustala swoje priorytety w programie prac, w którym są one jasno zaprezentowane;

— Komisja i grupa robocza mogłyby ewentualnie zebrać swoje ustalenia w protokole ustaleń;

— jest kwestią zasadniczą, by grupa robocza w pełni uczestniczyła w wykładni dyrektywy i przyczyniała się do dyskusji mających na celu ewentualne zmiany w dyrektywie.

VII. **WNIOSKI**

75. EIOD podziela główny wniosek Komisji, że dyrektywy w perspektywie krótkoterminowej nie należy zmieniać. Ten wniosek wspiera się również na charakterze dyrektywy oraz polityce prawodawczej Unii.

76. EIOD wyszedł od następujących przesłanek:

— w perspektywie krótkoterminowej najlepiej nakierować działania na usprawnienie wdrażania dyrektywy;

— w dalszej perspektywie zmiany w dyrektywie wydają się nieuchronne;

— należy już określić konkretny termin przeglądu, by przygotować wnioski dotyczące zmian. Taki termin byłby wyraźnym bodźcem do niezwłocznego rozpoczęcia refleksji nad przyszłymi zmianami.

77. Główne elementy przyszłych zmian są między innymi następujące:

— nie jest konieczne wprowadzenie nowych zasad, ale istnieje oczywista potrzeba wprowadzenia innych rozwiązań administracyjnych;

— szeroki zakres zastosowania prawa o ochronie danych do wszystkich sposobów wykorzystywania danych osobowych nie powinien ulec zmianie;

— prawo o ochronie danych powinno pozwalać w konkretnych przypadkach na wyważone podejście, a także umożliwiać organom ochrony danych określanie priorytetów;

— system powinien mieć w pełni zastosowanie do wykorzystywania danych osobowych do celów egzekwowania prawa, choć mogą być konieczne odpowiednie środki dodatkowe, by rozwiązać szczególne problemy w tej dziedzinie.

78. EIOD sugeruje, by Komisja szczegółowo opracowała: harmonogram działań omówionych w rozdziale 3 komunikatu; ostateczny termin przedstawienia kolejnego sprawozdania z wdrażania dyrektywy; zakres zadań umożliwiający ocenę realizacji przewidzianych działań; wskazówki co do sposobu postępowania w dalszej perspektywie.

79. EIOD z zadowoleniem przyjmuje przedstawione podejście do technologii jako jeden z istotnych pierwszych kroków i sugeruje rozpoczęcie dyskusji na temat podejścia długoterminowego, obejmującej m.in. debatę dotyczącą podstawowych zasad rozwoju społeczeństwa kontrolowanego. Również z zadowoleniem postrzega toczący się przegląd dyrektywy 2002/58/WE oraz ewentualną potrzebę określenia bardziej szczegółowych zasad odnoszących się do kwestii ochrony danych związanych z nowymi technologiami, takimi jak Internet i RFID. W tych działaniach należy brać pod uwagę całość zmieniającego się kontekstu, a w dalszej perspektywie objąć nimi również dyrektywę 95/46/WE.

80. EIOD wyraża ubolewanie, że globalne zagadnienia dotyczące prywatności i jurysdykcji odgrywają w komunikacie tak ograniczoną rolę i zwraca się o opracowanie praktycznych rozwiązań, które pogodziłyby potrzebę ochrony obywateli UE, których dotyczą dane, z ograniczeniami terytorialnymi Unii Europejskiej i jej państw członkowskich, takich jak: dalszy rozwój globalnych ram ochrony danych; dalszy rozwój szczególnych zasad przekazywania danych do państw trzecich; międzynarodowe porozumienia w sprawie jurysdykcji lub podobne porozumienia z państwami trzecimi; inwestycje w mechanizmy zgodności na szczeblu globalnym, takie jak stosowanie zasad wiążących dla przedsiębiorstw przez firmy międzynarodowe.

EIOD zachęca Komisję do rozpoczęcia — wraz z najważniejszymi zainteresowanymi stronami — refleksji nad tymi kwestiami.

81. Co do egzekwowania prawa EIOD pragnie przekazać Komisji następujące sugestie:

— dalszą refleksję nad implikacjami, jakie ma zaangażowanie przedsiębiorstw prywatnych w działania w zakresie egzekwowania prawa;

— zachowanie skuteczności art. 13 dyrektywy, z możliwością złożenia wniosków prawodawczych mających na celu harmonizację warunków stosowania wyjątków od art. 13 i związanych z nimi zabezpieczeń.

82. Pełne wdrożenie dyrektywy oznacza (1) zapewnienie całkowitego wypełniania przez państwa członkowskie ich obowiązków wynikających z prawa europejskiego oraz (2) pełne wykorzystanie innych, niewiążących narzędzi, które mogą przyczynić się do osiągnięcia wysokiego i zharmonizowanego poziomu ochrony danych. EIOD zwraca się do Komisji o jasne wskazanie sposobu wykorzystania tych różnych instrumentów oraz sposobu oddzielania jej własnych obowiązków od obowiązków grupy roboczej.

83. W odniesieniu do wspomnianych wyżej instrumentów:

— w niektórych przypadkach może okazać się niezbędne konkretne działanie prawodawcze na szczeblu UE;

— zachęca się Komisję do starania się o lepsze wdrażanie dyrektywy za pomocą postępowań o naruszenie prawa;

— zachęca się Komisję do wykorzystania komunikatu wyjaśniającego — z poszanowaniem roli doradczej grupy roboczej i EIOD — do omówienia następujących kwestii: pojęcia danych osobowych; definicji roli administratora danych lub przetwarzającego; określenia prawa właściwego; zasady ograniczenia celu i niezgodnego z nią wykorzystania danych; podstawy prawnej przetwarzania danych, szczególnie w odniesieniu do jednoznacznego wyrażenia zgody oraz do wyważenia interesów;

— niewiążące prawnie instrumenty obejmują instrumenty zasadzające się na pojęciu „prywatności wynikającej z projektu";

— w dalszej perspektywie: działania pewnych grup obywateli; działania zapoczątkowane przez osoby prawne, których działalność ma na celu ochronę pewnych kategorii osób; zobowiązanie administratorów danych do powiadamiania osób, których dotyczą dane, o naruszeniu bezpieczeństwa tych danych; przepisy ułatwiające stosowanie etykiet dotyczących ochrony prywatności lub przeprowadzanych przez strony trzecie kontroli zachowywania prywatności w sprawach międzynarodowych.

84. EIOD zachęca Komisję do przedłożenia grupie roboczej dokumentu, który zawierałby jasne wskazówki co do podziału ról między Komisję a grupę roboczą i podejmowałby następujące kwestie:

— złożone przez Komisję wnioski o podjęcie prac nad kilkoma konkretnymi zagadnieniami, oparte na jasnej strategii i priorytetach ustalonych przez grupę roboczą;

— możliwość zapisania uzgodnień w protokole ustaleń;

— pełne zaangażowanie grupy roboczej w interpretację dyrektywy oraz dyskusje prowadzące do jej ewentualnych zmian.

85. Należy starannie rozważyć skutki wejścia w życie traktatu reformującego, by zapewnić jak najszersze możliwe stosowanie zasad ochrony danych zawartych w dyrektywie. EIOD przedstawił swoje propozycje w piśmie skierowanym do przewodniczącego Konferencji Międzyrządowej.

Sporządzono w Brukseli, dnia 25 lipca 2007 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych