EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Opinia Europejskiego Inspektora Ochrony Danych na temat wniosku dotyczącego decyzji Parlamentu Europejskiego i Rady w sprawie ustanowienia wieloletniego wspólnotowego programu ochrony dzieci korzystających z Internetu i z innych technologii komunikacyjnych

(2009/C 2/02)

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,

uwzględniając wniosek o opinię, który Komisja Europejska wystosowała na podstawie art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 i który wpłynął w dniu 4 marca 2008 r.,

WYDAJE NASTĘPUJĄCĄ OPINIĘ:

I. **WPROWADZENIE**

Konsultacje z Europejskim Inspektorem Ochrony Danych

1. W dniu 4 marca 2008 r. Komisja — zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 –przesłała Europejskiemu Inspektorowi Ochrony Danych z prośbą o konsultację wniosek dotyczący decyzji Parlamentu Europejskiego i Rady w sprawie ustanowienia wieloletniego wspólnotowego programu ochrony dzieci korzystających z Internetu i z innych technologii komunikacyjnych (zwany dalej „wnioskiem"). O konsultacjach tych należy wyraźnie wspomnieć w preambule decyzji.

Wniosek i jego kontekst

2. Nowy program wieloletni (zwany dalej „programem") ma stanowić kontynuację programu Bezpieczniejszy Internet (1999–2004) i Bezpieczniejszy Internet Plus (2005–2008).

3. Ma on służyć czterem celom:

   — ograniczeniu niezgodnych z prawem treści i przeciwdziałaniu szkodliwym zachowaniom w sieci,

   — promowaniu bezpieczniejszego środowiska on-line,

   — rozwijaniu świadomości społecznej,

   — tworzeniu bazy wiedzy.

4. Program z założenia ma być spójny z odpowiednimi strategiami, programami i działaniami Wspólnoty i ma je uzupełniać. Z uwagi na fakt, że istnieją już liczne regulacje służące ochronie dzieci w kontekście nowych technologii, program koncentruje się raczej na działaniach niż na nowych uregulowaniach. Kładzie nacisk na wydajność i skuteczność planowanych inicjatyw i na dostosowanie do rozwoju nowych technologii. Z uwagi na to przewiduje wzmożoną wymianę informacji i najlepszych wzorców.

5. Ponieważ program jest instrumentem ramowym, nie zawiera szczegółowego opisu planowanych działań, ale pozwala zapraszać do składania wniosków i ofert, które odpowiadają czterem wspomnianym wyżej celom.

Zakres opinii

6. Formułując cele ogólne programu, odniesiono się do ochrony dzieci korzystających z Internetu i z innych technologii komunikacyjnych, ale nie położono przy tym nacisku na aspekty prywatności ([3]). Europejski Inspektor Ochrony Danych — choć w pełni popiera założenia programu — chciałby w swojej opinii zwrócić uwagę właśnie na te aspekty.

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

([3]) Pewne odniesienia do prywatności można znaleźć w ocenie skutków regulacji (3.2.2. Szczególne zagrożenia: ujawnianie danych osobowych; 3.3. Grupy docelowe 5.2. Analiza skutków opcji polityki), ale nie są one szerzej omówione.

7. Europejski Inspektor Ochrony Danych uważa, że planowane inicjatywy zdecydowanie muszą być zgodne z obowiązującym prawodawstwem, które przywołano we wniosku ([1]), a zwłaszcza z dyrektywą 2000/31 o handlu elektronicznym, dyrektywą 2002/58 o prywatności i łączności elektronicznej oraz z dyrektywą 95/46 o ochronie danych ([2]).

8. Problem ochrony danych osobowych należy uwzględnić w odniesieniu do różnych aspektów programu i różnych zaangażowanych w niego podmiotów. Podstawowym zadaniem jest oczywiście ochrona danych dzieci, ale nie jest to zadanie jedyne: należy również mieć na uwadze dane osobowe, które wiążą się z osobami i treściami kontrolowanymi w celu ochrony dzieci.

9. Problemy te omówiono w niniejszej opinii w następujący sposób:

   — W części II szerzej przedstawiono związki pomiędzy ochroną danych a bezpieczeństwem dzieci; zwrócono uwagę na fakt, że ochrona osobowych danych dzieci jest nieodzowna, by zapewnić dzieciom większe bezpieczeństwo i zapobiec ich wykorzystywaniu.

   — W części III położono nacisk na fakt, że przetwarzanie danych osobowych nieodłącznie wiąże się także ze zgłaszaniem, filtrowaniem lub blokowaniem podejrzanych treści lub osób w Internecie:

      — w punkcie pierwszym przeanalizowano problem ochrony danych w kontekście zgłaszania podejrzanych osób lub faktów,

      — w punkcie drugim zwrócono uwagę na rolę narzędzi technicznych,

      — w punkcie trzecim omówiono obowiązki usługodawców związane z nadzorem nad danymi użytkowników i nad danymi dotyczącymi treści.

II. **OCHRONA DANYCH OSOBOWYCH A BEZPIECZEŃSTWO DZIECI**

10. Europejski Inspektor Ochrony Danych w pełni popiera założenia programu oraz cele służące zwiększeniu ochrony dzieci korzystających z Internetu. Działaniami decydującymi, które należy dalej rozwijać, są przede wszystkim ograniczanie szkodliwych lub niezgodnych z prawem treści oraz rozwijanie świadomości dzieci i innych zaangażowanych osób.

11. Europejski Inspektor Ochrony Danych chciałby przypomnieć, że bezpieczeństwo dzieci korzystających z Internetu zależy w pierwszej kolejności od tego, czy odpowiednio chronione są ich dane osobowe. Na tego rodzaju powiązanie prywatności i bezpieczeństwa dzieci wyraźnie zwrócono uwagę w niedawnej deklaracji Komitetu Ministrów o ochronie godności, bezpieczeństwa i prywatności dzieci korzystających z Internetu ([3]). W deklaracji przypomniano o prawie dzieci do godności oraz do szczególnej ochrony i opieki, które są niezbędne dla ich dobra, a także o prawie do „ochrony przed wszelkimi formami dyskryminacji albo arbitralną lub bezprawną ingerencją w sferę życia prywatnego oraz przed bezprawnymi zamachami na ich honor i reputację".

12. W deklaracji zwrócono uwagę na zagrożenia związane z ochroną prywatności dzieci, np. na możność śledzenia ich aktywności w Internecie, co może narażać je na działania przestępcze, takie jak nagabywanie w celach seksualnych lub inne bezprawne działania. Za potencjalnie niebezpieczne uznano także profilowanie i zatrzymywanie danych osobowych związanych z aktywnością dzieci, ponieważ dane te mogą być wykorzystywane np. do celów handlowych lub mogą być przeszukiwane przez instytucje edukacyjne bądź przez ewentualnych pracodawców. W deklaracji wezwano zatem do kasowania lub usuwania — w możliwie krótkim czasie — treści i śladów aktywności pozostawionych przez dzieci w Internecie, do opracowywania i upowszechniania wśród dzieci stosownych informacji, przede wszystkim o właściwym użytkowaniu narzędzi umożliwiających dostęp do informacji, a także do rozwijania zdolności krytycznej analizy treści oraz odpowiednich umiejętności komunikacyjnych.

13. Europejski Inspektor Ochrony Danych zgadza się z powyższymi wnioskami. Uważa, że przede wszystkim należy zwracać uwagę dzieci na zagrożenia związane ze spontanicznym podawaniem danych osobowych, np. prawdziwego imienia i nazwiska, wieku lub miejsca zamieszkania.

14. Działania proponowane w punkcie 3 ([4]) programu wieloletniego są specjalnie poświęcone rozwijaniu świadomości społecznej (wśród dzieci, rodziców, opiekunów i wychowawców) na temat możliwości i zagrożeń, z którymi wiąże się z korzystanie z technologii sieciowych, oraz na temat sposobów zachowania bezpieczeństwa w sieci. Spośród metod wskazanych we wniosku dwie są szczególnie użyteczne i powinny wyraźnie uwzględnić problem ochrony osobowych danych dzieci: rozpowszechnianie stosownych informacji oraz tworzenie punktów kontaktowych, w których rodzice i dzieci będą mogli się dowiedzieć o sposobach zachowania bezpieczeństwa w sieci.

15. Europejski Inspektor Ochrony Danych chciałby podkreślić, że odpowiednimi partnerami do działań w tym zakresie są organy ochrony danych. Należy o tym wspomnieć we wniosku, zwłaszcza w kontekście przewidywanych działań mających na celu promowanie współpracy oraz wymianę informacji, doświadczeń i najlepszych wzorców na szczeblu krajowym i europejskim ([5]).

([1]) Uzasadnienie: 2.1. Kontekst legislacyjny. Streszczenie oceny skutków regulacji: 1.2. Obecna sytuacja: prawodawstwo.

([2]) — Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (Dz.U. L 178 z 17.7.2000, s. 1);
— Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. L 201 z 31.7.2002, s. 37);
— Dyrektywa 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 (Dz.U. L 281 z 23.11.1995, s. 31).

([3]) Deklaracja przyjęta przez Komitet Ministrów w dniu 20 lutego 2008 r. podczas 1018. posiedzenia zastępców ministrów. Jest dostępna pod adresem wcd.coe.int/ViewDoc.jsp?Ref=Decl(20.02.2008)&Ver=0001

([4]) Załącznik 1, działania, pkt 3.

([5]) Załącznik 1, działania, pkt 1.

16. Jako przykład można podać kilka inicjatyw podjętych niedawno w tym zakresie w państwach członkowskich UE lub państwach członkowskich Europejskiego Obszaru Gospodarczego. Szwedzki Inspektor Ochrony Danych co roku przeprowadza badanie na temat stosunku młodzieży do Internetu i nadzoru; podobnie brytyjski ([1]) — przeprowadził on badanie skierowane do 2000 młodych ludzi w wieku 14–21 lat. Norweski Inspektor Ochrony Danych we współpracy z Ministerstwem Edukacji w styczniu 2007 r. zainaugurował kampanię edukacyjną skierowaną do szkół ([2]). W Portugalii Inspektor Ochrony Danych i Ministerstwo Edukacji podpisali protokół o promowaniu ochrony danych w Internecie, a zwłaszcza w serwisach społecznościowych ([3]). W wyniku tego projektu portugalskie serwisy społecznościowe zaczęły używać interfejsu i maskotki skierowanych do dzieci w wieku 10–15 lat.

17. Powyższe przykłady wskazują na aktywną i decydującą rolę organów ochrony danych w ochronie dzieci korzystających z Internetu; dowodzą także, że o organach tych należy wyraźnie wspomnieć w programie wieloletnim jako o partnerach do planowanych działań.

III. OCHRONA PRAW I DANYCH OSOBOWYCH INNYCH ZAANGAŻOWANYCH STRON

I. *Zgłoszenia i wymiana informacji*

18. W pierwszym punkcie wniosku („Ograniczanie niezgodnych z prawem treści i przeciwdziałanie szkodliwym zachowaniom w sieci" ([4])) jako jedno z głównych działań przewidziano tworzenie punktów kontaktowych, w których można będzie zgłaszać niezgodne z prawem treści oraz szkodliwe zachowania w sieci. Niewątpliwie, aby treści te i zachowania można było skutecznie zwalczać, należy informować o nich właściwe władze. Punkty kontaktowe związane z ochroną dzieci w istocie już utworzono; utworzono je także np. w celu walki ze spamem ([5]).

19. Europejski Inspektor Ochrony Danych zwraca jednak uwagę, że pojęcie „szkodliwa treść" jest niejasne: nie wyjaśniono, kto miałby je zdefiniować i na podstawie jakich kryteriów. Jest to niepokojące, zważywszy na skutki ewentualnego zgłaszania takich treści.

20. Ponadto jak już wspomniano, w przypadku programu takiego jak obecny chodzi nie tylko o dane osobowe dzieci, lecz także o dane wszystkich osób w jakikolwiek sposób związanych z informacjami dostępnymi w sieci. Może to być na przykład osoba podejrzana o niewłaściwe zachowanie i zgłoszona jako taka, ale również osoba zgłaszająca podejrzane zachowanie lub treść bądź osoba będąca ofiarą nadużyć. Choć informacje te są niezbędne, by system zgłoszeniowy działał skutecznie, Europejski Inspektor Ochrony Danych chciałby przypomnieć, że zawsze powinny być przetwarzane zgodnie z zasadami ochrony danych.

21. Niektóre dane mogą wymagać nawet specjalnej ochrony, jeżeli są danymi szczególnie chronionymi w rozumieniu art. 8 dyrektywy WE/95/46. Może być tak w przypadku danych związanych ze sprawcami naruszeń oraz z ofiarami nadużyć, zwłaszcza jeśli chodzi o pornografię dziecięcą. Należy zwrócić uwagę, że niektóre systemy zgłoszeniowe wymagały wprowadzenia zmian do krajowego ustawodawstwa o ochronie danych, tak by można było przetwarzać dane sądowe osób podejrzanych o przestępstwa lub dane ofiar ([6]). Europejski Inspektor Ochrony Danych nalega, by wszelkie systemy zgłoszeniowe, które powstaną, uwzględniały istniejące uregulowania związane z ochroną danych. O zgodności z uregulowaniami decydują: wzgląd na interes publiczny oraz gwarancja nadzoru nad systemem — zasadniczo ze strony organów ochrony porządku publicznego.

II. *Rola narzędzi technicznych w kontekście prywatności*

22. Jednym z rozwiązań, które mają pomóc w zwalczaniu niezgodnych z prawem treści i szkodliwych zachowań ([7]), są narzędzia techniczne. Przykłady takich narzędzi można znaleźć w ocenie skutków regulacji ([8]), są to: rozpoznawanie wieku, rozpoznawanie twarzy (w celu zidentyfikowania ofiar przez organy ochrony porządku publicznego) lub techniki filtrowania. Zgodnie z wnioskiem narzędzia te powinny być lepiej dostosowane do praktycznych potrzeb i dostępne dla odpowiednich zainteresowanych stron.

23. Europejski Inspektor Ochrony Danych zdecydowane opowiedział się już ([9]) za korzystaniem z nowych technologii w celu zwiększenia ochrony praw indywidualnych. Uważa on, że zasada domyślnej ochrony prywatności powinna stanowić nieodłączny element nowych rozwiązań technicznych, które wiążą się z przetwarzaniem danych osobowych. Dlatego zachęca do opracowywania projektów, które miałyby służyć tworzeniu rozwiązań technicznych w tym zakresie.

24. Szczególnie ważne jest, by opracować systemy, które do minimum ograniczą dostępność danych osobowych dzieci i tym samym zapewnią im rzetelną ochronę, oraz by dać dzieciom możliwość bezpieczniejszego korzystania z nowych narzędzi oferowanych przez społeczeństwo informacyjne, takich jak serwisy społecznościowe.

([1]) Zob. www.ico.gov.uk/youngpeople
([2]) Zob. www.dubestemmer.no
([3]) Zob. dadus.cnpd.pt
([4]) Załącznik 1 wniosku.
([5]) Zob. np. strona internetowa uruchomiona w tym celu przez władze belgijskie: www.ecops.be
([6]) Por. belgijska ustawa o ochronie danych z dnia 8 grudnia 1992 r., art. 3 ust. 6 związany z przetwarzaniem danych przez ośrodek zgłaszania dzieci zaginionych lub wykorzystanych seksualnie.
([7]) Załącznik 1, działania, pkt 1.
([8]) Ocena skutków regulacji, pkt 3.1.
([9]) Roczne sprawozdanie EIOD z 2006 r., cz. 3.5.1: „Zagadnienia techniczne".

25. Należy jednak pamiętać, że narzędzia techniczne — zależnie od sposobu, w jaki są stosowane — mogą mieć różnorodne skutki dla użytkowników. Jeżeli stosuje się je, by filtrować lub blokować informacje, można tym samym zablokować dzieciom dostęp do potencjalnie szkodliwych treści, ale można też utrudnić dostęp do legalnych informacji.

26. Choć największym problemem jest w tym kontekście swoboda dostępu do informacji, istnieje też problem związany z prywatnością. Filtrowanie, zwłaszcza w przypadku najnowszych rozwiązań związanych z zarządzaniem tożsamością, może wymagać zastosowania określonych kryteriów, w tym danych osobowych, takich jak wiek osoby korzystającej z serwisu (aby zapobiec dostępowi dorosłych lub dzieci do określonych treści), treść informacji i dane o aktywności w sieci osoby będącej autorem informacji. Zależnie od tego, w jaki sposób te informacje osobowe zostaną — automatycznie — przetworzone, dana osoba może ponieść konsekwencje związane z prawem do komunikowania się w Internecie.

27. Narzędzia filtrujące lub blokujące, które pozwalają kontrolować dostęp do serwisów, należy zatem stosować rozważnie, uwzględniając przy tym ewentualne niepożądane skutki i w pełni wykorzystując techniki pozwalające zwiększyć ochronę prywatności.

28. Europejski Inspektor Ochrony Danych z zadowoleniem przyjmuje zapis znajdujący się w ocenie skutków regulacji ([1]), który mówi, że żadne z proponowanych rozwiązań nie powinno naruszać prawa do prywatności ani wolności wyrażania opinii. Podziela również opinię wyrażoną w tej ocenie, a mianowicie, że jednym z głównych celów jest usamodzielnienie użytkowników, tj. umożliwienie im dokonywania lepszych wyborów i podejmowania odpowiednich działań, by chronić dzieci ([2]).

III. *Zadania usługodawców*

29. Za element niezbędny, by zwiększyć ochronę dzieci korzystających z technologii komunikacyjnych, uznano we wniosku współpracę wszystkich zainteresowanych stron. Przewidziano w nim ([3]) m.in. udział i zaangażowanie usługodawców — przede wszystkim stosowanie przez nich samoregulacji.

30. Usługodawcy z tego sektora, odpowiedzialnego za dostarczanie usług telekomunikacyjnych i treści, mogliby odegrać pewną rolę w zgłaszaniu, filtrowaniu lub blokowaniu informacji uznanych za niezgodne z prawem lub szkodliwe. W jakim zakresie można by im powierzyć to zadanie — w sensie prawnym — jest jednak dyskusyjne.

31. Współpraca ze strony usługodawców w celu rozwijania świadomości dzieci i innych zaangażowanych stron, np. rodziców czy wychowawców, jest oczywiście mile widziana. Do niezbędnych zadań dostawców treści należy także udostępnianie systemów ostrzegania i zatrudnianie moderatorów na stronach internetowych, co pozwala wykluczać niewłaściwe treści.

32. Jeżeli chodzi o dostawców usług *telekomunikacyjnych*, monitorowanie komunikacji jest jednak kwestią dyskusyjną, bez względu na to, czy ma na celu kontrolę treści chronionych prawami własności intelektualnej czy innych nielegalnych treści. Problem dotyczy możliwości ingerowania podmiotu komercyjnego, oferującego określoną usługę (telekomunikacyjną), w sferę, w którą zasadniczo ingerować nie powinien, tj. kontrolowania komunikowanych treści. Europejski Inspektor Ochrony Danych przypomina, że usługodawcy zasadniczo nie powinni sprawować takiej kontroli, a na pewno nie w sposób systematyczny. Jeżeli w szczególnych okolicznościach kontrola taka jest konieczna, powinna zasadniczo należeć do organów ochrony porządku publicznego.

33. W opinii z dnia 18 stycznia 2005 r. Grupa Robocza Art. 29 przypomniała w związku z tą kwestią ([4]), że „zgodnie z art. 15 dyrektywy 2000/31 o handlu elektronicznym nie można nałożyć na dostawców usług internetowych obowiązku systematycznego nadzoru ani współpracy. (…) Jak głosi art. 8 dyrektywy o ochronie danych, dane dotyczące przestępstw, wyroków skazujących lub środków bezpieczeństwa mogą być przetwarzane jedynie na restrykcyjnych warunkach wprowadzanych przez państwa członkowskie. Pojedyncze osoby mają oczywiście prawo przetwarzać dane sądowe w związku ze swoją sprawą sądową, jednak zasada ta nie umożliwia dogłębnego śledzenia, gromadzenia ani centralizacji danych osobowych przez strony trzecie, w tym zwłaszcza systematycznych badań na szeroka skalę, takich jak przeszukiwanie Internetu (…). Takie poszukiwania należą do zadań organów sądowych".

34. W dziedzinie, w której stawką są wolność słowa, dostęp do informacji, prywatność i inne prawa podstawowe, takie ingerencje podmiotów prywatnych skłaniają do pytań o proporcjonalność podejmowanych działań. Parlament Europejski przyjął niedawno rezolucję, w której podkreślił, że potrzebne jest rozwiązanie, które nie byłoby sprzeczne z prawami podstawowymi ([5]). W pkt 23 rezolucji stwierdzono, że „Internet jest szeroką platformą wyrazu kulturowego, dostępu do wiedzy i demokratycznego uczestnictwa w twórczości europejskiej, która zbliża pokolenia poprzez społeczeństwo informacyjne; [Parlament] wzywa zatem Komisję i państwa członkowskie, aby unikały przyjmowania środków sprzecznych ze swobodami obywatelskimi i prawami człowieka oraz z zasadami proporcjonalności, skuteczności i perswazji, takich jak przerywanie dostępu do Internetu".

([1]) Ocena skutków regulacji, pkt 5.2.

([2]) W tym sensie włączanie filtrów należałoby do rodziców, którzy mogliby je również wyłączać, co pozwoliłoby im na pełną kontrolę nad efektem filtrowania.

([3]) Motyw 8 preambuły; załącznik 1: pkt 1. 4.; streszczenie oceny skutków regulacji: pkt 3.1.

([4]) Dokument roboczy Grupy Roboczej Art. 29 ds. Ochrony Danych Związanych z Prawami Własności Intelektualnej, WP 104.

([5]) Rezolucja Parlamentu Europejskiego z dnia 10 kwietnia 2008 r. w sprawie przemysłu kulturalnego w Europie (2007/2153(INI)), pkt 23.

35. Europejski Inspektor Ochrony Danych jest zdania, że należy wyważyć proporcje między zasadnym celem, którym jest zwalczanie niezgodnych z prawem treści, a odpowiednim charakterem podejmowanych działań. Przypomina, że wszelki nadzór nad sieciami telekomunikacyjnymi, jeśli wymagają tego szczególne okoliczności, powinien być zadaniem organów ochrony porządku publicznego.

IV. **WNIOSKI**

36. Europejski Inspektor Ochrony danych popiera wniosek dotyczący wieloletniego programu mającego służyć ochronie dzieci korzystających z Internetu i z innych technologii komunikacyjnych. Z zadowoleniem przyjmuje fakt, że celem programu jest opracowywanie nowych technologii i przygotowywanie konkretnych działań, które mają zwiększyć skuteczność ochrony dzieci.

37. Europejski Inspektor Ochrony Danych przypomina, że zasadniczym warunkiem bezpieczeństwa dzieci korzystających z Internetu jest ochrona danych osobowych. Należy zapobiegać wykorzystywaniu osobowych danych dzieci, podejmując działania zaproponowane w programie, a zwłaszcza:

— rozwijając świadomość u dzieci i innych zaangażowanych stron, np. rodziców i wychowawców,

— propagując wypracowywanie najlepszych wzorców przez usługodawców,

— propagując opracowywanie narzędzi technicznych pozwalających respektować prywatność,

— sprzyjając wymianie najlepszych wzorców i doświadczeń pomiędzy odpowiednimi organami, w tym organami ochrony danych.

38. Działania te należy podejmować, nie zapominając o tym, że tam, gdzie chroni się dzieci, w grę mogą wchodzić także prawa innych osób. Wszelkie inicjatywy polegające na gromadzeniu, blokowaniu lub zgłaszaniu informacji należy podejmować wyłącznie z poszanowaniem praw podstawowych przysługujących wszystkim zaangażowanym osobom i zgodnie z uregulowaniami prawnymi dotyczącymi ochrony danych. Europejski Inspektor Ochrony Danych przypomina zwłaszcza, że nadzór nad sieciami telekomunikacyjnymi, jeżeli wymagają tego szczególne okoliczności, powinien być zadaniem organów ochrony porządku publicznego.

39. Europejski Inspektor Ochrony Danych odnotowuje, że przedmiotowy program stanowi ogólną podstawę do dalszych konkretnych działań. Sądzi, że niektóre uwagi poczynione w niniejszej opinii są jedynie wstępne i mogą zostać rozwinięte w praktyczny sposób, przez odwołanie do planowanych projektów, zgodnie z celami programu. Zaleca, by w wypracowywanie tych praktycznych projektów ściśle włączyć organy ochrony danych. Zwraca również uwagę na działania Grupy Roboczej Art. 29 poświęcone temu zagadnieniu, a zwłaszcza na obecne prace tej grupy dotyczące serwisów społecznościowych ([1]).

Sporządzono w Brukseli, dnia 23 czerwca 2008 r.

Peter HUSTINX

Europejski inspektor ochrony danych

([1]) Zob. dokument roboczy 1/2008 z dnia 18 lutego 2008 r. o ochronie osobowych danych dzieci (WP 147) oraz program prac grupy roboczej na lata 2008–2009, zawierający ogólne informacje m.in. o serwisach społecznościowych, dostępny pod adresem: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_en.htm