Opinia Europejskiego Inspektora Ochrony Danych w sprawie komunikatu Komisji do Parlamentu Europejskiego i Rady dotyczącego przestrzeni wolności, bezpieczeństwa i sprawiedliwości w służbie obywateli

(2009/C 276/02)

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,

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, w szczególności jego art. 41,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

I. WPROWADZENIE

1. W dniu 10 czerwca 2009 r. Komisja przyjęła komunikat Komisji do Parlamentu Europejskiego i Rady dotyczący przestrzeni wolności, bezpieczeństwa i sprawiedliwości w służbie obywateli ([1]). Zgodnie z art. 41 rozporządzenia (WE) nr 45/2001 Inspektor przedstawia niniejszą opinię.

2. Przed przyjęciem przedmiotowego komunikatu Komisja przesłała w jego sprawie Inspektorowi – w piśmie z dnia 19 maja 2009 r. – nieformalną prośbę o konsultację. Inspektor odpowiedział na tę prośbę o konsultację w dniu 20 maja 2009 r., przesyłając nieformalne uwagi, których celem była dalsza poprawa brzmienia komunikatu. Ponadto Inspektor miał aktywny wkład w powstanie pisma Grupy Roboczej ds. Policji i Wymiaru Sprawiedliwości w sprawie programu wieloletniego w przestrzeni wolności, bezpieczeństwa i sprawiedliwości z dnia 14 stycznia 2009 r. ([2]).

3. W komunikacie (pkt 1) podkreśla się, że Unia „musi przyjąć nowy program wieloletni, który w oparciu o już poczynione postępy i po wyciągnięciu wniosków z obecnych słabszych punktów, nakreśli ambitne działania na przyszłość. W nowym programie należy określić priorytety na następne pięciolecie". Ten program wieloletni (znany jako „program sztokholmski") będzie kontynuacją programu haskiego i programu z Tampere, które stały się silnym bodźcem politycznym dla przestrzeni wolności, bezpieczeństwa i sprawiedliwości.

4. Omawiany komunikat ma stanowić podstawę tego nowego programu wieloletniego. Inspektor zauważa w związku z tym, że nawet jeśli programy wieloletnie same w sobie nie są aktami wiążącymi, mają znaczny wpływ na politykę prowadzoną przez instytucje w danej dziedzinie, ponieważ na takim programie wieloletnim opierać się będzie wiele konkretnych działań – ustawodawczych i innych.

5. Sam komunikat musi więc być rozpatrywany z tego punktu widzenia. Jest on kolejnym etapem w debacie, która rozpoczęła się w przybliżeniu od przedstawienia w czerwcu 2008 r. dwóch sprawozdań tzw. „grup doradczych ds. przyszłości", które zostały ustanowione przez prezydencję Rady z zadaniem dokonania wkładu w debatę: „Wolność, bezpieczeństwo, prywatność – europejskie sprawy wewnętrzne w otwartym świecie" ([3]) oraz „Propozycje dotyczące przyszłego programu w dziedzinie wymiaru sprawiedliwości UE" ([4]).

II. ZASADNICZA TREŚĆ OPINII

6. Niniejsza opinia jest nie tylko odpowiedzią na omawiany komunikat, ale stanowi także wkład Inspektora w bardziej ogólną debatę poświęconą przyszłości przestrzeni wolności, bezpieczeństwa i sprawiedliwości, która musi doprowadzić do powstania nowego strategicznego programu prac (program sztokholmski), zgodnie z zapowiedziami szwedzkiej prezydencji UE ([5]). W niniejszej opinii omówione zostaną także niektóre konsekwencje ewentualnego wejścia w życie traktatu lizbońskiego.

7. Po nakreśleniu najważniejszych perspektyw opinii w części III, w części IV przedstawiona zostanie ogólna ocena komunikatu.

8. W części V poruszona zostanie kwestia tego, jak należy odnieść się do potrzeby ciągłego zapewniania ochrony prywatności i danych osobowych w kontekście wzrastającej ilości wymienianych danych osobowych. Szczególny nacisk położony zostanie na pkt 2.3 komunikatu, w którym mowa jest o ochronie danych osobowych i prywatności oraz – w bardziej ogólnym ujęciu – na konieczność podjęcia działań ustawodawczych i innych środków w celu usprawnienia ram ochrony danych.

([1]) COM(2009) 262 wersja ostateczna („komunikat").

([2]) Nieopublikowane. Grupa Robocza ds. Policji i Wymiaru Sprawiedliwości została ustanowiona na Europejskiej Konferencji Komisarzy ds. Ochrony Danych w celu przygotowania stanowiska konferencji w zakresie egzekwowania prawa oraz w celu występowania w imieniu konferencji w sprawach niecierpiących zwłoki.

([3]) Dokument Rady nr 11657/08 zwany dalej „sprawozdaniem dotyczącym spraw wewnętrznych".

([4]) Dokument Rady nr 11549/08 („sprawozdanie dotyczące wymiaru sprawiedliwości").

([5]) Rządowy program prac UE, http://www.regeringen.se

9. W części VI znajduje się omówienie potrzeb i możliwości przechowywania i wymiany informacji oraz dostępu do nich, jako narzędzi egzekwowania prawa lub, aby zacytować komunikat, narzędzi „Europy, która chroni". W pkt 4 komunikatu określono szereg celów dotyczących przepływu informacji i instrumentów technologicznych, w szczególności w pkt 4.1.2 (Kontrola nad informacjami), 4.1.3 (Wykorzystywanie niezbędnych instrumentów technologicznych) i 4.2.3.2 (Systemy informacyjne). Stworzenie europejskiego modelu informacji (pkt 4.1.2) może być postrzegane w tym kontekście jako największe wyzwanie. W opinii Inspektora znajduje się dogłębna analiza tej propozycji.

10. W części VII znajduje się zwięzłe omówienie konkretnego zagadnienia z zakresu przestrzeni wolności, bezpieczeństwa i sprawiedliwości mającego znaczenie dla ochrony danych, a mianowicie dostępu do wymiaru sprawiedliwości i e-sprawiedliwości.

III. **PERSPEKTYWY OPINII**

11. Osią analizy komunikatu i – w bardziej ogólnym ujęciu – przyszłości przestrzeni wolności, bezpieczeństwa i sprawiedliwości w kształcie ujętym w nowym programie wieloletnim będzie w niniejszej opinii potrzeba ochrony praw podstawowych. Ponadto podstawą niniejszej opinii będzie wkład Inspektora – zwłaszcza w charakterze konsultacyjnym – w rozwój polityki UE w tej dziedzinie. Inspektor przyjął dotychczas ponad trzydzieści opinii i uwag, które dotyczą inicjatyw powstałych w wyniku programu haskiego i które wszystkie zamieszczono na jego stronie internetowej.

12. W swojej ocenie komunikatu Inspektor uwzględni w szczególności następujące cztery perspektywy, które są istotne dla przyszłości przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Wszystkie te perspektywy odgrywają kluczową rolę także w komunikacie.

13. Pierwszą z perspektyw jest wykładniczy wzrost ilości zapisanych cyfrowo informacji dotyczących obywateli, który wynika z rozwoju technologii informatycznych i komunikacyjnych ([6]). Społeczeństwo zmierza w kierunku koncepcji nazywanej często „społeczeństwem nadzoru", w której każda czynność i niemal każde działanie obywateli najprawdopodobniej pozostawi po sobie ślad w postaci cyfrowego zapisu. Szybki rozwój koncepcji takich jak „Internet przedmiotów" i społeczeństwo oparte na inteligentnym otoczeniu technologicznym już teraz jest faktem dzięki wykorzystaniu identyfikatorów RFID. Coraz powszechniejsze staje się korzystanie z zapisanych w formie cyfrowej danych dotyczących ciała ludzkiego (dane biometryczne). Prowadzi to do powstawania świata oplecionego coraz gęstszą siecią połączeń, w którym organizacje bezpieczeństwa publicznego mogą uzyskiwać dostęp do ogromnych ilości potencjalnie użytecznych informacji mogących mieć bezpośredni wpływ na życie zainteresowanych osób.

14. Drugą perspektywą jest internacjonalizacja. Z jednej strony w erze cyfrowej wymiana danych nie jest ograniczona granicami zewnętrznymi Unii Europejskiej, a z drugiej strony coraz bardziej potrzebna staje się współpraca międzynarodowa w pełnym zakresie działań UE w przestrzeni wolności, bezpieczeństwa i sprawiedliwości: zwalczanie terroryzmu, współpraca policyjna i sądowa, wymiar sprawiedliwości w sprawach cywilnych i kontrola granic to tylko niektóre z przykładów.

15. Trzecią perspektywą jest wykorzystanie danych do celów egzekwowania prawa: ostatnie zagrożenia społeczne, związane z terroryzmem i nie tylko, doprowadziły do (żądań) stworzenia organom ścigania większych możliwości gromadzenia, przechowywania i wymiany danych osobowych. W wielu przypadkach w procesie tym uczestniczą aktywnie podmioty prywatne, co pokazała m.in. dyrektywa w sprawie zatrzymywania danych ([7]) oraz szereg różnych aktów w sprawie danych dotyczących przelotu pasażera ([8]).

16. Czwarta perspektywa dotyczy swobody przemieszczania się. Stopniowy rozwój przestrzeni wolności, bezpieczeństwa i sprawiedliwości wymaga dalszego usuwania granic wewnętrznych i ewentualnych barier ograniczających swobodę przemieszczania się w tym obszarze. Nowe akty dotyczące tej przestrzeni nie powinny pod żadnym pozorem prowadzić do ponownego tworzenia barier. Swoboda przemieszczania się obejmuje w aktualnym kontekście z jednej strony swobodę przemieszczania się osób, a z drugiej strony swobodny przepływ danych (osobowych).

17. Te cztery perspektywy pokazują, że kontekst, w jakim wykorzystywane są informacje, ulega szybkim zmianom. Dlatego też nie może być wątpliwości co do tego, jak istotny jest silny mechanizm ochrony praw podstawowych obywatela, a w szczególności ochrony jego prywatności i danych. Z tych właśnie względów Inspektor zdecydował, że główną osią jego analizy będzie konieczność istnienia takiej ochrony, o czym wspomniano w pkt 11.

([6]) W sprawozdaniu dotyczącym spraw wewnętrznych określa się to nawet mianem „cyfrowego tsunami".

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

([8]) Zob. np. Umowa między Unią Europejską a Stanami Zjednoczonymi Ameryki o przetwarzaniu i przekazywaniu przez przewoźników lotniczych danych dotyczących przelotu pasażera (PNR) do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych (DHS) (Umowa PNR z 2007 r.), Dz.U. L 204 z 4.8.2007, s. 18 i wniosek dotyczący decyzji ramowej Rady w sprawie wykorzystywania danych dotyczących rezerwacji pasażera (danych PNR) w celu egzekwowania prawa, COM(2007) 654 wersja ostateczna.

IV. **OGÓLNA OCENA**

18. Celem komunikatu i programu sztokholmskiego jest określenie zamiarów UE na nadchodzące pięć lat, jednak ich skutki mogą być bardziej długofalowe. Inspektor zauważa, że komunikat napisany został w sposób neutralny w stosunku do traktatu z Lizbony. Inspektor zdaje sobie doskonale sprawę, dlaczego Komisja przyjęła takie podejście, ale ubolewa nad tym, że komunikat nie był w stanie w pełni wykorzystać dodatkowych możliwości, które daje traktat lizboński. Perspektywa traktatu lizbońskiego zostanie w niniejszej opinii omówiona dokładniej.

19. Komunikat jest rozwinięciem wyników działań podejmowanych przez UE w ostatnich latach w zakresie przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Można stwierdzić, że wyniki te dotyczą konkretnych zdarzeń, z naciskiem na środki zwiększające uprawnienia organów ścigania i środki ingerujące w życie obywateli. Dotyczy to z pewnością dziedzin, w których dane osobowe wykorzystywane i wymieniane są w sposób intensywny i które z tego względu mają kluczowe znaczenie dla ochrony danych. Wyniki dotyczą konkretnych zdarzeń, ponieważ to właśnie wydarzenia zewnętrzne, takie jak zamachy w USA z dnia 11 września 2001 r. oraz zamachy bombowe w Madrycie i Londynie, dały silny impuls do rozpoczęcia działań ustawodawczych. Na przykład przekazywanie danych pasażerów do USA może być postrzegane jako rezultat zamachów z dnia 11 września 2001 r. ([9]), natomiast do przyjęcia dyrektywy 2006/24/WE w sprawie zatrzymania danych ([10]) doprowadziły zamachy bombowe w Londynie. Nacisk położono na bardziej inwazyjne środki, ponieważ prawodawcy w UE skupiali się na środkach ułatwiających wykorzystywanie i wymianę danych, natomiast mniej uwagi poświęcono środkom mającym na celu zapewnienie ochrony danych osobowych. Najważniejszym środkiem ochronnym przyjętym po trzech latach rozmów w Radzie była decyzja ramowa Rady 2008/977/WSiSW w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych ([11]). Ta decyzja ramowa nie jest w pełni zadowalająca (zob. pkt 29–30).

20. Doświadczenie ostatnich lat uczy, że przed przyjmowaniem nowych aktów prawnych należy brać pod rozwagę wynikające z nich konsekwencje dla organów ścigania i obywateli Unii Europejskiej. Należy przy tym należycie uwzględniać wpływ takich rozwiązań na ochronę prywatności i ich użyteczność dla egzekwowania prawa – najpierw przy zgłaszaniu propozycji nowych aktów prawnych i ich omawianiu, ale później także po ich wdrożeniu, za pomocą okresowych kontroli. Taka analiza jest także niezbędna przed nakreśleniem w nowym programie wieloletnim głównych inicjatyw na najbliższą przyszłość.

21. Inspektor z zadowoleniem przyjmuje fakt, że komunikat uznaje ochronę praw podstawowych, w szczególności ochronę danych osobowych, za jedną z kluczowych kwestii przyszłości przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Punkt 2 komunikatu określa UE jako wyjątkowy obszar ochrony praw podstawowych w oparciu o wspólne wartości. Dobrze stało się także, że jako priorytetowy kierunek działań – a nawet pierwszy priorytetowy kierunek działań komunikatu – wymieniono przystąpienie do Europejskiej Konwencji Praw Człowieka. Przystąpienie do konwencji jest ważnym krokiem w kierunku zapewnienia harmonijnego i spójnego systemu ochrony praw podstawowych. Nie można także zapomnieć o tym, że poczesne miejsce w komunikacie zajmuje kwestia ochrony danych.

22. W komunikacie przejawia się w tym aspekcie wyraźnie dążenie do zapewnienia ochrony praw obywateli, a tym samym do przyjęcia bardziej wyważonego podejścia. Rządy potrzebują odpowiednich narzędzi do zapewnienia bezpieczeństwa obywateli, jednak w naszym europejskim społeczeństwie muszą także zagwarantować pełne poszanowanie ich praw podstawowych. Służba obywatelom ([12]) wymaga od Unii Europejskiej stania na straży tej równowagi.

23. Zdaniem Inspektora komunikat bardzo dobrze uwzględnia potrzebę takiej równowagi, w tym konieczność ochrony danych osobowych. Uznaje on potrzebę przesunięcia punktu ciężkości. Jest to istotne, ponieważ polityka dotycząca przestrzeni wolności, bezpieczeństwa i sprawiedliwości nie powinna wspierać stopniowej przemiany naszego społeczeństwa w społeczeństwo nadzoru. Inspektor oczekuje, że Rada przyjmie takie samo podejście w programie sztokholmskim, w tym z uwzględnieniem wskazówek zawartych w pkt 25 niniejszego dokumentu.

24. Jest to tym ważniejsze, że przestrzeń wolności, bezpieczeństwa i sprawiedliwości jest przestrzenią, która „wpływa na warunki życia obywateli, w szczególności na prywatną przestrzeń ich własnej odpowiedzialności oraz bezpieczeństwa osobowego i społecznego, którą chronią prawa podstawowe", co niedawno podkreślił niemiecki Trybunał Konstytucyjny w swym orzeczeniu z dnia 30 czerwca 2009 r. nawiązującym do traktatu lizbońskiego ([13]).

([9]) Umowa PNR z 2007 r. wymieniona w poprzednim przypisie i dokumenty ją poprzedzające.

([10]) Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE, Dz.U. L 105 z 13.4.2006, s. 54. Chociaż podstawą prawną jest art. 95 Traktatu WE, taka była pierwsza reakcja na zamachy bombowe w Londynie.

([11]) 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.

([12]) Zob. tytuł komunikatu.

([13]) Komunikat prasowy Federalnego Trybunału Konstytucyjnego Niemiec nr 72/2009 z 30 czerwca 2009 r., pkt 2 lit. c).

25. Inspektor podkreśla, że w takiej przestrzeni:

— wymiana informacji między organami państw członkowskich, w tym, w odnośnych sytuacjach, organami lub bazami danych UE, powinna opierać się na odpowiednich i skutecznych mechanizmach zapewniających pełne poszanowanie praw podstawowych obywatela i wzajemne zaufanie,

— wymaga to nie tylko dostępności informacji w powiązaniu ze wzajemnym uznawaniem systemów prawnych państw członkowskich (oraz UE), ale także harmonizacji standardów ochrony informacji, na przykład, choć nie tylko, za pomocą wspólnych ram ochrony danych,

— takie wspólne standardy powinny być stosowane nie tylko w sytuacjach o wymiarze transgranicznym. Wzajemne zaufanie możliwe jest tylko wtedy, gdy takie standardy są solidne i zawsze przestrzegane, nawet wtedy, gdy transgraniczny wymiar danej sprawy nie jest lub przestaje być oczywisty. Poza tym, zwłaszcza jeśli chodzi o wykorzystanie informacji, różnice między danymi „wewnętrznymi" i „transgranicznymi" nie mogą mieć odzwierciedlenia w praktyce ([14]).

V. **INSTRUMENTY OCHRONY DANYCH**

V.1. **W stronę pełnego systemu ochrony danych**

26. Inspektor popiera strategiczne podejście, zgodnie z którym ochrona danych zajmuje w komunikacie poczesne miejsce. Wiele inicjatyw w przestrzeni wolności, bezpieczeństwa i sprawiedliwości uzależnionych jest bowiem od wykorzystania danych osobowych, a dobra ochrona danych jest kluczowa dla powodzenia tych inicjatyw. Poszanowanie prywatności i ochrona danych to nie tylko obowiązek prawny, który coraz bardziej upowszechnia się na szczeblu UE, ale także kwestia niezmiernie ważna dla obywateli UE, jak pokazują wyniki eurobarometru ([15]). Ponadto ograniczanie dostępu do danych osobowych jest niezbędne do zapewnienia zaufania ze strony organów ścigania.

27. W pkt 2.3 komunikatu jest mowa o tym, że Unia powinna przyjąć pełny system ochrony danych osobowych obejmujący wszystkie obszary, w których przysługuje jej właściwość ([16]). Inspektor w pełni wspiera te dążenia, niezależnie od wejścia w życie traktatu lizbońskiego. Zauważa on również, że taki system nie musi oznaczać, iż do przetwarzania wszystkich danych stosowane muszą być jedne i te same ramy prawne. Na mocy obowiązujących traktatów możliwości przyjęcia jednych, pełnych ram prawnych mających zastosowanie do przetwarzania wszystkich danych są ograniczone z uwagi na strukturę filarową oraz na fakt, że – przynajmniej w pierwszym filarze – ochrona danych przetwarzanych przez instytucje europejskie ma inną podstawę prawną (art. 286 Traktatu WE). Inspektor zauważa jednak, że niektóre udoskonalenia można wprowadzić poprzez pełne wykorzystanie możliwości, które dają obowiązujące traktaty, jak podkreśliła już Komisja w swoim komunikacie „Realizacja programu haskiego: przyszłe działania" ([17]). Po wejściu w życie traktatu lizbońskiego art. 16 TFUE stanowić będzie niezbędną podstawę prawną do wprowadzenia wspólnych, pełnych ram prawnych mających zastosowanie do przetwarzania wszystkich informacji.

28. Inspektor zauważa, że konieczne jest – niezależnie od okoliczności – zapewnienie spójności w ramach prawnych dotyczących ochrony danych – tam, gdzie będzie to konieczne – za pomocą harmonizacji i konsolidacji poszczególnych aktów prawnych stosowanych w przestrzeni wolności, bezpieczeństwa i sprawiedliwości.

Sytuacja w świetle obowiązujących traktatów

29. Pierwszym krokiem stało się ostatnio przyjęcie decyzji ramowej Rady 2008/977/WSiSW ([18]). Ten akt prawny nie może być jednak określony mianem pełnych ram prawnych zasadniczo dlatego, że jego przepisy nie mają zastosowania ogólnego. Nie mają zastosowania do sytuacji wewnętrznych, w których dane osobowe mają swój początek w wykorzystującym je państwie członkowskim. Takie ograniczenie z pewnością obniży wartość dodaną decyzji ramowej Rady, chyba że wszystkie państwa członkowskie zdecydują się uwzględnić sytuacje wewnętrzne w krajowych przepisach wykonawczych, co nie jest zbyt prawdopodobne.

30. Drugim powodem, dla którego Inspektor uznaje, że na dłuższą metę decyzja ramowa Rady 2008/977/WSiSW nie tworzy zadowalających ram ochrony danych w przestrzeni wolności, bezpieczeństwa i sprawiedliwości, jest to, że niektóre z jej istotnych przepisów są niezgodne z dyrektywą 95/46/WE. W świetle obowiązujących traktatów, drugim krokiem mogłoby być poszerzenie zakresu zastosowania decyzji ramowej Rady i dostosowanie jej do dyrektywy 95/46/WE.

31. Kolejnym impulsem do wprowadzenia pełnego systemu ochrony danych mogłoby się stać nakreślenie wyrazistej i długoterminowej wizji. Wizja ta mogłaby obejmować całościowe i spójne podejście do definicji gromadzenia i wymiany danych – oraz wykorzystywania istniejących baz danych – a jednocześnie zawierać gwarancje ochrony danych. Taka wizja zapobiegłaby zbędnemu nakładaniu się

([14]) Zob. również podobne zalecenia Inspektora w opinii z dnia 19 grudnia 2005 r. w sprawie wniosku dotyczącego decyzji ramowej Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (COM(2005) 475 wersja ostateczna), Dz.U. C 47 z 25.2.2006, s. 27, pkt 30–32.

([15]) Ochrona danych w Unii Europejskiej – Punkt widzenia obywateli – Sprawozdanie analityczne, Flash Eurobarometer Series 225, styczeń 2008 roku, http://www.ec.europa.eu/public_opinion/flash/fl_225_en.pdf

([16]) Zob. również priorytetowe kierunki działań nakreślone w komunikacie.

([17]) COM(2006) 331 wersja ostateczna z dnia 28 czerwca 2006 r.

([18]) Zob. przypis 11.

na siebie aktów prawnych i dublowaniu ich (co dotyczy również przetwarzania danych osobowych). Powinna ona również wspierać spójność polityki UE w tym zakresie, a także zaufanie co do sposobu przetwarzania danych obywateli przez organy publiczne. Inspektor zaleca Radzie, aby ogłosiła w programie sztokholmskim potrzebę nakreślenia takiej wyrazistej i długoterminowej wizji.

32. Kolejnym zaleceniem Inspektora jest rozpatrzenie w odpowiedniej perspektywie i ocena środków, które zostały już w tej dziedzinie przyjęte, jak również ich konkretnego wdrożenia i ich skuteczności. Taka ocena powinna w odpowiedni sposób uwzględnić wpływ na ochronę prywatności i użyteczność takich rozwiązań dla egzekwowania prawa. Jeżeli z oceny tej wynikać będzie, że niektóre środki nie przynoszą spodziewanych rezultatów lub nie są proporcjonalne do założonych celów, należy rozważyć następujące kroki:

— krokiem pierwszym powinna być zmiana lub uchylenie takich środków, o ile ich istnienia nie uzasadniają konkretne, płynące z nich korzyści dla organów ścigania i obywateli UE,

— drugim krokiem powinna być ocena możliwości usprawnienia stosowania istniejących środków,

— dopiero trzecim krokiem powinno być zaproponowanie nowych środków prawodawczych, jeżeli takie nowe środki najprawdopodobniej są potrzebne do osiągnięcia założonych celów. Nowe akty należy przyjmować tylko, jeśli przynoszą one wyraźne i konkretne korzyści organom ścigania i obywatelom UE.

Inspektor zaleca umieszczenie w programie sztokholmskim odniesienia do systemu oceny istniejących środków.

33. Nie można też zapomnieć o tym, że należy położyć szczególny nacisk na lepsze stosowanie istniejących mechanizmów ochronnych, zgodnie z komunikatem Komisji w sprawie kontynuacji programu prac na rzecz skuteczniejszego wdrażania dyrektywy o ochronie danych ([19]) oraz sugestiami Inspektora zawartymi w jego opinii dotyczącej tego komunikatu ([20]). Niestety w trzecim filarze Komisja nie ma możliwości wszczęcia postępowania w sprawie naruszenia przepisów.

Sytuacja w świetle traktatu lizbońskiego

34. Traktat lizboński otwiera możliwość wprowadzenia autentycznych, pełnych ram ochrony danych. Artykuł 16.2 Traktatu o funkcjonowaniu Unii Europejskiej wymaga, aby Rada i Parlament Europejski wprowadziły przepisy dotyczące ochrony danych przez instytucje, organy, urzędy i agencje unijne, przez państwa członkowskie wykonujące działania wchodzące w zakres zastosowania prawa unijnego oraz przez osoby prywatne.

35. Inspektor zdaje sobie sprawę, że położony w komunikacie nacisk na pełny system ochrony danych jest przejawem ambicji Komisji w zakresie przedstawienia ram prawnych mających zastosowanie do wszystkich działań związanych z przetwarzaniem danych. Inspektor w pełni popiera te ambicje, ponieważ zwiększają one spójność systemu, zapewniają pewność prawa, a co za tym idzie, także poprawiają poziom ochrony. W szczególności pozwoliłoby to w przyszłości uniknąć problemów związanych z określeniem linii podziału między poszczególnymi filarami w przypadku, gdy dane zgromadzone w sektorze prywatnym do celów komercyjnych wykorzystywane byłyby później dla potrzeb egzekwowania prawa. Ta linia podziału między filarami nie odzwierciedla w pełni rzeczywistości, jak pokazały ważne orzeczenia Trybunału Sprawiedliwości w sprawie danych dotyczących przelotu pasażera ([21]) i zatrzymania danych ([22]).

36. Inspektor sugeruje podkreślenie w programie sztokholmskim tego uzasadnienia dla wprowadzenia pełnego systemu ochrony danych. Pokazuje ono, że taki system nie jest zwykłym kaprysem, ale koniecznością z uwagi na zmiany w praktykach wykorzystania danych. Inspektor zaleca uwzględnienie jako priorytetu w programie sztokholmskim potrzeby nowych ram prawnych, które zastąpiłyby m.in. decyzję ramową Rady 2008/977/WSiSW.

37. Inspektor podkreśla, że koncepcja pełnego systemu ochrony danych opartego na ogólnych ramach prawnych nie wyklucza przyjęcia dodatkowych przepisów regulujących ochronę danych w policji i sądownictwie. Takie dodatkowe przepisy mogłyby uwzględniać konkretne potrzeby egzekwowania prawa przewidziane w Deklaracji 21 dołączonej do traktatu lizbońskiego ([23]).

V.2. **Powtórzenie zasad ochrony danych**

38. W komunikacie zwraca się uwagę na postęp techniczny, który wpływa na zmianę form komunikacji między osobami prywatnymi a organizacjami publicznymi i prywatnymi. Zdaniem Komisji taki stan rzeczy wymaga powtórzenia szeregu podstawowych zasad ochrony danych.

([19]) COM(2007) 87 wersja ostateczna z dnia 7 marca 2007 r.

([20]) Opinia z dnia 25 lipca 2007 r., Dz.U. C 255 z 27.10.2007, s. 1, w szczególności pkt 30.

([21]) Orzeczenie Trybunału z dnia 30 maja 2006 r., Parlament Europejski przeciwko Radzie Unii Europejskiej (C-317/04) i Komisji Wspólnot Europejskich (C-318/04), sprawy połączone C-317/04 i C-318/04, Zb.Orz. 2006, s. I-4721.

([22]) Orzeczenie Trybunału z dnia 10 lutego 2009 r., Irlandia przeciwko Parlamentowi Europejskiemu i Radzie Unii Europejskiej, sprawa C-301/06, jeszcze nieopublikowane.

([23]) Zob. Deklaracja 21 w sprawie ochrony danych osobowych w dziedzinie współpracy sądowej w sprawach karnych i współpracy policyjnej dołączona do Aktu końcowego konferencji międzyrządowej, która przyjęła Traktat z Lizbony, Dz.U. C 115 z 9.5.2008, s. 345.

39. Inspektor z zadowoleniem przyjmuje ten zamiar wyrażony przez Komisję. W perspektywie zmian technologicznych ocena skuteczności takich zasad jest niezwykle przydatna. Na wstępie należy zauważyć, że powtórzenie i potwierdzenie zasad ochrony danych nie zawsze musi bezpośrednio wiązać się z rozwojem techniki. Takie powtórzenie i potwierdzenie może być też wymagane w świetle innych perspektyw wymienionych w części III powyżej, w związku z internacjonalizacją, wzrostem wykorzystania danych do celów egzekwowania prawa i swobodą przemieszczania się.

40. Ponadto, zdaniem Inspektora, taka ocena może być częścią konsultacji publicznych ogłoszonych przez Komisję na konferencji „Dane osobowe – częstsze wykorzystanie, lepsza ochrona?", która odbyła się w dniach 19 i 20 maja 2009 r. Takie konsultacje publiczne mogłyby dostarczyć cennych informacji ([24]). Inspektor sugeruje, aby Rada w programie sztokholmskim i Komisja w swych oświadczeniach publicznych dotyczących tych konsultacji podkreśliły powiązanie między zamiarami wyrażonymi w pkt 2.3 komunikatu a konsultacjami publicznymi w sprawie przyszłości ochrony danych.

41. Wspomniana ocena mogłaby na przykład zawierać następujące elementy:

— dane osobowe dotyczące przestrzeni wolności, bezpieczeństwa i sprawiedliwości to najprawdopodobniej dane szczególnie poufne, takie jak dane dotyczące wyroków skazujących w sprawach karnych, dane policyjne i dane biometryczne, takie jak odciski palców i profile DNA,

— ich przetwarzanie może wiązać się z negatywnymi konsekwencjami dla osób, których dane dotyczą, szczególnie biorąc pod uwagę środki przymusu, którymi dysponują organy ścigania. Ponadto monitorowanie i analiza danych podlega w coraz większym stopniu automatyzacji i dosyć często odbywa się bez udziału człowieka. Technologia pozwala na wykorzystanie baz danych osobowych do przeprowadzania wyszukiwań o charakterze ogólnym (eksploracja danych, profilowanie itp.). Należy wyraźnie określić obowiązki prawne, którym podlega przetwarzanie danych,

— podstawą prawa o ochronie danych jest to, że dane osobowe gromadzone są do określonych celów i nie są wykorzystywane w sposób niezgodny z tymi celami. Wykorzystanie danych w sposób niezgodny z określonymi celami powinno być dozwolone wyłącznie w zakresie przewidzianym przez prawo i w przypadku konieczności ochrony określonych interesów publicznych, takich jak te wymienione w art. 8.2 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności,

— konieczność poszanowania zasady ograniczenia celu może mieć wpływ na aktualne tendencje w wykorzystaniu danych. Organy ścigania korzystają z danych zgromadzonych do celów komercyjnych przez przedsiębiorstwa prywatne w sektorze telekomunikacyjnym, transportowym i finansowym. Ponadto budowane są wielkoskalowe systemy informatyczne, na przykład dla potrzeb imigracji i kontroli granic. Co więcej, dopuszczalne jest tworzenie powiązań między różnymi bazami danych i umożliwianie wzajemnego dostępu do nich, co zwiększa zakres zastosowań danych w porównaniu z celami, do jakich te dane pierwotnie zgromadzono. Konieczna jest refleksja nad tymi aktualnymi tendencjami, która w razie potrzeby powinna uwzględniać ewentualne korekty lub dodatkowe zabezpieczenia,

— oprócz zasad ochrony danych wymienionych w komunikacie, w omawianej ocenie należy zwrócić uwagę na potrzebę przejrzystości procesów przetwarzania danych, tak aby osoby, których dane dotyczą, mogły wykorzystywać przysługujące im prawa. Przejrzystość to szczególnie trudne zagadnienie, jeśli chodzi o egzekwowanie prawa, zwłaszcza dlatego, że kwestię przejrzystości należy tu przeciwstawić zagrożeniom, które wiążą się z dochodzeniami,

— należy opracować rozwiązania w zakresie wymiany danych z państwami trzecimi.

42. Omawiana ocena powinna również koncentrować się na możliwościach poprawy skuteczności zastosowania zasad ochrony danych. W związku z tym wskazane mogłoby być zwrócenie się ku aktom, które pozwalają na rozszerzenie zakresu odpowiedzialności administratorów danych. Akty takie musiałyby przewidywać pełną odpowiedzialność administratorów danych za zarządzanie danymi. Przydatnym terminem w tym kontekście jest „opieka nad danymi". Obejmuje on wszystkie środki prawne, techniczne i organizacyjne stosowane przez organizacje w celu zapewnienia pełnej odpowiedzialności za przetwarzanie danych, takie jak planowanie i kontrola, wykorzystanie racjonalnych technologii, odpowiednie szkolenie personelu, kontrole zgodności z przepisami itp.

V.3. **Technologie niezagrażające prywatności**

43. Inspektor z zadowoleniem przyjmuje fakt, że w pkt 2.3 komunikatu poruszona została kwestia certyfikatów dotyczących prywatności. Oprócz tego można by dodać wzmiankę o „domyślnej ochronie prywatności" i konieczności określenia „najlepszych dostępnych technik" zgodnych z ramami ochrony danych w UE.

44. Zdaniem Inspektora „domyślna ochrona prywatności" i technologie niezagrażające prywatności mogłyby być pomocne w zapewnieniu lepszej ochrony i bardziej efektywnego wykorzystania informacji. Inspektor proponuje dwa kierunki dalszych działań, które mogą być zastosowane wspólnie:

— system certyfikatów w zakresie ochrony prywatności i danych osobowych ([25]) jako opcja dla twórców i użytkowników systemów informatycznych, ewentualnie finansowany ze środków UE lub wspierany przepisami unijnymi,

([24]) Grupa Robocza ds. Ochrony Danych powołana na mocy art. 29, w której pracach Inspektor uczestniczy, postanowiła intensywnie dążyć do wniesienia swego wkładu w te konsultacje publiczne.

([25]) Przykładem takiego systemu jest europejski system etykiet prywatności (EuroPriSe).

— obowiązek prawny dotyczący twórców systemów informatycznych i użytkowników takich systemów, przewidujący korzystanie z systemów zgodnych z zasadą domyślnej prywatności. Może to wymagać rozszerzenia aktualnego zakresu zastosowania prawa o ochronie danych, tak aby twórcy systemów informatycznych byli odpowiedzialni za swoje produkty ([26]).

Inspektor sugeruje zamieszczenie w programie sztokholmskim wzmianki o tych kierunkach dalszych działań.

V.4. **Aspekty zewnętrzne**

45. Kolejną kwestią poruszoną w komunikacie jest wypracowanie i propagowanie międzynarodowych standardów ochrony danych. Obecnie podejmuje się wiele działań w celu ustanowienia realistycznych standardów o zastosowaniu globalnym, na przykład na Międzynarodowej Konferencji Komisarzy ds. Ochrony Danych i Prywatności. W najbliższej przyszłości może to zaowocować porozumieniem międzynarodowym. Inspektor sugeruje, aby w programie sztokholmskim wyrażono poparcie dla takich działań.

46. W komunikacie pojawia się też wzmianka o zawarciu umów dwustronnych dzięki postępom poczynionym w pracach z USA. Inspektor zgadza się, że potrzebne są przejrzyste ramy prawne umożliwiające przekazywanie danych państwom trzecim, z zadowoleniem przyjął więc współpracę organów UE i USA w grupie kontaktowej wysokiego szczebla zmierzającą do wprowadzenia ewentualnego transatlantyckiego rozwiązania prawnego w zakresie ochrony danych, zwrócił jednak uwagę na konieczność doprecyzowania niektórych kwestii i położenia na nie większego nacisku ([27]). W związku z tym interesujące wydają się również koncepcje sformułowane w sprawozdaniu dotyczącym spraw wewnętrznych w sprawie euro-atlantyckiej przestrzeni współpracy w dziedzinie wolności, bezpieczeństwa i sprawiedliwości; zgodnie z tym sprawozdaniem decyzję dotyczącą takiej przestrzeni UE powinna podjąć do 2014 roku. Taka przestrzeń nie mogłaby powstać bez odpowiednich gwarancji dotyczących ochrony danych.

47. Według Inspektora europejskie standardy ochrony danych oparte na Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych ([28]) oraz na orzecznictwie Europejskiego Trybunału Sprawiedliwości i Europejskiego Trybunału Praw Człowieka powinny określać poziom ochrony przewidziany w ogólnym porozumieniu z USA w sprawie ochrony i wymiany danych. Takie ogólne porozumienie mogłoby stać się podstawą do konkretnych ustaleń w kwestii wymiany danych osobowych. Jest to tym ważniejsze, że zgodnie z zamiarem wyrażonym w pkt 4.2.1 komunikatu Unia Europejska powinna w razie potrzeby zawierać umowy o współpracy policyjnej.

48. Inspektor doskonale rozumie potrzebę zacieśnienia współpracy międzynarodowej, w niektórych przypadkach również z państwami niezapewniającymi ochrony praw podstawowych. Jednakże ([29]) należy zwrócić uwagę na to, że taka współpraca międzynarodowa doprowadzi prawdopodobnie do znacznego wzrostu ilości danych gromadzonych i przekazywanych międzynarodowo. Dlatego też jest niezwykle ważne, aby zasady uczciwego i zgodnego z prawem przetwarzania – oraz generalnie zasady należytego przetwarzania – miały zastosowanie do gromadzenia i przekazywania danych osobowych za granice UE oraz aby dane osobowe były przekazywane państwom trzecim lub organizacjom międzynarodowym tylko wówczas, gdy te państwa trzecie zagwarantują odpowiedni poziom ochrony lub odpowiednie zabezpieczenia.

49. Podsumowując, Inspektor zaleca, aby w programie sztokholmskim podkreślono, jak istotne jest zawarcie ze Stanami Zjednoczonymi i innymi państwami trzecimi ogólnego porozumienia w sprawie ochrony i wymiany danych gwarantującego poziom ochrony zapewniony na terytorium UE. W szerszym ujęciu Inspektor wskazuje na to, jak ważne w relacjach z państwami trzecimi i organizacjami międzynarodowymi jest aktywne propagowanie poszanowania praw podstawowych, a w szczególności ochrony danych ([30]). Ponadto w programie sztokholmskim mogłaby znaleźć się ogólna wzmianka o tym, że wymiana danych osobowych z państwami trzecimi wymaga istnienia w tych państwach trzecich odpowiedniego poziomu ochrony lub innych właściwych zabezpieczeń.

VI. **WYKORZYSTANIE INFORMACJI**

VI.1. **W stronę europejskiego modelu informacji**

50. Poprawa wymiany informacji to podstawowy cel polityki Unii Europejskiej w przestrzeni wolności, bezpieczeństwa i sprawiedliwości. W punkcie 4.1.2 komunikatu autorzy podkreślają, że bezpieczeństwo w Unii Europejskiej zależy od skutecznych mechanizmów wymiany informacji między organami krajowymi a innymi podmiotami europejskimi. Ten nacisk na wymianę informacji jest logiczny z uwagi

([26]) Użytkownicy danych objęci są prawem o ochronie danych, tak jak administratorzy danych bądź osoby przetwarzające dane.

([27]) Zob. opinia Inspektora z dnia 11 listopada 2008 r. 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.

([28]) ETS nr 108 z 28.1.1981.

([29]) Zob. pismo Inspektora z dnia 28 listopada 2005 r. w sprawie komunikatu Komisji dotyczącego zewnętrznego wymiaru przestrzeni wolności, bezpieczeństwa i sprawiedliwości, które dostępne jest na stronie Inspektora.

([30]) Ostatnie orzecznictwo dotyczące wykazów terrorystów potwierdza potrzebę wprowadzenia odpowiednich gwarancji – także w relacjach z ONZ – tak aby zapewnić, że środki przeciwdziałające terroryzmowi są zgodne ze standardami UE w zakresie praw podstawowych (sprawy połączone C-402/05 P i C-415/05 P, Kadi i Fundacja Al Barakaat przeciwko Radzie, orzeczenie z dnia 3 września 2008 r., jeszcze nieopublikowane).

na brak policji europejskiej, europejskiego systemu sądownictwa w sprawach karnych i kontroli na granicach wewnętrznych UE. Środki dotyczące informacji stanowią zatem niezbędny wkład Unii Europejskiej umożliwiający organom państw członkowskim skuteczne radzenie sobie z przestępczością transgraniczną i skuteczną ochronę granic zewnętrznych. Jednakże środki te przyczyniają się nie tylko do bezpieczeństwa obywateli, ale także do ich wolności – wspomniano już tutaj wcześniej o swobodnym przemieszczaniu się osób jako jednej z perspektyw niniejszej opinii – i sprawiedliwości.

51. Właśnie z tych względów wprowadzono w programie haskim zasadę dostępności. Zakłada ona, że informacje potrzebne do walki z przestępczością powinny być przekazywane ponad granicami wewnętrznymi UE bez utrudnień. Ostatnie doświadczenia pokazują, że trudno było zastosować tę zasadę w środkach ustawodawczych. Wniosek Komisji dotyczący decyzji ramowej Rady w sprawie wymiany informacji w ramach zasady dostępności z dnia 12 października 2005 r. ([31]) nie został przez Radę zaakceptowany. Państwa członkowskie nie były przygotowane na pogodzenie się ze wszystkimi następstwami stosowania zasady dostępności. Zamiast tego wprowadzono bardziej ograniczone akty ([32]), takie jak decyzja Rady 2008/615/WSiSW z dnia 23 czerwca 2008 r. w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej (decyzja z Prüm) ([33]).

52. Chociaż zasada dostępności była kluczowym elementem programu haskiego, Komisja wydaje się teraz zajmować bardziej umiarkowane stanowisko. Przewiduje dalsze pobudzenie wymiany informacji między organami państw członkowskich poprzez wprowadzenie europejskiego modelu informacji. Szwedzka prezydencja UE zgadza się z tym tokiem myślenia ([34]). Przedstawi propozycję strategii wymiany informacji. Rada rozpoczęła już pracę nad ambitnym przedsięwzięciem polegającym na stworzeniu strategii Unii Europejskiej w zakresie zarządzania informacjami, która ściśle wiąże się z europejskim modelem informacji. Inspektor przyjmuje te wydarzenia z wielkim zainteresowaniem i podkreśla, że w przedsięwzięciach tych należy zwrócić należytą uwagę na elementy z zakresu ochrony danych.

Europejski model informacji i ochrony danych

53. Na wstępie należy podkreślić, że przyszłość przestrzeni wolności, bezpieczeństwa i sprawiedliwości nie powinna być uzależniona od technologii, co oznacza, że niemal nieograniczone możliwości, które dają nowe technologie, powinny być zawsze sprawdzane pod kątem odnośnych zasad ochrony danych i wykorzystywane tylko wtedy, jeśli będą zgodne z tymi zasadami.

54. Inspektor zauważa, że w komunikacie model informacji przedstawiony został nie tylko jako model techniczny: posiada on zaawansowane zdolności analizy strategicznej oraz umożliwia usprawnione gromadzenie i przetwarzanie informacji operacyjnych. Wynika z niego również, że należy brać pod uwagę aspekty dotyczące polityki, takie jak kryteria gromadzenia, wymiany i przetwarzania informacji, a jednocześnie przestrzegać zasad ochrony danych.

55. Kluczowe są – i nadal takimi pozostaną – technologia informatyczna i uwarunkowania prawne. Inspektor z zadowoleniem przyjmuje fakt, że komunikat rozpoczyna się od założenia, zgodnie z którym europejski model informacji nie może być postrzegany przez pryzmat kwestii technicznych. Informacje powinny być gromadzone, wymieniane i przetwarzane wyłącznie na podstawie konkretnych potrzeb w zakresie bezpieczeństwa i z uwzględnieniem zasad ochrony danych. Inspektor w pełni zgadza się z potrzebą opracowania mechanizmu późniejszej oceny funkcjonowania wymiany informacji. Sugeruje, aby Rada dodatkowo rozwinęła te kwestie w programie sztokholmskim.

56. W związku z tym Inspektor podkreśla, że ochrona danych, która ma za zadanie ochronę obywatela, nie powinna być postrzegana jako przeszkoda w skutecznym zarządzaniu danymi. Dostarcza ona pomocnych narzędzi pozwalających na usprawnienie przechowywania i wymiany danych oraz dostępu do nich. Prawa osób, których dane dotyczą, do dostępu do informacji o tym, które spośród ich danych są przetwarzane, oraz do poprawiania informacji nieprawidłowych mogą również doprowadzić do poprawy dokładności danych w systemach zarządzania danymi.

57. Prawo o ochronie danych zasadniczo rodzi następujące skutki: jeśli dane są potrzebne do konkretnego i zgodnego z prawem celu, ich wykorzystanie jest dozwolone; jeżeli dane osobowe nie są potrzebne do ściśle określonego celu, nie powinny być wykorzystywane. W tym pierwszym przypadku do zapewnienia odpowiednich zabezpieczeń mogą być potrzebne dodatkowe środki.

58. Inspektor krytycznie podchodzi jednak do zawartej w komunikacie wzmianki o „określaniu przyszłych potrzeb", które ma być częścią modelu informacji. Podkreśla, że również w przyszłości zasada ograniczenia celu powinna być naczelną zasadą stosowaną przy budowaniu systemów informatycznych ([35]). Jest to jedna z najważniejszych gwarancji, którą system ochrony danych daje obywatelowi: musi on wiedzieć zawczasu, do jakich celów przetwarzane są dane go dotyczące, i mieć pewność, że będą one wykorzystywane wyłącznie do tego celu, szczególnie w przyszłości. Ta gwarancja jest nawet sformułowana w art. 8 Karty praw podstawowych Unii Europejskiej. Zasada ograniczenia celu dopuszcza wyjątki – dotyczą one w szczególności przestrzeni wolności, bezpieczeństwa i sprawiedliwości – ale takie wyjątki nie powinny stanowić o konstrukcji systemu.

([31]) COM(2005) 490 wersja ostateczna.

([32]) Z punktu widzenia dostępności; decyzja z Prüm zawiera dalej idące przepisy w zakresie wykorzystania danych biometrycznych (DNA i odcisków palców).

([33]) Dz.U. L 210 z 6.8.2008, s. 1.

([34]) Zob. Rządowy program prac UE, o którym mowa w przypisie 5, s. 23.

([35]) Zob. też punkt 41 powyżej.

Wybór odpowiedniej architektury

59. Pierwszym krokiem jest wybór odpowiedniej architektury wymiany informacji. W komunikacie podkreśla się znaczenie odpowiedniej architektury systemów informacyjnych (pkt 4.1.3), jednak niestety tylko w kontekście interoperacyjności.

60. Inspektor podkreśla natomiast inny aspekt: w europejskim modelu informacji wymogi w zakresie ochrony danych powinny być integralną częścią wszystkich prac nad budową systemu i nie powinny być postrzegane wyłącznie jako warunek zapewnienia zgodności systemu z prawem ([36]). Należy wykorzystywać koncepcję „domyślnej ochrony prywatności" i zwrócić uwagę na potrzebę określenia „najlepszych dostępnych technik" ([37]), o których mowa w pkt 43 powyżej. Europejski model informacji powinien być rozwinięciem tych koncepcji. Oznacza to konkretnie, że systemy informatyczne służące zapewnieniu bezpieczeństwa publicznego powinny być zawsze tworzone zgodnie z zasadą „domyślnej ochrony prywatności". Inspektor zaleca, aby Rada uwzględniła te kwestie w programie sztokholmskim.

Interoperacyjność systemów

61. Inspektor podkreśla, że interoperacyjność nie jest wyłącznie kwestią techniczną, ale ma też wpływ na ochronę obywatela, w szczególności na ochronę danych. Z perspektywy ochrony danych, interoperacyjność systemów, jeżeli zostanie sprawnie wdrożona, ma oczywistą zaletę, a mianowicie pozwala na uniknięcie dublowania przechowywania danych. Jednakże oczywistym jest także, że tworzenie możliwości technicznych dostępu do danych albo ich wymiany jest w wielu przypadkach silnym bodźcem do faktycznego uzyskiwania dostępu do takich danych lub ich wymiany. Innymi słowy, interoperacyjność wiąże się z określonymi zagrożeniami dotyczącymi powiązań wzajemnych między bazami danych przeznaczonymi do różnych celów ([38]). Może to wpłynąć na ścisłe ograniczenie celu baz danych.

62. Krótko mówiąc, sam fakt, że wymiana informacji cyfrowych między interoperacyjnymi bazami danych lub łączenie takich baz danych jest technicznie możliwe, nie uzasadnia wprowadzenia odstępstwa od zasady ograniczenia celu. Interoperacyjność powinna być w konkretnych przypadkach uzależniona od jednoznacznych i rozważnych decyzji politycznych. Inspektor sugeruje, aby kwestia ta została rozwinięta w programie sztokholmskim.

([36]) Zob. „Wytyczne i kryteria dotyczące tworzenia, wdrażania i stosowania technologii bezpieczeństwa zwiększających ochronę prywatności" opracowane w ramach projektu PRISE (http://www.prise.oeaw.ac.at).

([37]) Najlepsze dostępne techniki oznaczają najbardziej efektywny i zaawansowany etap rozwoju działań i sposobów ich wdrażania, które wskazują na praktyczną przydatność określonych technik, tak aby takie techniki mogły zasadniczo stanowić podstawę do zapewnienia zgodności aplikacji i systemów informatycznych z wymogami ram regulacyjnych UE w dziedzinie prywatności, ochrony danych i bezpieczeństwa.

([38]) Patrz uwagi Inspektora w sprawie komunikatu Komisji dotyczącego interoperacyjności europejskich baz danych z dnia 10 marca 2006 r., które dostępne są pod adresem internetowym: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf

VI.2. **Wykorzystywanie informacji gromadzonych do innych celów**

63. Komunikat nie nawiązuje w sposób wyraźny do jednej z najważniejszych tendencji ostatnich lat, a mianowicie do wykorzystywania na potrzeby egzekwowania prawa danych gromadzonych do celów komercyjnych w sektorze prywatnym. Tendencja ta charakteryzuje nie tylko dane dotyczące ruchu w sieciach elektronicznej wymiany informacji czy dane pasażerów podróżujących samolotem do (określonych) państw trzecich ([39]), ale jest obecna także w sektorze finansowym. Przykładem jest tu dyrektywa 2005/60/WE Parlamentu Europejskiego i Rady z dnia 26 października 2005 r. w sprawie przeciwdziałania korzystaniu z systemu finansowego w celu prania pieniędzy oraz finansowania terroryzmu ([40]). Kolejny znany i będący przedmiotem częstych dyskusji przykład dotyczy przetwarzania – przez Stowarzyszenie Międzynarodowej Teletransmisji Danych Finansowych (SWIFT) ([41]) – danych osobowych wykorzystywanych dla potrzeb programu śledzenia środków finansowych należących do terrorystów wdrażanego przez amerykański Departament Skarbu.

64. Inspektor uznaje, że takie tendencje zasługują na szczególną uwagę w programie sztokholmskim. Mogą być one uznawane za odstępstwa od zasady ograniczenia celu i często stanowią poważne naruszenie prywatności, ponieważ wykorzystywanie takich danych może dostarczyć wielu informacji o zachowaniu osób, których te dane dotyczą. W przypadku proponowania takich środków konieczne są zawsze bardzo mocne dowody uzasadniające konieczność wprowadzenia tak inwazyjnych rozwiązań. Jeżeli takie dowody zostaną przedstawione, należy zapewnić pełną ochronę praw jednostek.

65. Zdaniem Inspektora wykorzystywanie na potrzeby egzekwowania prawa danych osobowych gromadzonych do celów handlowych powinno być dopuszczalne wyłącznie po spełnieniu następujących, surowych warunków:

— dane są wykorzystywane do ściśle określonych celów, takich jak walka z terroryzmem lub poważną przestępczością, przy czym ocena spełnienia tego warunku powinna być przeprowadzana dla każdego przypadku osobno,

— dane powinny być przekazywane metodą „dostarczania", a nie metodą „pobierania" ([42]),

([39]) Zob. np. pkt 15 powyżej.

([40]) Dz.U. L 309 z 25.11.2005, s. 15.

([41]) Zob. opinia 10/2006 Grupy Roboczej ds. Ochrony Danych powołanej na mocy art. 29, na temat przetwarzania danych osobowych przez Stowarzyszenie Międzynarodowej Teletransmisji Danych Finansowych (SWIFT).

([42]) Metoda „dostarczania" polega na tym, że administrator wysyła („dostarcza") dane na żądanie organu ścigania. Metoda „pobierania" zakłada, że organ ścigania posiada dostęp do bazy danych administratora i sam pozyskuje („pobiera") z niej dane. Metoda „pobierania" sprawia, że administratorowi danych trudniej jest odpowiadać za dane.

— żądania dotyczące danych powinny być proporcjonalne, konkretnie ukierunkowane i zasadniczo oparte na podejrzeniach dotyczących określonych osób,

— należy unikać rutynowego wyszukiwania, eksploracji danych i profilowania,

— wszystkie przypadki wykorzystania danych dla potrzeb egzekwowania prawa należy rejestrować w celu umożliwienia skutecznej kontroli takiego wykorzystywania przez osobę, której dane dotyczą, w ramach wykonywania przysługujących jej praw, przez organy zajmujące się ochroną danych i przez system sądownictwa.

VI.3. **Systemy informatyczne i organy UE**

Systemy informatyczne z pamięcią scentralizowaną i bez takiej pamięci ([43])

66. W ostatnich latach znacznie zwiększyła się w przestrzeni wolności, bezpieczeństwa i sprawiedliwości liczba systemów informatycznych opartych na przepisach UE. Niekiedy podejmowane są decyzje o stworzeniu systemu opartego na scentralizowanym przechowywaniu danych na szczeblu europejskim, w innych przypadkach prawo przewiduje jedynie wymianę informacji między krajowymi bazami danych. System informacyjny Schengen jest przypuszczalnie najlepszym przykładem systemu o pamięci scentralizowanej. Decyzja Rady 2008/615/WSiSW (decyzja z Prüm) ([44]) jest z perspektywy ochrony danych najważniejszym przykładem ustanowienia systemu bez pamięci scentralizowanej, ponieważ przewiduje masową wymianę danych biometrycznych między organami państw członkowskich.

67. Komunikat pokazuje, że ta tendencja w tworzeniu nowych systemów będzie trwać dalej. Pierwszy przykład, widoczny w pkt 4.2.2, to system informatyczny rozszerzający zastosowanie europejskiego systemu przekazywania informacji z rejestrów karnych (ECRIS) na obywateli państw spoza UE. Komisja zleciła już badania nad europejskim wykazem obywateli państw trzecich skazanych prawomocnym wyrokiem sądu (EICTCN), co może doprowadzić do powstania scentralizowanej bazy danych. Drugim przykładem jest wymiana danych osób figurujących w rejestrach niewypłacalności w innych państwach członkowskich w ramach e-sprawiedliwości (pkt 3.4.1 komunikatu), bez użycia scentralizowanej pamięci.

68. System zdecentralizowany miałby pewną przewagę z punktu widzenia ochrony danych. Pozwala bowiem na uniknięcie dublowania przechowywania danych – zarówno przez organ państwa członkowskiego, jak i w systemie scentralizowanym; odpowiedzialność za dane jest jasno określona, bo organ państwa członkowskiego jest administratorem, a kontrola sprawowana przez system sądowniczy i przez organy zajmujące się ochroną danych może odbywać się na szczeblu państwa członkowskiego. Jednak system ten ma również słabe punkty związane z wymianą danych z innymi jurysdykcjami, co dotyczy na przykład zapewnienia, że przechowywane informacje są aktualne zarówno w państwie ich pochodzenia, jak i w państwie docelowym, oraz kwestii zagwarantowania skutecznej kontroli po obu stronach. Jeszcze bardziej złożoną kwestią jest określenie odpowiedzialności za system techniczny służący do wymiany danych. Te niedociągnięcia można wyeliminować, decydując się na to, aby przynajmniej część systemu (np. infrastruktura techniczna) miała formę systemu scentralizowanego, za który odpowiadać będą organy UE.

69. W tym kontekście przydatne byłoby opracowanie merytorycznych kryteriów wyboru między systemem scentralizowanym i zdecentralizowanym, które pozwoliłyby na dokonywanie jednoznacznych i rozważnych decyzji politycznych w konkretnych przypadkach. Te kryteria mogą mieć wpływ na funkcjonowanie samych systemów, ale także na ochronę danych obywateli. Inspektor sugeruje umieszczenie w programie sztokholmskim wzmianki o zamiarze stworzenia takich kryteriów.

Wielkoskalowe systemy informatyczne

70. W pkt 4.2.3.2 komunikatu znajduje się krótkie omówienie przyszłości wielkoskalowych systemów informatycznych ze szczególnym uwzględnieniem systemu informacyjnego Schengen (SIS) i wizowego systemu informacyjnego (VIS).

71. W pkt 4.2.3.2 znajduje się również wzmianka o utworzeniu systemu elektronicznej rejestracji wjazdu na terytorium państw członkowskich i wyjazdu z niego oraz programu rejestrowania podróżnych. System ten był wcześniej zapowiadany przez Komisję w ramach „pakietu kontroli granic" z inicjatywy wiceprzewodniczącego Frattiniego ([45]). W swych początkowych uwagach ([46]) Inspektor wyrażał się dość krytycznie o tej propozycji, ponieważ nie wykazano w dostateczny sposób konieczności utworzenia tak inwazyjnego systemu, zwłaszcza że istnieją już inne systemy wielkoskalowe. Inspektor nie dostrzega żadnych dodatkowych argumentów przemawiających za potrzebą wprowadzenia takiego systemu i sugeruje Radzie, aby w programie sztokholmskim tę kwestię pominęła.

72. W związku z tym Inspektor pragnie odwołać się do swoich opinii dotyczących różnych inicjatyw z dziedziny wymiany informacji w UE ([47]), w których zawarł szereg sugestii i uwag dotyczących wpływu, jaki na ochronę danych będzie miało wykorzystanie dużych baz danych na

([43]) Pamięć scentralizowana w tym kontekście rozumiana jest jako pamięć centralna na szczeblu europejskim, natomiast pamięć zdecentralizowana to pamięć przechowywana na szczeblu państw członkowskich.

([44]) Zob. przypis 33.

([45]) Komunikat Komisji „Przygotowanie kolejnych etapów rozwoju zarządzania granicami w Unii Europejskiej" z 13.2.2008, COM(2008), s. 69.

([46]) Wstępne uwagi Inspektora z dnia 3 marca 2008 r. dotyczące trzech komunikatów Komisji w sprawie zarządzania granicami (COM(2008) 69, COM(2008) 68 i COM(2008) 67): http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf

([47]) W szczególności: Opinia z dnia 23 marca 2005 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie Systemu Informacji Wizowej (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych, Dz.U. C 181 z 23.7.2005, s. 13 i opinia z dnia 19 października 2005 r. w sprawie trzech wniosków dotyczących systemu informacyjnego Schengen drugiej generacji (SIS II), Dz.U. C 91 z 19.4.2006, s. 38.

szczeblu UE. Szczególną uwagę zwrócił między innymi na potrzebę wprowadzenia silnych i odpowiednio dostosowanych zabezpieczeń, jak również na proporcjonalność i konieczność przeprowadzania ocen wpływu przed zaproponowaniem lub podjęciem jakichkolwiek środków w tym zakresie. Inspektor zawsze bronił odpowiedniej i zgodnej z wymogami ochrony danych równowagi między wymogami bezpieczeństwa i ochroną prywatności osób ujętych w systemach. To samo stanowisko zajął, występując w charakterze nadzorcy centralnych elementów systemu.

73. Ponadto Inspektor pragnie skorzystać z okazji, aby podkreślić potrzebę przyjęcia spójnego podejścia do wymiany informacji w UE całościowo w zakresie spójności prawnej, technicznej i nadzorczej między systemami już istniejącymi a tymi, które dopiero powstaną. Teraz jeszcze wyraźniej potrzebna jest odważna i całościowa wizja wymiany informacji w UE i przyszłości wielkoskalowych systemów informatycznych. Utworzenie systemu elektronicznej rejestracji wjazdu na terytorium państw członkowskich i wyjazdu z niego można by ponownie rozważyć wyłącznie w oparciu o taką wizję.

74. Inspektor sugeruje umieszczenie w programie sztokholmskim wzmianki o zamiarze stworzenia takiej wizji, co mogłoby obejmować refleksję dotyczącą ewentualnego wejścia w życie traktatu lizbońskiego i konsekwencje tego dla systemów opierających się na pierwszym i trzecim filarze.

75. Ponadto w komunikacie znajduje się informacja o powołaniu nowej agencji, która według komunikatu powinna być organem właściwym do obsługi systemu elektronicznej rejestracji wjazdu i wyjazdu. Komisja zaproponowała w międzyczasie utworzenie takiej agencji ([48]). Inspektor popiera ten wniosek co do zasady, ponieważ może on usprawnić działanie tych systemów, w tym ochrony danych. Przedstawi w odpowiednim terminie opinię dotyczącą tego wniosku.

Europol i Eurojust

76. W komunikacie kilkakrotnie pojawiają się wzmianki o roli Europolu i podkreśla się, że priorytetem jest odgrywanie przez Europol głównej roli w koordynacji, wymianie informacji i szkoleniu pracowników. Również w ust. 4.2.2 komunikatu mowa jest o najnowszych zmianach w ramach prawnych współpracy Eurojustu i Europolu oraz pojawia się informacja o tym, że nadal prowadzone będą prace w kierunku wzmocnienia Eurojustu, szczególnie pod względem prowadzenia dochodzeń w sprawach dotyczących transgranicznej przestępczości zorganizowanej. Inspektor w pełni popiera te cele z zastrzeżeniem odpowiedniego poszanowania mechanizmów ochrony danych.

77. W związku z tym Inspektor z zadowoleniem przyjmuje nowy projekt umowy wypracowany niedawno przez Europol i Eurojust ([49]) i mający na celu usprawnienie i rozszerzenie współpracy między tymi dwoma organami oraz zapewnienie wydajnej wymiany informacji między nimi. W tym przedsięwzięciu wydajna i skuteczna ochrona danych odgrywa kluczową rolę.

VI.4. **Wykorzystanie danych biometrycznych**

78. Inspektor zauważa, że komunikat nie porusza kwestii coraz częstszego wykorzystywania danych biometrycznych w różnych aktach prawnych Unii Europejskiej dotyczących wykorzystania wymiany danych, w tym w aktach ustanawiających wielkoskalowe systemy informatyczne. Jest to godne ubolewania ze względu na szczególną wagę i delikatny charakter tej sprawy w kontekście ochrony danych i prywatności.

79. Chociaż Inspektor uznaje ogólne zalety wykorzystania danych biometrycznych, wciąż podkreśla, jak duży wpływ ma wykorzystanie takich danych na prawa jednostki i sugeruje wprowadzenie rygorystycznych zabezpieczeń w zakresie wykorzystania danych biometrycznych w poszczególnych systemach. Najnowsze orzeczenie Europejskiego Trybunału Praw Człowieka w sprawie *S. i Marper przeciwko Zjednoczonemu Królestwu* ([50]) zawiera cenne wskazówki w tym zakresie, szczególnie w kwestii uzasadnienia i granic wykorzystania danych biometrycznych. Dane dotyczące DNA mogą w szczególności pozwolić na ujawnienie chronionych informacji dotyczących danej osoby, zwłaszcza że możliwości techniczne pozyskiwania informacji z kodu DNA wciąż się zwiększają. W przypadku wykorzystania danych biometrycznych na wielką skalę w systemach informatycznych występuje także problem związany z nieuniknionymi błędami w zakresie gromadzenia i porównywania danych biometrycznych. Z tych względów prawodawca europejski powinien wykazać się powściągliwością w wykorzystaniu takich danych.

80. Kolejną powracającą kwestią było w ostatnich latach wykorzystanie odcisków palców dzieci i osób starszych, szczególnie z uwagi na niedające się uniknąć niedociągnięcia systemów biometrycznych w zakresie przetwarzania danych osób z tych przedziałów wiekowych. Inspektor poprosił o wykonanie dogłębnej analizy w celu odpowiedniego określenia precyzji takich systemów ([51]). Zaproponował wprowadzenie granicy wieku 14 lat w przypadku dzieci, chyba że wyniki badania zadecydują inaczej. Inspektor zaleca, aby kwestia ta została wspomniana w programie sztokholmskim.

([48]) Wniosek Komisji z dnia 24 czerwca 2009 r. w sprawie rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego agencję ds. zarządzania operacyjnego systemem informacyjnym Schengen (SIS II), wizowym systemem operacyjnym (VIS), systemem EURODAC i innymi wielkoskalowymi systemami informatycznymi w przestrzeni wolności, bezpieczeństwa i sprawiedliwości (COM(2009) 293/2).

([49]) Projekt umowy zatwierdzony przez Radę i oczekujący na podpisy obydwu stron. Zob. rejestr Rady:
http://register.consilium.europa.eu/pdf/en/09/st10/st10019.en09.pdf
http://register.consilium.europa.eu/pdf/en/09/st10/st10107.en09.pdf

([50]) Wnioski połączone 30562/04 i 30566/04, S. i Marper przeciwko Zjednoczonemu Królestwu, orzeczenie z dnia 4 grudnia 2008 r., ECHR, jeszcze nieopublikowane.

([51]) Opinia z dnia 26 marca 2008 r. dotycząca rozporządzenia zmieniającego rozporządzenie Rady (WE) nr 2252/2004 w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez państwa członkowskie, Dz.U. C 200 z 6.8.2008, s. 1.

81. Inspektor stwierdza jednak, że pożyteczne byłoby wprowadzenie merytorycznych kryteriów w zakresie wykorzystania danych biometrycznych. Celem tych kryteriów byłoby dopilnowanie, aby dane były wykorzystywane tylko w razie potrzeby, w sposób odpowiedni i proporcjonalny oraz z zastrzeżeniem wykazania przez prawodawcę jednoznacznego, konkretnego i zgodnego z prawem celu. Konkretniej mówiąc, nie należy używać danych biometrycznych, a w szczególności danych dotyczących DNA, jeżeli taki sam rezultat można osiągnąć z wykorzystaniem innych, mniej chronionych informacji.

VII. **DOSTĘP DO WYMIARU SPRAWIEDLIWOŚCI I E-SPRAWIEDLIWOŚCI**

82. Jako narzędzie usprawnienia współpracy sądowej będzie również wykorzystywana technologia. W pkt 3.4.1 komunikatu e-sprawiedliwość przedstawiona została jako zapewnianie obywatelom łatwiejszego dostępu do wymiaru sprawiedliwości. Składa się ona z portalu oferującego dostęp do informacji i wideokonferencji w ramach postępowania prawnego. Umożliwia także przeprowadzanie postępowań prawnych w Internecie i przewiduje ustanowienie połączenia między różnymi rejestrami krajowymi, takimi jak rejestry niewypłacalności. Inspektor odnotowuje, że w komunikacie brak jest wzmianki o nowych inicjatywach z zakresu e-sprawiedliwości, natomiast znajdują się w nim skonsolidowane informacje o przedsięwzięciach już będących w toku. Inspektor uczestniczy w niektórych spośród tych działań w następstwie wydanej przez niego w dniu 19 grudnia 2008 r. opinii w sprawie komunikatu Komisji – Droga do europejskiej strategii w dziedzinie e-sprawiedliwości ([52]).

83. E-sprawiedliwość to ambitny projekt, który wymaga pełnego wsparcia. Może on skutecznie usprawnić działanie wymiaru sprawiedliwości w Europie oraz ochronę sądową obywatela. Jest to ważny krok w kierunku europejskiej przestrzeni sprawiedliwości. Mimo tej pozytywnej oceny pojawia się kilka uwag:

— systemy techniczne stanowiące część systemu e-sprawiedliwości należy tworzyć w oparciu o zasadę „domyślnej ochrony prywatności". Jak już wspomniano w odniesieniu do europejskiego modelu informacji, pierwszym krokiem jest wybór odpowiedniej architektury,

— sposób realizacji połączeń i interoperacyjności systemów powinien być zgodny z zasadą ograniczenia celu,

— należy precyzyjnie nakreślić zakresy odpowiedzialności poszczególnych podmiotów,

— należy wcześniej przeanalizować, jaki wpływ na obywateli będzie miało powiązanie rejestrów krajowych zawierających szczególnie chronione dane osobowe, takich jak rejestry niewypłacalności.

VIII. **WNIOSKI**

84. Inspektor popiera fakt, że komunikat uznaje ochronę praw podstawowych, w szczególności ochrony danych osobowych, za jedną z kluczowych kwestii przyszłości przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Zdaniem Inspektora komunikat słusznie dąży do zrównoważenia potrzeby istnienia odpowiednich instrumentów gwarantujących bezpieczeństwo obywateli z potrzebą ochrony ich praw podstawowych. Przyznaje też, że kwestii ochrony danych należy poświęcić więcej uwagi.

85. Inspektor w pełni popiera założenia pkt 2.3 komunikatu, w którym wzywa się do utworzenia kompleksowego systemu ochrony danych obejmującego wszystkie obszary właściwości UE, niezależnie od wejścia w życie traktatu lizbońskiego. W tym kontekście zaleca on:

— ogłoszenie w programie sztokholmskim potrzeby stworzenia wyrazistej i długoterminowej wizji dotyczącej takiego kompleksowego programu,

— ocenę przyjętych w tym zakresie środków, ich konkretnego wdrożenia oraz ich skuteczności, z uwzględnieniem wpływu takich środków na ochronę prywatności i ich użyteczności do celów egzekwowania prawa,

— uwzględnienie jako priorytetu w programie sztokholmskim potrzeby nowych ram prawnych, które zastąpiłyby m.in. decyzję ramową Rady 2008/977/WSiSW.

86. Inspektor z zadowoleniem przyjmuje wyrażony przez Komisję zamiar potwierdzenia zasad ochrony danych, które musi odbyć się w powiązaniu z konsultacjami publicznymi ogłoszonymi przez Komisję na konferencji „Dane osobowe – częstsze wykorzystanie, lepsza ochrona?" zorganizowanej w dniach 19 i 20 maja 2009 r. Zasadniczo Inspektor podkreśla znaczenie zasady ograniczenia celu jako podstawy prawa o ochronie danych oraz znaczenie wykorzystywania możliwości poprawy skuteczności stosowania zasad ochrony danych za pomocą instrumentów, które mogą rozszerzyć zakres odpowiedzialności administratorów danych.

87. „Domyślna ochrona prywatności" i technologie niezagrażające prywatności można promować za pomocą:

— systemu certyfikatów z zakresu ochrony danych i prywatności jako opcji dla twórców i użytkowników systemów informatycznych,

— obowiązku prawnego dotyczącego twórców i użytkowników systemów informatycznych, przewidującego korzystanie z systemów zgodnych z zasadą domyślnej prywatności.

88. Jeśli chodzi o aspekty zewnętrzne ochrony danych, Inspektor zaleca:

— podkreślenie w programie sztokholmskim znaczenia ogólnych porozumień ze Stanami Zjednoczonymi i innymi państwami trzecimi w sprawie ochrony i wymiany danych,

([52]) Opinia Inspektora z dnia 19 grudnia 2008 r. w sprawie komunikatu Komisji – Droga do europejskiej strategii w dziedzinie e-sprawiedliwości, Dz.U. C 128 z 6.6.2009, s. 13.

— aktywne propagowanie poszanowania dla praw podstawowych, a w szczególności ochrony danych, w relacjach z państwami trzecimi i organizacjami międzynarodowymi,

— umieszczenie w programie sztokholmskim wzmianki o tym, że wymiana danych osobowych z państwami trzecimi wymaga istnienia w tych państwach trzecich odpowiedniego poziomu ochrony lub innych właściwych zabezpieczeń.

89. Inspektor z wielkim zainteresowaniem śledzi prace nad strategią Unii Europejskiej w zakresie zarządzania informacjami i europejskim modelem informacji i podkreśla, że w przedsięwzięciach tych należy zwrócić uwagę na kwestie dotyczące ochrony danych, które powinny zostać rozwinięte w programie sztokholmskim. Architektura wymiany informacji powinna być oparta na zasadach „domyślnej ochrony prywatności" i „najlepszych dostępnych technik".

90. Sam fakt, że wymiana informacji cyfrowych między interoperacyjnymi bazami danych lub łączenie takich baz danych jest technicznie możliwe, nie uzasadnia wprowadzenia odstępstwa od zasady ograniczenia celu. Interoperacyjność powinna być w konkretnych przypadkach uzależniona od zrozumiałych i ostrożnych decyzji politycznych. Inspektor sugeruje, aby kwestia ta została rozwinięta w programie sztokholmskim.

91. Wykorzystywanie na potrzeby egzekwowania prawa danych osobowych gromadzonych do celów handlowych powinno być zdaniem Inspektora dopuszczalne wyłącznie po spełnieniu surowych warunków określonych w pkt 65 niniejszej opinii.

92. Pozostałe sugestie dotyczące wykorzystania danych osobowych:

— opracowanie merytorycznych kryteriów wyboru między systemami scentralizowanymi i zdecentralizowanymi oraz umieszczenie w programie sztokholmskim wzmianki o zamiarze opracowania takich kryteriów,

— w programie sztokholmskim nie należy wspominać o utworzeniu systemu elektronicznej rejestracji wjazdu na terytorium państw członkowskich i wyjazdu z niego ani programu rejestrowania podróżnych,

— wsparcie dla wzmocnienia Europolu i Eurojustu oraz dla nowej, niedawno wypracowanej umowy między Europolem i Eurojustem,

— opracowanie merytorycznych kryteriów wykorzystania danych biometrycznych w celu dopilnowania, aby dane były wykorzystywane tylko w razie potrzeby, w sposób odpowiedni i proporcjonalny oraz z zastrzeżeniem wykazania przez prawodawcę jednoznacznego, konkretnego i zgodnego z prawem celu. Nie należy używać danych dotyczących DNA, jeżeli taki sam rezultat można osiągnąć z wykorzystaniem innych informacji niebędących szczególnie chronionymi.

93. Inspektor popiera e-sprawiedliwość i zgłosił kilka uwag w sprawie usprawnienia tego przedsięwzięcia (zob. pkt 83).

Sporządzono w Brukseli dnia 10 lipca 2009 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych