EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Opinia Europejskiego Inspektora Ochrony Danych na temat inicjatywy Królestwa Belgii, Republiki Bułgarii, Republiki Federalnej Niemiec, Królestwa Hiszpanii, Republiki Francuskiej, Wielkiego Księstwa Luksemburga, Królestwa Niderlandów, Republiki Austrii, Republiki Słowenii, Republiki Słowackiej, Republiki Włoskiej, Republiki Finlandii, Republiki Portugalskiej, Rumunii i Królestwa Szwecji w celu przyjęcia decyzji Rady w sprawie intensywniejszej współpracy transgranicznej, szczególnie w walce z terroryzmem i przestępczością transgraniczną

(2007/C 169/02)

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 ([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. **Uwagi wstępne**

Przedmiotowa inicjatywa a opinia Europejskiego Inspektora Ochrony Danych

1. W lutym 2007 r. piętnaście państw członkowskich wystąpiło z inicjatywą, która miała na celu przyjęcie decyzji Rady w sprawie intensywniejszej współpracy transgranicznej, szczególnie w walce z terroryzmem i przestępczością transgraniczną ([3]). Inicjatywa dotyczy kwestii z zakresu przetwarzania danych osobowych. Europejski Inspektor Ochrony Danych ma obowiązek zająć stanowisko na temat tej inicjatywy, gdyż jest to w zakresie zadań powierzonych mu zwłaszcza na mocy art. 41 rozporządzenia (WE) nr 45/2001. Europejski Inspektor Ochrony Danych wydaje niniejszą opinię z urzędu, gdyż nie otrzymał żadnego wniosku o zajęcie stanowiska ([4]). Jego zdaniem niniejsza opinia powinna zostać wymieniona w preambule decyzji Rady ([5]).

([1]) Dz.U. L 281 z 23.11.1995, str. 31.
([2]) Dz.U. L 8 z 12.1.2001, str. 1.
([3]) Odnośne państwa członkowskie są wymienione w tytule niniejszej opinii. Ich inicjatywa została opublikowana w dniu 28 marca 2007 r. w Dz.U. C 71, str. 35.
([4]) Art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 obliguje Komisję, żeby zasięgała opinii Europejskiego Inspektora Ochrony Danych, gdy przyjmuje ona wniosek legislacyjny, który wiąże się z ochroną praw i swobód osób fizycznych podczas przetwarzania danych osobowych. Jeżeli z inicjatywą występuje jedno państwo członkowskie (lub więcej), wymóg ten nie ma zastosowania; wystąpienie do Europejskiego Inspektora Ochrony Danych o opinię jest dla zaangażowanych państw członkowskich fakultatywne.
([5]) Tak jak Komisja postąpiła w innych przypadkach (mających niedawno miejsce). Najnowszy przykład: zobacz opinię Europejskiego Inspektora Ochrony Danych z dnia 12 grudnia 2006 r. na temat wniosków w sprawie zmiany rozporządzenia finansowego mającego zastosowanie do budżetu ogólnego Wspólnot Europejskich oraz zmiany zasad wykonywania tego rozporządzenia (COM(2006) 213 wersja ostateczna i SEC(2006) 866 wersja ostateczna); opinia została opublikowana na stronie www.edps.europa.eu.

Rodowód omawianej inicjatywy i jej treść

2. Omawiana inicjatywa zrodziła się w sposób nie mający precedensu we współpracy w ramach trzeciego filaru. Służy temu, by najważniejsze części konwencji z Prüm, podpisanej w dniu 27 maja 2005 r. przez siedem państw członkowskich ([6]), zaczęły obowiązywać we wszystkich państwach członkowskich. Niektóre z owych siedmiu państw członkowskich już ratyfikowały odnośne części konwencji, w innych proces ratyfikacji trwa. Jest zatem oczywiste, że te najważniejsze części nie będą zmieniane pod względem merytorycznym ([7]).

3. Jak wynika z motywów decyzji, inicjatywa ma być traktowana jako narzędzie wdrożenia zasady dostępności, która w programie haskim z roku 2004 została przedstawiona jako innowacja w transgranicznej wymianie informacji między organami ochrony porządku publicznego ([8]). Inicjatywa została przedstawiona jako rozwiązanie alternatywne względem wniosku dotyczącego ramowej decyzji Rady w sprawie wymiany informacji w ramach zasady dostępności; Europejski Inspektor Ochrony Danych zaopiniował wniosek w dniu 28 lutego 2006 r. ([9]), ale Rada wniosku nie omawiała ani nie rozpatrywała jego ewentualnego przyjęcia.

4. W opiniowanej inicjatywie przyjęto podejście całkowicie inne niż we wspomnianym wniosku dotyczącym ramowej decyzji Rady. O ile wniosek przewiduje bezpośredni dostęp do zgromadzonych informacji, o tyle inicjatywa mówi o dostępie pośrednim, przez dane referencyjne. Ponadto inicjatywa obliguje państwa członkowskie do gromadzenia i przechowywania określonych informacji, nawet gdy informacjami tymi nie dysponuje się jeszcze na terytorium podlegającym krajowej jurysdykcji.

5. Inicjatywa kładzie istotny akcent na wymianę informacji biometrycznych między policją a organami sądowymi państw członkowskich, a zwłaszcza na wymianę danych ze zbiorów analiz DNA i zautomatyzowanych systemów informacji daktyloskopijnej (systemów zawierających odciski palców ([10])).

6. Rozdział 6 inicjatywy ma tytuł „Przepisy ogólne o ochronie danych". Zawiera on przepisy sformułowane specjalnie z myślą o szczególnym charakterze wymiany danych, którą reguluje ([11]). Zawiera także odwołanie do konwencji Rady Europy nr 108 ([12]) i do odnośnych dokumentów Rady Europy, które — ponieważ nie przyjęto jeszcze ramowej decyzji Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych — wyznaczają ogólne ramy ochrony danych ([13]).

II. **Główny przedmiot opinii Europejskiego Inspektora Ochrony Danych**

7. W niniejszej opinii zostanie uwzględniony bezprecedensowy charakter przedmiotowej inicjatywy, a konkretniej fakt, że nie przewiduje się większych merytorycznych zmian w jej przepisach. Dlatego Europejski Inspektor Ochrony Danych skupi się na pewnych ogólniejszych kwestiach dotyczących samej inicjatywy i jej kontekstu. Modyfikacje proponowane przez Europejskiego Inspektora Ochrony Danych mają głównie poprawić sam tekst, a nie zmieniać cały system wymiany informacji.

8. Pierwsza kwestia dotyczy zagadnień proceduralnych. Z tekstu inicjatywy wynika, że pewna mała liczba państw członkowskich dokonuje wyborów dotyczących polityki za wszystkie państwa członkowskie w dziedzinie objętej postanowieniami Traktatu o UE, a zwłaszcza jego tytułu VI (trzeci filar). Nie dotrzymano procedur określonych w tytule VI w zakresie pogłębionej współpracy.

9. Druga kwestia dotyczy zasady dostępności. Choć opiniowana inicjatywa ma być traktowana jako narzędzie wdrożenia tej zasady, to nie zapewnia ona dostępności jako takiej, lecz jest zaledwie kolejnym krokiem ku temu, by informacje służące do ochrony porządku publicznego były dostępne bez względu na granice państw członkowskich. Jest częścią stopniowych działań mających ułatwić wymianę informacji, które służą do ochrony porządku publicznego.

([6]) Konwencjaz Prüm z dnia 27 maja 2005 r. zawarta między Królestwem Belgii, Republiką Federalną Niemiec, Królestwem Hiszpanii, Republiką Francuską, Wielkim Księstwem Luksemburga, Królestwem Niderlandów i Republiką Austrii w sprawie intensywniejszej współpracy transgranicznej, szczególnie w walce z terroryzmem, przestępczością transgraniczną i nielegalną migracją.

([7]) Patrz dalej, pkt 15.

([8]) Program haski dotyczący wzmacniania wolności, bezpieczeństwa i sprawiedliwości w Unii Europejskiej, w wersji zatwierdzonej przez Radę Europejską w dniu 5 listopada 2004 r.

([9]) COM (2005) 490 wersja ostateczna. Opinia Europejskiego Inspektora Ochrony Danych została opublikowana w Dz.U. C 116 z 17.5.2006, str. 8.

([10]) W opinii będzie stosowany powszechniejszy termin „odciski palców" — zamiast „danych daktyloskopijnych" używanych w tekście inicjatywy.

([11]) Patrz motyw nr 17 inicjatywy.

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

([13]) Co do szczegółów patrz część VII niniejszej opinii.

10. Trzecią kwestię można określić jako kwestię proporcjonalności. Trudno ocenić, czy przepisy omawianej inicjatywy w sprawie decyzji Rady są uzasadnione potrzebą zwalczania terroryzmu i przestępczości transgranicznej. Europejski Inspektor Ochrony Danych przypomina, że konwencja z Prüm powstała jako eksperyment w transgranicznej wymianie informacji, a zwłaszcza zbiorów analiz DNA i odcisków palców. Tymczasem obecna inicjatywa została przedstawiona, zanim w praktyce przeprowadzono próby wymiany informacji ([14]).

11. Czwarta kwestia dotyczy wykorzystywania danych biometrycznych. Tekst inicjatywy nakazuje gromadzić, przechowywać i wymieniać (w ograniczonym zakresie) zbiory analiz DNA i odciski palców. Wykorzystanie tych danych biometrycznych do ochrony porządku publicznego przedstawia konkretne zagrożenia dla osób, których te dane dotyczą, i wymaga dodatkowych gwarancji co do ochrony praw tych osób.

12. Piąta kwestia wynika z tego, że decyzja Rady powinna mieć za podstawę odpowiednie przepisy ogólne o ochronie danych w trzecim filarze, tymczasem przepisów takich jeszcze nie ma na szczeblu UE. W niniejszej opinii Europejski Inspektor Ochrony Danych zilustruje, jak ważne są takie przepisy ogólne jako *condicio sine qua non* wymiany danych osobowych między organami ochrony porządku publicznego na podstawie przedmiotowej inicjatywy.

III.. **Kwestia proceduralna i podstawa prawna**

13. Konwencja z Prüm jest często porównywana do układu z Schengen z roku 1985 i do konwencji z Schengen z 1990, i to z powodów oczywistych. Zaangażowane są tu właściwie te same państwa, przedmiot konwencji jest podobny, a także jest ścisły związek ze współpracą w ramach UE ([15]). Jest i jednak fundamentalna różnica względem aktów schengeńskich: obecnie istnieją europejskie przepisy ramowe, które pozwalają Unii Europejskiej regulować odnośne zagadnienia; były też nawet plany, by przepisy te wykorzystać w (głównych) kwestiach objętych konwencją z Prüm. Konkretnie chodzi o to, że gdy zawierano konwencję z Prüm, Komisja przygotowywała wniosek dotyczący ramowej decyzji Rady ([16]).

14. Jednak zaangażowane państwa członkowskie wybrały formułę wielostronnego układu, dzięki której uniknęły prawodawczych komplikacji trzeciego filaru wymagającego jednomyślności. Ominęły także merytoryczne i proceduralne wymogi zacieśnionej współpracy, określone w art. 40, 40a, 43 i 43a Traktatu o UE ([17]). Jest to tym istotniejsze, że procedura zacieśnionej współpracy obowiązywałaby, gdyby we współpracy uczestniczyło przynajmniej osiem państw członkowskich. Tymczasem tylko siedem państw członkowskich podpisało konwencję z Prüm, ale nakłoniły one potem kolejne państwa członkowskie, by się przyłączyły. Na tej podstawie można by dowodzić, że konwencja z Prüm narusza prawo Unii Europejskiej. Dowodzenie to miałoby jednak głównie teoretyczny charakter, skoro w trzecim filarze Komisja ma ograniczone kompetencje, by nadzorować przestrzeganie prawa Unii Europejskiej przez państwa członkowskie; ograniczone kompetencje mają też Europejski Trybunał Sprawiedliwości i inne sądy.

15. Sytuacja obecna jest taka, że 15 państw członkowskich wyszło z inicjatywą, by konwencję z Prüm zastąpić decyzją Rady. I choć możliwość modyfikacji istoty przepisów nie jest formalnie wykluczona, ani też zresztą nie można jej formalnie wykluczyć, jasne jest, że celem państw członkowskich, które wyszły z inicjatywą, jest niedopuszczenie do żadnych istotnych zmian. Cel taki wynika z tego, że siedem państw „z grona Prüm" właśnie przeniosło konwencję do prawa krajowego (lub też ich prace są zaawansowane), i nie chce znów zmieniać swoich przepisów krajowych. Cel ten widać w sposobie postępowania prezydencji niemieckiej w Radzie. Przykładowo: czas przewidziany na przyjęcie inicjatywy jest bardzo ograniczony, a sama inicjatywa nie będzie omawiana przez grupę roboczą Rady, jedynie przez Komitet Art. 36 (komitet koordynacyjny złożony z urzędników wyższego szczebla i powołany na mocy art. 36 TUE).

16. W konsekwencji inne państwa członkowskie pozbawione są faktycznej możliwości zajęcia stanowiska co do wyboru zasad współpracy. Mogą jedynie wybrać między uczestniczeniem a nieuczestniczeniem. Trzeci filar wymaga jednomyślności, więc jeżeli jedno państwo członkowskie nie zaaprobuje tekstu, skutek może być taki, że inne państwa członkowskie podejmą działania w trybie zacieśnionej współpracy.

([14]) Oprócz pierwszej próby wymiany informacji przeprowadzonej przez Niemcy i Austrię i wspomnianej w pkt 33.

([15]) W epoce Schengen chodziło o współpracę w ramach Europejskiej Wspólnoty Gospodarczej. O konwencji z Prüm mówi się często: Schengen III.

([16]) Wniosek ten (wspomniany już w pkt 3) Komisja przyjęła już po tym, jak została przyjęta konwencja z Prüm.

([17]) Przywołane artykuły nakazują m.in. zaangażować Komisję i Parlament Europejski oraz korzystać z formuły zacieśnionej współpracy tylko w ostateczności.

17. Taki rodowód całej inicjatywy oddziałuje także na demokratyczną legitymację propozycji, skoro opinia Parlamentu Europejskiego, wymagana w art. 39 TUE, właściwie nie może mieć wpływu na wybór zasad współpracy. A zatem opinia taka może mieć tylko ograniczony efekt.

18. Zdaniem Europejskiego Inspektora Ochrony Danych wybór takiego trybu działania był niefortunny. Przyjmując ten tryb, zakwestionowano jakąkolwiek potrzebę demokratycznej i przejrzystej procedury legislacyjnej, skoro nie uwzględniono w nim nawet już i tak bardzo ograniczonych prerogatyw przewidzianych w trzecim filarze. Na obecnym etapie Europejski Inspektor Ochrony Danych przyjmuje do wiadomości, że właśnie taki tryb został wybrany; w dalszej części swojej opinii skupi się zatem głównie na istocie omawianej inicjatywy.

19. I wreszcie, Europejski Inspektor Ochrony Danych pragnie zauważyć, że omawiana inicjatywa dotyczy decyzji Rady, a nie ramowej decyzji Rady, mimo że chodzi w niej o zbliżenie przepisów i uregulowań państw członkowskich. Wybór takiej formuły prawnej może wynikać z tego, że gdy chodzi o decyzje Rady zapadające na mocy art. 34 ust. 2 lit. c) TUE, można uchwalać przepisy wykonawcze większością kwalifikowaną. O tych przepisach wykonawczych mówi art. 34 omawianej inicjatywy.

20. Europejski Inspektor Ochrony Danych zaleca, żeby do art. 34 opiniowanej inicjatywy w sprawie decyzji Rady dodać zdanie w brzmieniu: „Przed przyjęciem takich przepisów wykonawczych Rada zasięga opinii Europejskiego Inspektora Ochrony Danych." Powód takiej zmiany jest oczywisty: przepisy wykonawcze będą w większości przypadków dotyczyć przetwarzania danych osobowych. Poza tym jeżeli Komisja nie obejmie inicjatywy w sprawie tych przepisów, art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 nie będzie miał zastosowania.

21. Przy okazji należy zwrócić uwagę, że owe siedem państw członkowskich, które podpisały konwencję z Prüm, zawarło oprócz tego w dniu 5 grudnia 2006 r. porozumienie wykonawcze z postanowieniami niezbędnymi do wdrożenia i wykonania konwencji pod względem administracyjnym i technicznym ([18]). Można przypuszczać, że to porozumienie wykonawcze posłuży za wzór dla przepisów wykonawczych, o których mowa w art. 34 inicjatywy w sprawie decyzji Rady. Niniejsza opinia będzie zatem w takim stopniu dotyczyć wspomnianego porozumienia wykonawczego, w jakim będzie to pomocne w lepszym rozumieniu samej inicjatywy.

IV. **Przedmiotowa inicjatywa a zasada dostępności**

22. Zasadę dostępności można traktować jako ważne narzędzie pozwalające urzeczywistniać przestrzeń wolności, bezpieczeństwa i sprawiedliwości niepodzieloną granicami wewnętrznymi. Swobodna wymiana informacji między organami ochrony porządku publicznego jest ważnym krokiem w pokonywaniu barier terytorialnych, które utrudniają walkę z przestępczością; istniejące granice wewnętrzne blokują bowiem dochodzenia.

23. Jak głosi program haski, zasada dostępności oznacza, że „na obszarze całej Unii urzędnik organu ścigania w jednym państwie członkowskim, który potrzebuje informacji w celu wykonania swoich obowiązków, może je uzyskać od drugiego państwa członkowskiego oraz że organ ścigania w tym drugim państwie członkowskim, który posiada informacje, udostępni je we wskazanym celu (…)". Ponadto w programie podkreślono, że „metody wymiany informacji powinny w pełni wykorzystywać nową technologię i muszą być dostosowane do każdego typu informacji, w stosownych przypadkach, poprzez wzajemny dostęp lub połączenie krajowych baz danych na podstawie ich interoperacyjności lub bezpośredniego dostępu (on-line)".

24. Na tym tle widać, że omawiana inicjatywa jest tylko małym krokiem. Nie jest tak ambitna jak wniosek Komisji dotyczący ramowej decyzji Rady w sprawie wymiany informacji w ramach zasady dostępności. Może kwalifikować się jako krok w kierunku zapewnienia dostępności, ale nie urzeczywistnia ona ściśle pojętej zasady dostępności. Uzupełnia inne przepisy, które mają ułatwiać wymianę informacji do ochrony porządku publicznego, takie jak ramową decyzję Rady 2006/960/WSiSW z dnia 18 grudnia 2006 r. w sprawie uproszczenia wymiany informacji i danych wywiadowczych między organami ścigania państw członkowskich Unii Europejskiej ([19]), i które mają zagwarantować, że informacje oraz dane wywiadowcze będą na żądanie przekazywane organom innych państw członkowskich.

([18]) Porozumienie to przedstawiono w dokumencie Rady nr 5473/07 z dnia 22 stycznia 2007 r. Patrz http://www.statewatch.org/news/2007/jan/prum-implementing-agreement.pdf.

([19]) Dz.U. L 368 z 29.12.2006, str. 89. Przywołana decyzja ramowa jest przyjęta z inicjatywy Szwecji.

25. W swojej opinii na temat odnośnego wniosku Komisji Europejski Inspektor Ochrony Danych opowiedział się za tym, by zasadę dostępności wprowadzać w sposób ostrożniejszy, stopniowy. Przy takim podejściu należałoby ograniczyć rodzaje danych wymienianych zgodnie z zasadą dostępności i dopuścić tylko dostęp pośredni, przez odnośniki ([20]). Dzięki takiemu stopniowemu podejściu zainteresowane strony mogłyby kontrolować skuteczność wymiany danych do ochrony porządku publicznego oraz konsekwencje w dziedzinie ochrony danych osobowych dotyczących obywateli.

26. Uwagi te są nadal aktualne w obecnej sytuacji. Europejski Inspektor Ochrony Danych odnotowuje z zadowoleniem, że w przedmiotowej inicjatywie przyjęto właśnie takie ostrożne, stopniowe podejście do wdrażania zasady dostępności.

27. Jako przykład tego podejścia można potraktować art. 5 i 10. Mówią one o dostarczaniu bardziej szczegółowych danych osobowych (i innych informacji) po tym, gdy zostanie stwierdzona zgodność odpowiednio: profili DNA lub odcisków palców. W obu przypadkach ma decydować prawo krajowe zapytanego państwa członkowskiego, w tym jego przepisy o pomocy prawnej. Skutek prawny obu artykułów jest ograniczony. Ustanawiają one normę kolizyjną (zasady o charakterze deklaratywnym, a nie zmieniającym obecną sytuację), ale nie urzeczywistniają one zasady dostępności ([21]).

V. **Konieczność i proporcjonalność**

28. Sprawna wymiana informacji do ochrony porządku publicznego jest kluczową kwestią we współpracy policyjnej i sądowej. Jeżeli przestrzeń wolności, bezpieczeństwa i sprawiedliwości niepodzielona granicami wewnętrznymi ma rozwijać się, istotne jest, aby informacje były do dyspozycji bez względu na granice krajowe. Aby ułatwić wymianę informacji, potrzeba stworzyć odpowiednie uregulowania prawne.

29. Inną kwestią jest pytanie, czy przepisy omawianej inicjatywy są uzasadnione potrzebą zwalczania terroryzmu i przestępczości transgranicznej — innymi słowy: czy przepisy te są konieczne i proporcjonalne.

30. Po pierwsze, na szczeblu Unii Europejskiej przyjęto różne przepisy, by ułatwić wymianę informacji do ochrony porządku publicznego. W niektórych przypadkach przepisy te przewidują utworzenie centralnego organu, takiego jak Europol czy Eurojust, lub centralnego systemu informacyjnego, takiego jak system informacyjny Schengen. Inne przepisy, jak np. omawiana inicjatywa, dotyczą bezpośredniej wymiany informacji między państwami członkowskimi. Zupełnie niedawno przyjęto decyzję ramową Rady 2006/960/WSiSW, która ma uprościć wymianę informacji do ochrony porządku publicznego.

31. Zasadniczo nowe akty prawne w dziedzinie współpracy policyjnej i sądowej należy przyjmować dopiero wtedy, gdy w wyniku oceny środków już istniejących stwierdzi się, że te istniejące środki nie wystarczają. W motywach omawianej inicjatywy nie wspomniano pełnej oceny istniejących środków. Wspomniano w nich natomiast decyzję ramową Rady 2006/960/WSiSW i stwierdzono, że należy w pełni wykorzystywać nowe technologie i wzajemnie ułatwiać dostęp do krajowych baz danych. Dokładnie określone informacje powinny być wymieniane szybko i sprawnie. To wszystko. Nie ma na przykład odniesienia do wymiany informacji między państwami członkowskimi przez system informacyjny Schengen, który jest zasadniczym narzędziem wymiany informacji między państwami członkowskim.

32. Europejski Inspektor Ochrony Danych żałuje, że z omawianą inicjatywą wystąpiono, nie dokonawszy odpowiedniej oceny istniejących środków wymiany informacji do ochrony porządku publicznego, oraz apeluje do Rady, by zapewniła taką ocenę podczas procedury przyjmowania opiniowanej propozycji.

33. Po drugie, jak już wspomniano, konwencja z Prüm powstała jako eksperyment w transgranicznej wymianie informacji, a zwłaszcza zbiorów analiz DNA i odcisków palców. Dzięki niej zaangażowane państwa członkowskie mogły poprzeprowadzać próby takiej wymiany. Do dnia, w którym wystąpiono z opiniowaną inicjatywą decyzji Rady, właściwie nie wykonano takich prób na szerszą skalę, poza pierwszą wymianą przeprowadzoną przez Niemcy i Austrię ([22]).

([20]) Opinia Europejskiego Inspektora Ochrony Danych z dnia 28 lutego 2006 r., Dz.U. C 116 z 17.5.2006, str. 8, pkt 69.

([21]) Europejski Inspektor Ochrony Danych ogólnie z zadowoleniem odnotowuje przyjęcie podejścia stopniowego (pkt 26). Jednakże, jak zostanie pokazane w pkt 37, w tym konkretnym przypadku lepiej byłoby minimalnie zharmonizować zasadnicze elementy gromadzenia i wymiany różnych rodzajów danych.

([22]) Wyniki zautomatyzowanego porównania profili DNA w niemieckich i austriackich bazach DNA przedstawiono na nieoficjalnym spotkaniu ministrów WSiSW w Dreźnie (w dniach 14–16 stycznia 2007 r.) i opublikowano na stronie prezydencji niemieckiej (www.bmi.bund.de). Pochodzą one, ogólnie rzecz biorąc, z listopada i grudnia 2006 r. Wśród wyników tej pierwszej wymiany jest godna podziwu liczba trafień: ponad 2 000 w ciągu dwóch miesięcy; w niektórych przypadkach było ewidentne, że trafienia dotyczyły poważnych przestępstw.

34. Europejski Inspektor Ochrony Danych nie jest przekonany, żeby owe pierwsze wyniki takiej ograniczonej wymiany informacji (prowadzonej krótko i tylko przez dwa państwa członkowskie) dawały — mimo swojej atrakcyjności — odpowiednie podstawy empiryczne do wprowadzenia tego systemu we wszystkich państwach członkowskich.

35. Inna jest skala problemów, gdy tworzy się system wymiany informacji między kilkoma państwami członkowskimi, które już mają doświadczenia w korzystaniu z baz DNA, a inna, gdy tworzy się system ogólnoeuropejski, obejmujący państwa członkowskie bez żadnego doświadczenia. Ponadto przedsięwzięcia na małą skalę umożliwiają zaangażowanym państwom ścisły kontakt; kontakt ten można też wykorzystać do monitorowania zagrożeń, które mogą osłabić ochronę danych osobowych odnośnych osób. Poza tym przedsięwzięcia na małą skalę łatwiej jest nadzorować. A zatem nawet gdyby sama konwencja z Prüm była aktem koniecznym i proporcjonalnym, nie oznaczałoby to jeszcze, że omawiana inicjatywa zasługuje na podobną ocenę.

36. Po trzecie, jak zostanie wykazane w dalszej części niniejszej opinii, przepisy krajowe poszczególnych państw członkowskich znacznie różnią się między sobą, jeżeli chodzi o gromadzenie i wykorzystywanie danych biometrycznych do ochrony porządku publicznego. Także brak harmonizacji co do praktyki w poszczególnych krajach. Przy okazji należy też zauważyć, że nie przyjęto jeszcze zharmonizowanych przepisów ramowych o ochronie danych w trzecim filarze.

37. Opiniowana inicjatywa nie harmonizuje zasadniczych elementów gromadzenia ani wymiany różnych rodzajów danych, o których w niej mowa. Na przykład nie określa ona jednoznacznie celów, jakim mają służyć to gromadzenie i ta wymiana. Czy przepisy o profilach DNA dotyczą wszystkich przestępstw, czy też państwo członkowskie może ograniczyć ich zastosowanie tylko do przestępstw poważniejszych? Inicjatywa nie precyzuje też wyraźnie kręgu osób, których dane gromadziłoby się i wymieniało. Czy w bazach danych są tylko informacje (biometryczne) o podejrzanych lub skazanych, czy także informacje o innych osobach, których dotyczą dane, takich jak świadkowie lub inne osoby akurat znajdujące się w pobliżu w chwili, gdy popełniane było przestępstwo? Zdaniem Europejskiego Inspektora Ochrony Danych bardziej wskazana byłaby minimalna harmonizacja tych zasadniczych elementów — także dlatego, że pozwoliłaby dochować zasady konieczności i zasady proporcjonalności.

38. Europejski Inspektor Ochrony Danych stwierdza zatem: są jednoznaczne przesłanki, by przewidywać, że opiniowana inicjatywa będzie aktem pożytecznym we współpracy policyjnej. Przesłanki te okazują jeszcze bardziej uzasadnione w świetle wyników pierwszych doświadczeń Niemiec i Austrii ze stosowaniem konwencji z Prüm. Nie jest jednak łatwo stwierdzić, jak dalece inicjatywa ta jest konieczna i proporcjonalna. Europejski Inspektor Ochrony Danych żałuje, że omawianą inicjatywę wysunięto, nie przeprowadziwszy odpowiedniej oceny jej wpływu, w której by uwzględniono uwagi wyrażone w niniejszej części opinii. Apeluje do Rady, aby dokonała takiej oceny podczas przyjmowania aktu i by rozpatrzyła w niej inne warianty działania, w miarę możliwości powodujące mniejszą ingerencję w życie prywatne ([23]).

39. Europejski Inspektor Danych Osobowych proponuje, aby klauzulę o ocenie zamieścić w rozdziale 7 inicjatywy („Postanowienia wykonawcze i końcowe"). Klauzula taka mogłaby mieć następujące brzmienie: „Najpóźniej w terminie trzech lat od dnia, w którym niniejsza decyzja Rady zacznie obowiązywać, Komisja przedłoży Parlamentowi Europejskiemu i Radzie ocenę jej stosowania, która pozwoli określić, czy przepisy niniejszej decyzji Rady wymagają zmiany".

40. Taka klauzula o ocenie jest szczególnie użyteczna w obecnej sytuacji — gdy konieczność i proporcjonalność przedmiotowej inicjatywy nie zostały (jeszcze) jasno stwierdzone, a ogólnoeuropejski system wymiany informacji jest wprowadzany na podstawie niewielu doświadczeń.

VI. **Różne rodzaje danych: profile DNA, odciski palców i inne dane rejestracyjne pojazdów**

Uwagi ogólne

41. W rozdziale 2, zatytułowanym „Dostęp *on-line* i dalsze zapytania", wyróżniono trzy rodzaje danych: profile DNA, odciski palców i inne dane rejestracyjne pojazdów. W kwestii tego rozróżnienia należy uczynić dwie ogólne uwagi.

42. Po pierwsze, należy zwrócić uwagę, że wszystkie dane przetwarzane na mocy decyzji Rady, oprócz danych określonych w art. 13 ([24]), to dane osobowe w rozumieniu dyrektywy 95/46/WE ([25]) i innych aktów prawa wspólnotowego. Według art. 2 lit. a) wspomnianej dyrektywy „dane osobowe" oznaczają wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;

([23]) Chodzi o „ocenę regulacji pod względem jej wpływu na życie prywatne".
([24]) I być może też niezidentyfikowanych profili DNA, wspomnianych w art. 2 ust. 2 opiniowanej inicjatywy.
([25]) Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych, Dz.U. L 281, str. 31.

osoba możliwa do zidentyfikowania to taka osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, w szczególności na podstawie numeru identyfikacyjnego lub co najmniej jednej cechy właściwej dla jej tożsamości fizycznej, fizjologicznej, psychicznej, ekonomicznej, kulturowej czy społecznej. Tę samą definicję zastosowano we wniosku dotyczącym ramowej decyzji Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej; jeżeli decyzja ta zostanie przyjęta, będzie miała zastosowanie do wymiany informacji objętej opiniowaną inicjatywą. Europejski Inspektor Ochrony Danych żałuje, że w opiniowanej inicjatywie nie podano definicji danych osobowych, i proponuje, by w trosce o jasność prawną definicja taka została ujęta w art. 24.

43. Niezależnie od tego, definicja przywołana w poprzednim punkcie nie pozostawia wątpliwości co do tego, że również bazy danych, które zawierają tylko profile DNA oraz dane referencyjne ze zbiorów analiz DNA i z systemów identyfikacji odcisków palców, uznawane są w całości lub w przeważającej części za zbiory danych osobowych.

44. Po drugie, wymiana każdego z tych trzech rodzajów danych osobowych — profili DNA, odcisków palców i danych rejestracyjnych pojazdów — służy innemu celowi: co do DNA— państwa członkowskie zakładają i prowadzą krajowe zbiory analiz DNA, by umożliwić wykrywanie przestępstw (art. 2 ust. 1); co do odcisków palców — dopilnowują one, aby dostępne były dane referencyjne ze zbioru wykorzystywanego w krajowych zautomatyzowanych systemach automatycznej identyfikacji odcisków palców, które to systemy stworzono do celów prewencji kryminalnej i wykrywania przestępstw (art. 8); a co do danych rejestracyjnych pojazdów — wymiana służy nie tylko prewencji kryminalnej i wykrywaniu przestępstw, ale także zwalczaniu określonych wykroczeń oraz ochronie porządku i bezpieczeństwa publicznego (art. 12 ust. 1).

45. Podobnie wymiana danych DNA i odcisków palców oraz dostęp do obu tych kategorii danych podlega ostrzejszym gwarancjom, niż ma to miejsce w przypadku danych rejestracyjnych pojazdów. Jeśli chodzi o dane DNA i odciski palców, dostęp ograniczony jest początkowo do danych referencyjnych, które nie pozwalają na bezpośrednią identyfikację osoby. W omawianej inicjatywie sformułowana jest zasada rozdzielania danych biometrycznych od tekstowych danych identyfikacyjnych i przechowywania ich w dwóch odrębnych bazach danych. Dostęp do bazy danych drugiej kategorii jest możliwy dopiero wtedy, gdy nastąpiło trafienie w bazie danych pierwszej kategorii. Do takiego rozdzielenia baz danych nie dochodzi w przypadku danych rejestracyjnych pojazdów: dostęp do nich jest automatyczny i bezpośredni i nie ma wymogu zakładania innej bazy danych.

46. Europejski Inspektor Danych Osobowych popiera taki stopniowy dostęp i uważa, że stanowi on dobry sposób ochrony osoby, której dotyczą dane: im większej ochrony dane wymagają, tym węższe jest ich wykorzystanie i tym bardziej ograniczony jest dostęp do nich. A co do samych danych DNA, które spośród danych personalnych objętych przedmiotową inicjatywą wymagają potencjalnie największej ochrony, to mogą one być wymieniane wyłącznie do ścigania przestępstw, a nie do celów prewencyjnych. Ponadto wolno pobierać profile tylko niekodującej części DNA.

Szczegółowe uwagi dotyczące danych DNA

47. Jeżeli chodzi o dane DNA, Europejski Inspektor Ochrony Danych odsyła do swoich wcześniejszych opinii ([26]). Kwestią zasadniczej wagi jest to, by pojęcie „dane DNA" było precyzyjnie zdefiniowane oraz by istniało rozróżnienie między profilami DNA a danymi DNA, które mogą nieść informacje o cechach genetycznych osoby lub o stanie jej zdrowia. Należy także wziąć pod uwagę postęp w nauce: to, co w danym momencie uważane jest za niewinny profil DNA, może wraz z upływem czasu być źródłem znacznie większej liczby informacji, niż się tego spodziewano lub niż to było potrzebne.

48. Według omawianej inicjatywy profile DNA mają być dostępne tylko o tyle, o ile ustalone są na podstawie niekodującej części DNA. W tekście inicjatywy brak jednak precyzyjnej definicji profili DNA; nie mówi on też, w jakim trybie takie wspólne definicje by ustalano zależnie od aktualnego poziomu rozwoju nauki. Porozumienie wykonawcze do konwencji z Prüm ([27]) zawiera następującą definicję części niekodującej: segmenty chromosomów nie zawierające informacji genetycznych, czyli takie segmenty, o których nie wiadomo, by niosły informacje o konkretnych cechach dziedzicznych. Europejski Inspektor Ochrony Danych sugeruje, aby definicję części niekodującej umieścić w tekście samej inicjatywy oraz aby stworzyć procedurę gwarantującą, że ani obecnie, ani w przyszłości nie będzie można z części niekodującej uzyskać żadnych innych informacji.

([26]) Zobacz np. wskazaną w przypisie nr 9 opinię Europejskiego Inspektora Ochrony Danych na temat zasady dostępności, pkt 59–60.
([27]) Patrz przypis 18.

49. W omawianej inicjatywie przyjęto założenie, że podstawowym środkiem współpracy policji jest ustalanie zgodności profili DNA. Dlatego wszystkie państwa członkowskie muszą stworzyć bazy danych DNA do celów karnosądowych. Z uwagi na koszty związane z tymi bazami danych oraz zagrożenia dotyczące ochrony danych należy wcześniej dokładnie ocenić skuteczność opiniowanego aktu. Niewielkie doświadczenie z wymianą danych DNA między Niemcami a Austrią to za mało.

50. Pod tym względem Europejski Inspektor Ochrony Danych dostrzega, że omawiana inicjatywa obliguje wszystkie państwa członkowskie, by stworzyły krajowe zbiory analiz DNA. Należy podkreślić, że kilka państw członkowskich dysponuje już dobrze rozwiniętymi krajowymi bazami danych DNA, podczas gdy inne państwa członkowskie mają w tej dziedzinie mniej doświadczenia, lub nie mają żadnego. Najlepiej rozwiniętą bazą danych w Europie (i na świecie) jest baza danych DNA w Zjednoczonym Królestwie. Obejmuje ona ponad 3 miliony wpisów i tym samym jest najbogatszym zbiorem profili DNA. Ujęte są w niej osoby skazane za popełnienie przestępstwa, osoby zatrzymywane, a także osoby, które dobrowolnie złożyły próbki swojego DNA zapobiegawczo ([28]). W innych państwach sytuacja jest odmienna. Na przykład w Niemczech przechowuje się jedynie profile osób, które skazano za popełnienie poważnych przestępstw. Można by nawet przypuszczać, że gromadzenie danych DNA do szerszych celów byłoby w Niemczech sprzeczne z orzecznictwem Trybunału Konstytucyjnego ([29]).

51. Europejski Inspektor Ochrony Danych żałuje, że w opiniowanej inicjatywie nie wskazano kategorii osób, które byłyby ujęte w bazach danych DNA. Dzięki wskazaniu ich nie tylko by zharmonizowano odnośne przepisy krajowe — co z kolei usprawniłoby współpracę transgraniczną — ale być może również by zwiększono proporcjonalność gromadzenia i wymiany danych osobowych, o ile by ograniczono kategorie osób.

52. Kolejna kwestia z tej dziedziny, pozostawiona do rozstrzygnięcia ustawodawcom państw członkowskich, dotyczy okresu przechowania danych w zbiorach analiz DNA. Prawo krajowe może głosić, że profile utworzone w tych zbiorach przechowuje się przez cały okres życia osoby, której profile te dotyczą, bez względu na wynik postępowania sądowego; mogłoby też głosić, że profile zachowuje się tylko wtedy, gdy danej osobie zostały postawione zarzuty i w związku z tym została ona skazana przez sąd, lub też że potrzeba dalszego przechowywania profilu jest regularnie weryfikowana ([30]).

53. Na koniec Europejski Inspektor Ochrony Danych pragnie zwrócić uwagę na art. 7, „Pobieranie materiału komórkowego i dostarczanie profili DNA". Nie przewidziano analogicznego przepisu co do odcisków palców. Wspomniany przepis obliguje państwo członkowskie, żeby na wniosek innego państwa członkowskiego i w związku z toczącym się dochodzeniem lub postępowaniem karnym pobrało i przeanalizowało materiał komórkowy danej osoby, a następnie przekazało uzyskany profil DNA temu innemu państwu członkowskiemu pod określonymi warunkami. Artykuł ten jest dość radykalny. Obliguje państwo członkowskie, żeby faktycznie pobierało (i analizowało) materiał biometryczny danej osoby, o ile jego pobranie i analiza są dopuszczalne w zapytującym państwie członkowskim (warunek b).

54. Przepis ten jest nie tylko radykalny, ale i niejasny. Po pierwsze, nie ogranicza wspomnianych działań do poważniejszych przestępstw, ani nawet do osób podejrzanych o popełnienie przestępstwa; po drugie, nakazuje, by spełnione były prawne wymogi zapytanego państwa członkowskiego (warunek c), ale nie określa, czego te wymogi miałyby dotyczyć. Zdaniem Europejskiego Inspektora Ochrony Danych artykuł ten należy doprecyzować, najlepiej przez skonkretyzowanie jego tekstu. Niezależnie od wszystkiego zasada proporcjonalności wymaga węższego rozumienia tego artykułu.

VII. **Przepisy ogólne o ochronie danych**

55. W niniejszej części opinii zostaną omówione następujące zagadnienia dotyczące ochrony danych:

— potrzeba przepisów ogólnych o ochronie danych w trzecim filarze,

— przykłady pokazujące, dlaczego mimo przepisów rozdziału 6 omawianej inicjatywy potrzebne są jeszcze przepisy ogólne,

— krótka analiza samego rozdziału 6.

([28]) Patrz opracowanie pt. „Analiza dotycząca konwencji z Prüm" (*Inquiry into the Prüm Convention*), które brytyjski inspektor dostępu do informacji (*Information Commissioner*) przekazał podkomisji F (do spraw wewnętrznych) działającej w ramach stałej komisji Izby Lordów ds. Unii Europejskiej (pkt 10 opracowania). „Zapobiegawczo" czyli po to, by wykluczyć siebie z kręgu osób podejrzanych o popełnienie przestępstwa.

([29]) Patrz np. orzeczenie z dnia 14 grudnia 2000 r., sygnatura: BvR 1741/99, w którym uznano, że korzystanie z próbek DNA w przypadku lżejszych przestępstw jest niezgodne z zasadą proporcjonalności.

([30]) Co do tego wariantu patrz art. 20 ust. 1 wniosku dotyczącego decyzji Rady w sprawie ustanowienia Europejskiego Urzędu Policji (Europolu) [COM(2006) 817 wersja ostateczna] oraz opinię Europejskiego Inspektora Ochrony Danych z dnia 16 lutego 2007 r. (pkt 26).

56. Na wstępie Europejski Inspektor Ochrony Danych pragnie zauważyć, że art. 1 omawianej inicjatywy podaje cel i jej zakres zastosowania, ale nie odsyła do rozdziału 6, chociaż planowana decyzja Rady zawiera rozdział o ochronie danych. Dlatego Europejski Inspektor Ochrony Danych zaleca umieszczenie takiego odesłania w tekście.

Potrzeba przepisów ogólnych

57. Jak już kilkakrotnie stwierdzono ([31]), zdaniem Europejskiego Inspektora Ochrony Danych istotne jest, aby konkretne akty prawne ułatwiające wymianę informacji do ochrony porządku publicznego — czyli takie, jak opiniowana właśnie inicjatywa w sprawie decyzji Rady — nie były przyjmowane, dopóki Rada nie przyjmie przepisów ogólnych o ochronie danych, które to przepisy zagwarantują odpowiedni poziom ochrony danych zgodnie z wnioskami przedstawionymi przez Europejskiego Inspektora Ochrony Danych w jego dwóch opiniach na temat projektu Komisji dotyczącego ramowej decyzji Rady w sprawie ochrony danych w trzecim filarze ([32]).

58. Ogólne przepisy o ochronie danych są *condicio sine qua non* wymiany danych osobowych między organami ochrony porządku publicznego, tak jak tego wymaga art. 30 ust. 1 lit. b) Traktatu o UE i jak to uznano w kilku dokumentach UE dotyczących polityki. W praktyce jednak akty ułatwiające wymianę danych są przyjmowane, zanim zostanie zagwarantowany odpowiedni poziom ochrony danych. Kolejność tę należy odwrócić.

59. Odwrócenie tej kolejności jest ważne także dlatego, że szczegółowe rozwiązania co do ochrony danych zawarte w omawianej inicjatywie mogą kolidować z przyszłymi, wciąż dyskutowanymi przepisami ogólnymi o ochronie danych w trzecim filarze. Poza tym nie jest to konstruktywne, by do wdrażania przepisów o ochronie danych zawartych w omawianej inicjatywie — która przewiduje zresztą uchwalenie standardów ochrony danych i procedur administracyjnych oraz wyznaczenie właściwych organów — przystępować, zanim nie przyjmie się decyzji ramowej o ochronie danych, która to decyzja może przewidywać odmienne wymogi, a tym samym wymagać zmiany już przyjętych przepisów krajowych.

60. Art. 25 ust. 1 opiniowanej inicjatywy odsyła obecnie do 108. konwencji Rady Europy, protokołu dodatkowego do niej z dnia 8 listopada 2001 r. i zalecenia nr R (87) 15 mówiących o wykorzystywaniu danych osobowych przez policję. Wspomniane akty Rady Europy powinny zapewnić minimalny poziom ochrony danych osobowych. Jednakże jak Europejski Inspektor Ochrony Danych zaznaczył już wcześniej ([33]), przywołana konwencja, która obowiązuje wszystkie państwa członkowskie, nie cechuje się konieczną precyzją, co już zauważono przy okazji przyjmowania dyrektywy 95/46/WE. Zalecenie to z natury rzeczy nie jest wiążące.

Przykłady ilustrujące potrzebę ogólnych przepisów mimo rozdziału 6

61. Po pierwsze, przepisy rozdziału 6 omawianej inicjatywy mają, w zamiarze legislatorów, nawiązywać do przepisów ogólnych o ochronie danych (patrz art. 25 inicjatywy). Należy je zatem traktować jako *lex specialis* dotyczące danych, których dostarczono na mocy omawianej decyzji Rady. Niestety obecne przepisy ogólne zawarte w 108. konwencji Rady Europy i związanych z nią aktach są niezadowalające. Już sam jednak zamiar legislatorów sugeruje, że potrzebne są odpowiednie przepisy ogólne ustalone w ramowej decyzji Rady. Nie jest to bynajmniej jedyny przykład pokazujący, że takie przepisy ogólne są potrzebne.

62. Po drugie, omawiana inicjatywa obejmuje tylko część procesów przetwarzania danych osobowych do ochrony porządku publicznego i tylko część procesów wymiany takich danych między państwami członkowskimi. Zakres rozdziału 6 ogranicza się z natury rzeczy do przetwarzania danych w związku z wymianą informacji przewidzianą w przedmiotowej inicjatywie. A zatem nie obejmuje on żadnych innych procesów wymiany innych informacji policyjnych i sądowych na mocy omawianej inicjatywy, a zwłaszcza informacji niezwiązanych z profilami DNA, odciskami palców czy danymi rejestracyjnymi pojazdów. Inny przykład pokazujący, jak fragmentaryczny jest zakres zastosowania rozdziału 6 omawianej inicjatywy, dotyczy dostępu — służącego ochronie porządku publicznego — do danych zgromadzonych przez firmy prywatne, skoro inicjatywa mówi o wymianie informacji między agencjami odpowiedzialnymi za prewencję kryminalną i wykrywanie przestępstw (art. 1 inicjatywy).

([31]) Najnowszy przykład: zobacz opinię Europejskiego Inspektora Ochrony Danych z dnia 16 lutego 2007 r. na temat wniosku dotyczącego decyzji Rady w sprawie ustanowienia Europejskiego Urzędu Policji (Europolu).

([32]) Opinia Europejskiego Inspektora Ochrony Danych z dnia 19 grudnia 2005 r. (Dz.U. C 47 z 25.2.2006, str. 27) i z dnia 29 listopada 2006 r., opublikowana na stronie internetowej Europejskiego Inspektora Ochrony Danych.

([33]) Zobacz na przykład (pierwszą) opinię na temat wniosku Komisji dotyczącego ramowej decyzji Rady w sprawie ochrony danych w trzecim filarze, pkt. 4

63. Po trzecie, jeżeli chodzi o zakres zastosowania przepisów rozdziału 6, tekst inicjatywy jest niejednoznaczny i stąd brak mu przejrzystości prawnej. Według art. 24 ust. 2 omawianej inicjatywy, przepisy tego rozdziału dotyczą danych, które są dostarczane lub zostały dostarczone na mocy przedmiotowej decyzji Rady. Zdaniem Europejskiego Inspektora Ochrony Danych dzięki takiemu sformułowaniu rozdział obejmuje bezpośredni dostęp do profili DNA, odcisków palców, danych rejestracyjnych pojazdów, a także szczególny przypadek określony w art. 7 omawianej inicjatywy ([34]). Nie ma też wątpliwości, że rozdział obejmuje też dostarczanie danych osobowych na mocy art. 14 (duże wydarzenia) oraz art. 16 (zapobieganie przestępstwom terrorystycznym).

64. Nie jest jednak jasne, czy rozdział 6 dotyczy tylko danych osobowych wymienianych lub wymienionych między państwami członkowskimi czy także materiału DNA i odcisków palców gromadzonych i przetwarzanych w państwie członkowskim na mocy art. 2 i 8 omawianej inicjatywy. Innymi słowy: czy rozdział 6 dotyczy danych osobowych, które zostały zgromadzone na mocy decyzji Rady, ale nie zostały (jeszcze) dostarczone organom innego państwa członkowskiego? Ponadto nie jest jasne, czy obejmuje on bardziej szczegółowe dane osobowe dostarczane, gdy stwierdzi się zgodność profili DNA lub odcisków palców; z jednej strony motyw 11 sugeruje, że dostarczanie bardziej szczegółowych informacji (w trybie procedur wzajemnej pomocy) mieści się w zakresie zastosowania decyzji Rady, z drugiej strony art. 5 i 10 mówią wyraźnie, że dostarczanie takich danych jest regulowane prawem krajowym. Na koniec należy zauważyć, że art. 24 ust. 2 mówi o sytuacji, w której rozdział 6 nie obowiązuje: jego przepisy mają zastosowanie, „o ile poprzednie rozdziały nie stanowią inaczej". Zdaniem Europejskiego Inspektora Ochrony Danych zastrzeżenie to pozbawione jest merytorycznej wartości (Europejski Inspektor Ochrony Danych nie zauważył żadnych kolidujących przepisów w poprzednich rozdziałach), ale mimo to może obniżać klarowność tekstu, jeżeli chodzi o stosowanie rozdziału 6.

65. Europejski Inspektor Ochrony Danych zaleca, żeby w art. 24 ust. 2 jasno określić, że rozdział 6 ma zastosowanie do gromadzenia i przetwarzania materiału DNA i odcisków palców w państwie członkowskim oraz obejmuje także dostarczanie bardziej szczegółowych danych osobowych w ramach omawianej decyzji. Ponadto należy skreślić zastrzeżenie: „o ile poprzednie rozdziały nie stanowią inaczej". Dzięki takim doprecyzowaniom przepisy rozdziału 6 będą miały istotne skutki.

66. Po czwarte, sam charakter przepisów rozdziału 6 o ochronie danych — w takim zakresie, w jakim przepisy te nawiązują do tradycyjnego rozumienia wzajemnej pomocy prawnej w sprawach karnych — pokazuje, że potrzebne są przepisy ogólne. Aby wymieniać informacje, potrzeba wcześniej w minimalnym stopniu zharmonizować podstawowe przepisy o ochronie danych albo przynajmniej nawzajem uznać swoje przepisy krajowe; dzięki temu współpraca nie straci na skuteczności przez różnice między przepisami państw członkowskich.

67. Chociaż omawiana inicjatywa przewiduje harmonizację w niektórych ważnych kwestiach prawa ochrony danych, to w innych ważnych kwestiach przepisy rozdziału 6 o ochronie danych nie harmonizują prawa krajowego ani nie nakazują jego wzajemnego uznawania. Odwołują się natomiast do równoczesnego obowiązywania (co najmniej) dwóch systemów prawnych: danych wolno najczęściej dostarczać tylko wtedy, gdy nie narusza to praw ani państwa członkowskiego dostarczającego danych, ani państwa członkowskiego je otrzymującego. Innymi słowy, w tych kwestiach opiniowana inicjatywa, zamiast współkształtować niepodzieloną granicami wewnętrznymi przestrzeń wolności, bezpieczeństwa i sprawiedliwości, umacnia tradycyjny system wzajemnej pomocy prawnej w sprawach karnych, oparty na suwerenności narodowej ([35]).

68. Zdaniem Europejskiego Inspektora Ochrony Danych rozdział 6 w swojej obecnej postaci nie ułatwia wymiany danych osobowych, a tylko dodatkowo ją komplikuje, zwłaszcza że inicjatywa służy objęciu wszystkich 27 państw członkowskich systemem konwencji z Prüm i że wspólne przepisy ogólne o ochronie danych nie zostały przyjęte. Na przykład art. 26 ust. 1 dopuszcza przetwarzanie danych w innych celach wyłącznie wtedy, gdy zezwala na to prawo krajowe zarówno państwa członkowskiego dostarczającego danych, jak i państwa członkowskiego je otrzymującego. Inny przykład to art. 28 ust. 3, który głosi, że dane osobowe, których nie należało dostarczać (ani przyjmować), się usuwa. Ale skąd otrzymujące je państwo członkowskie ma wiedzieć, że — w świetle prawa państwa członkowskiego ich dostarczającego — danych tych dostarczono bezprawnie? Taka sytuacja może rodzić trudne pytania, gdy kwestie te wynikną w sprawach rozpatrywanych przez sądy krajowe.

([34]) Patrz pkt 53 niniejszej opinii.

([35]) Patrz również motyw 11 omawianej inicjatywy, zgodnie z którym państwa członkowskie mają „występować o bardziej szczegółowe informacje w trybie procedur wzajemnej pomocy".

69. Po piąte, wspólne przepisy ogólne o ochronie danych są ważne, tym bardziej że między przepisami państw członkowskich są istotne różnice, zarówno w prawie karnym materialnym, jak i w prawie karnym procesowym. Różnice te mogą nie tylko mieć wpływ na współpracę między organami państw członkowskich, ale też bezpośrednio oddziaływać na osoby fizyczne w sytuacji, w której ich dane są wymieniane między organami w co najmniej dwóch państwach członkowskich. Na przykład mogą one w rzeczywistości nie dysponować we wszystkich państwach członkowskich takimi samymi środkami dochodzenia swoich praw.

70. Podsumowując: omawiana propozycja harmonizuje niektóre elementy wymiany danych między właściwymi organami i dlatego zawiera rozdział o ochronie danych, ale nie harmonizuje jednak wszystkich gwarancji ochrony danych. Jej przepisy nie są ani kompleksowe (a przepisy ogólne — *lex generalis* — takie być powinny), ani wyczerpujące (brakuje bowiem ważnych elementów, co zostanie wykazane w pkt 75).

71. Nie ulega wątpliwości, że w dziedzinach nieobjętych zakresem zastosowania inicjatywy potrzebne są wspólne przepisy ogólne o ochronie danych. Obywatele mają prawo liczyć na minimalny zharmonizowany poziom ochrony danych, bez względu na to, gdzie w Unii Europejskiej przetwarza się ich dane w celu ochrony porządku publicznego.

72. Ale takie wspólne przepisy są potrzebne także w dziedzinach objętych przedmiotową inicjatywą. Dotyczy ona bowiem m.in. gromadzenia, przetwarzania i wymiany danych biometrycznych, które potencjalnie wymagają ochrony, takich jak materiał DNA. Ponadto krąg osób objętych tym systemem nie ogranicza się do osób podejrzanych o (lub skazanych za) popełnienie określonego przestępstwa. W tej sytuacji tym bardziej należałoby oczekiwać przejrzystego i adekwatnego systemu ochrony danych.

73. Przy okazji należy powtórzyć, że zakres zastosowania przedmiotowej inicjatywy oraz jej rozdziału 6 nie jest jasno określony. Dlatego ze względu na bezpieczeństwo prawne ważne jest, aby dane osobowe były dobrze chronione, bez względu na to, czy i kiedy zakres zastosowania inicjatywy je obejmuje. Z tych samych powodów należy zagwarantować spójność między przepisami obowiązującymi w ramach zakresu zastosowania inicjatywy oraz poza nim.

Przepisy rozdziału 6

74. Przepisy rozdziału 6 o ochronie danych, zawarte w przedmiotowej inicjatywie, dotyczą danych dostarczanych lub dostarczonych na mocy odnośnej decyzji. Obejmują one wiele ważnych kwestii i zostały pieczołowicie sformułowane jako przepisy szczegółowe uzupełniające przepisy ogólne o ochronie danych. Europejski Inspektor Ochrony Danych stwierdza, że ogólnie rzecz biorąc, przepisy te zapewniają w swej istocie odpowiednią ochronę.

75. Jednakże do wcześniejszych uwag o kształcie przepisów rozdziału 6 Europejski Inspektor Ochrony Danych pragnie dodać, że dostrzegł inne usterki w przepisach rozdziału 6 ([36]):

— Art. 30, dotyczący rejestrowania czynności, ma zastosowanie jedynie do wymiany danych osobowych, ale już nie do dostępu do tych danych służącego ochronie porządku publicznego. Byłoby lepiej, gdyby artykuł ten został tak zredagowany, by wszystkie czynności wykonywane względem tych danych musiały być rejestrowane.

— W myśl art. 31 prawo osoby, której dane dotyczą, do informacji ogranicza się do prawa do otrzymania informacji na własny wniosek. Wymóg ten jest sprzeczny z podstawową zasadą ochrony danych, a mianowicie zasadą, że administrator danych udziela osobie, od której pobrano dane o niej samej, podstawowych informacji dotyczących ich pobrania i że osoba ta wcale nie musi o to specjalnie występować ([37]). Zresztą w wielu przypadkach osoba ta nawet nie będzie wiedziała, że dane o niej są gromadzone. Oczywiście wykonanie prawa do informacji można obwarować wyjątkami, warunkami i ograniczeniami, na przykład ze względu na dobro toczącego się dochodzenia karnego, ale w ten sposób nie wolno pozbawiać tego prawa jego merytorycznej wartości przez to, że rutynowo wymaga się od osoby, której dotyczą dane, by występowała z odnośnym wnioskiem ([38]).

([36]) W punkcie tym nie przedstawiono wyczerpującej liczby tych wad; wspomniano tylko najważniejsze z punktu widzenia ochrony danych.
([37]) Patrz na przykład art. 10 dyrektywy 95/46/WE (odesłanie w przypisie nr 25).
([38]) Europejski Inspektor Ochrony Danych zwraca uwagę, że art. 31 odsyła do dyrektywy 95/46/WE, gdy tymczasem w akcie dotyczącym trzeciego filaru logiczniejsze byłoby odesłanie do aktu prawnego obowiązującego w tym filarze, czyli w tym przypadku do protokołu do 108. konwencji Rady Europy.

— Rozdział 6 nie przewiduje rozróżniania danych według odrębnych kategorii osób (ofiar, podejrzanych czy innych osób, których dane są przechowywane w bazie). Takie rozróżnienie między kategoriami osób, oparte na charakterze udziału tych osób w popełnianiu przestępstwa, wprowadzono do wniosku Komisji dotyczącego ramowej decyzji Rady w sprawie ochrony danych w trzecim filarze; rozróżnienie to jest jeszcze ważniejsze w kontekście omawianej inicjatywy, gdyż pozwala przetwarzać dane — niekiedy szczególnie chronione — osób, które nie uczestniczą bezpośrednio w popełnianiu przestępstwa.

— Jedna uwaga pojawiła się już wcześniej: brak jest definicji danych osobowych ([39]).

76. Europejski Inspektor Ochrony Danych zaleca, żeby w celu usunięcia opisanych usterek Rada zmieniła tekst inicjatywy lub ujęła wspomniane elementy w ramowej decyzji Rady o ochronie danych w trzecim filarze. Zdaniem Europejskiego Inspektora Ochrony Danych rozwiązanie pierwsze nie musi wcale oznaczać modyfikowania samego systemu wymiany informacji ani nie jest ono sprzeczne z intencją 15 państw członkowskich, które wystąpiły z inicjatywą, by nie zmieniać najważniejszych części konwencji z Prüm.

VIII. **Wnioski**

77. W niniejszej opinii uwzględniono bezprecedensowy charakter przedmiotowej inicjatywy, a konkretniej fakt, że nie przewiduje się większych merytorycznych zmian w jej przepisach. Zmiany proponowane przez Europejskiego Inspektora Ochrony Danych służą głównie temu, by tekst poprawić, nie modyfikując przy tym samego systemu wymiany informacji.

78. Europejski Inspektor Ochrony Danych odnotowuje z zadowoleniem, że w przedmiotowej inicjatywie przyjęto ostrożne, stopniowe podejście do wdrażania zasady dostępności. Żałuje jednak, że inicjatywa nie harmonizuje zasadniczych elementów gromadzenia ani wymiany różnych rodzajów danych; harmonizacja taka zagwarantowałaby m.in. spełnienie zasady konieczności i proporcjonalności.

79. Europejski Inspektor Ochrony Danych z żalem stwierdza, że omawianą inicjatywę podjęto bez odpowiedniej oceny jej wpływu, i apeluje do Rady, aby dokonała takiej oceny podczas przyjmowania aktu i by rozpatrzyła w niej inne warianty działania, w miarę możliwości powodujące mniejszą ingerencję w życie prywatne.

80. Europejski Inspektor Ochrony Danych popiera przyjęte w inicjatywie podejście do różnych rodzajów danych osobowych: im większej ochrony dane wymagają, tym węższe jest ich wykorzystanie i tym bardziej ograniczony jest dostęp do nich.

81. Europejski Inspektor Ochrony Danych żałuje, że w opiniowanej inicjatywie nie wskazano kategorii osób, które byłyby ujęte w bazach danych DNA, i że nie ograniczono w niej okresu przechowywania ich danych.

82. Rada nie powinna przyjmować przedmiotowej decyzji Rady, dopóki nie przyjmie ramowej decyzji Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych i tym samym nie zapewni odpowiedniego poziomu ochrony.

83. Przepisy rozdziału 6 o ochronie danych, zawarte w inicjatywie, nie ułatwiają wymiany danych osobowych, a tylko dodatkowo ją komplikują tam, gdzie nawiązują one do tradycyjnego rozumienia wzajemnej pomocy prawnej w sprawach karnych.

84. Europejski Inspektor Ochrony Danych zaleca, żeby tekst inicjatywy zmieniono w następujący sposób:

— w art. 1 dodać odesłanie do rozdziału 6 o ochronie danych,

— dodać definicję niekodującej części DNA oraz przewidzieć procedurę gwarantującą, że ani obecnie, ani w przyszłości nie będzie można z części niekodującej uzyskać żadnych innych informacji,

— doprecyzować brzmienie art. 7, pamiętając, że zasada proporcjonalności wymaga węższego rozumienia tego artykułu,

([39]) Patrz pkt 42.

— dodać definicję danych osobowych w art. 24,

— w art. 24 ust. 2 określić, że rozdział 6 ma zastosowanie do gromadzenia i przetwarzania materiału DNA i odcisków palców w państwie członkowskim oraz obejmuje także dostarczanie bardziej szczegółowych danych osobowych w ramach omawianej decyzji,

— w art. 24 ust. 2 skreślić zastrzeżenie „o ile poprzednie rozdziały nie stanowią inaczej",

— art. 30 zmienić tak, by wszystkie czynności wykonywane względem tych danych musiały być rejestrowane,

— art. 31 zmienić tak, by osobie, której dane dotyczą, gwarantował prawo do informacji i nie wymagał występowania z odnośnym wnioskiem,

— w rozdziale 6 przewidzieć rozróżnianie danych według odrębnych kategorii osób (ofiar, podejrzanych czy innych osób, których dane są przechowywane w bazie),

— w art. 34 inicjatywy w sprawie decyzji Rady dodać zdanie w brzmieniu: „Przed przyjęciem takich przepisów wykonawczych Rada zasięga opinii Europejskiego Inspektora Ochrony Danych.",

— w rozdziale 7 inicjatywy dodać klauzulę o ocenie.

85. Europejski Inspektor Ochrony Danych zaleca ogólnie, żeby w celu usunięcia opisanych usterek Rada zmieniła tekst inicjatywy lub ujęła wspomniane elementy w ramowej decyzji Rady o ochronie danych w trzecim filarze. Zdaniem Europejskiego Inspektora Ochrony Danych rozwiązanie pierwsze (dotyczące elementów wymienionych w poprzednim punkcie) nie musi wcale oznaczać modyfikowania samego systemu wymiany informacji ani nie jest ono sprzeczne z intencją 15 państw członkowskich, które wystąpiły z inicjatywą, by nie zmieniać najważniejszych części konwencji z Prüm.

86. Na koniec, niniejsza opinia powinna zostać wymieniona w preambule do decyzji Rady.

Sporządzono w Brukseli, dnia 4 kwietnia 2007 r.

Peter HUSTINX

Europejski inspektor ochrony danych