GRUPA ROBOCZA ARTYKUŁU 29 DS. OCHRONY DANYCH

01189/09/EN

WP 163

Opinia 5/2009 w sprawie portali społecznościowych

Przyjęta 12 czerwca 2009 r.

Niniejsza Grupa Robocza została powołana na mocy artykułu 29 Dyrektywy 95/46/WE. Jest to niezależny europejski organ doradczy w sprawach ochrony danych i prywatności. Jego zadania opisane zostały w artykule 30 Dyrektywy 95/46/WE i artykule 15 Dyrektywy 2002/58/WE.

Obsługę Sekretariatu zapewnia Dyrekcja C (Sądownictwo Cywilne, Prawa i Obywatelstwo) Komisji Europejskiej, Dyrekcja Generalna ds. Sprawiedliwości, Wolności i Bezpieczeństwa, B-1049 Bruksela, Belgia, Biuro nr LX-46 01/43.

Strona internetowa: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

Spis treści

Streszczenie

Niniejsza Opinia koncentruje się na kwestii, w jaki sposób działanie portali społecznościowych (SNS) ma sprostać wymogom ustawodawstwa o ochronie danych UE. Ma na celu przede wszystkim zapewnić wytyczne dla dostawców portali społecznościowych dotyczące środków, jakie muszą być stosowane w celu zapewnienia zgodności z prawem UE.

W Opinii stwierdza się, że dostawcy SNS oraz, w wielu przypadkach, dostawcy aplikacji będący stronami trzecimi są administratorami danych posiadającymi zobowiązania wobec użytkowników SNS. Opinia wskazuje, ilu użytkowników działa w sferze czysto osobistej, kontaktując się z osobami w ramach zarządzania swoimi sprawami osobistymi, rodzinnymi czy dotyczącymi gospodarstwa domowego. W takich przypadkach wedle Opinii ma zastosowanie 'wyłączenie do celów domowych', nie mają zaś zastosowania uregulowania dotyczące administratorów danych. Opinia określa także okoliczności, w których działania użytkownika SNS nie są objęte 'wyłączeniem do celów domowych'. Rozpowszechnianie i wykorzystywanie informacji dostępnych na SNS do innych wtórnych, niezamierzonych celów jest kluczową kwestią będącą przedmiotem zainteresowania Grupy Roboczej Artykułu 29. W całej Opinii zalecane są solidne domyślne ustawienia dotyczące bezpieczeństwa i ochrony prywatności jako idealny punkt wyjścia w odniesieniu do wszystkich oferowanych usług. Kluczowym przedmiotem zainteresowania jest dostęp do informacji w profilu. Poruszone są także tematy, takie jak przetwarzanie danych szczególnie chronionych i obrazów, reklama i marketing bezpośredni na SNS oraz kwestie przechowywania danych.

Kluczowe zalecenia dotyczą zobowiązania dostawców SNS do zapewnienia zgodności z dyrektywą o ochronie danych oraz do przestrzegania i umacniania praw użytkowników. Niezwykle istotne jest, aby dostawcy SNS od samego początku informowali użytkowników o swojej tożsamości oraz wskazali wszystkie cele, w których przetwarzają dane osobowe. Dostawcy SNS powinni zachować szczególną ostrożność przy przetwarzaniu danych osobowych osób niepełnoletnich. Wedle zaleceń zawartych w Opinii użytkownicy powinni umieszczać na portalu zdjęcia lub informacje na temat innych osób tylko za ich zgodą, a SNS mają również obowiązek informowania użytkowników na temat praw do ochrony prywatności innych osób.

GRUPA ROBOCZA DS. OCHRONY OSÓB FIZYCZNYCH W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

powołana na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. [1],

uwzględniając art. 29 i 30 ust. 1 lit. a) i ust. 3 niniejszej dyrektywy oraz art. 15 ust. 3 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r.,

uwzględniając art. 255 Traktatu WE i rozporządzenie (WE) nr 1049/2001 Parlamentu Europejskiego i Rady z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji,

uwzględniając własny regulamin wewnętrzny,

PRZYJMUJE NINIEJSZY DOKUMENT:

1. WPROWADZENIE

Rozwój społeczności internetowych oraz usług dostarczanych przez firmy hostingowe (*hosted services*) takich jak portale społecznościowe (SNS) to zjawisko stosunkowo nowe, a liczba użytkowników takich stron wciąż zwiększa się w postępie wykładniczym.

Dane osobowe zamieszczane przez użytkowników on-line wraz z informacjami określającymi działania i interakcje użytkowników z innymi osobami tworzą bogaty profil prezentujący działania i zainteresowania danej osoby. Dane osobowe publikowane na SNS mogą być wykorzystywane przez strony trzecie do szeregu różnorodnych celów, w tym celów komercyjnych, i mogą skutkować istotnymi zagrożeniami takimi jak kradzież tożsamości, strata finansowa, utrata możliwości rozwoju firmy lub szans zawodowych oraz szkoda fizyczna.

Berlińska Grupa Robocza ds. Ochrony Danych w Sektorze Telekomunikacji przyjęła w marcu 2008 r. *Memorandum z Rzymu*[2]. Dokument ten poświęcony jest zagrożeniom dla prywatności i bezpieczeństwa, jakie mogą stwarzać portale społecznościowe oraz zawiera wytyczne dla organów regulacyjnych, dostawców i użytkowników. Przyjęta ostatnio Rezolucja w sprawie Ochrony Prywatności na Portalach Społecznościowych[3] jest również poświęcona wyzwaniom stwarzanym przez SNS. Grupa Robocza wzięła również pod rozwagę opracowanie opublikowane w październiku 2007 r. przez Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA): Stanowisko w sprawie *„Kwestii bezpieczeństwa i zaleceń dla internetowych portali*

---

[1] Dziennik Urzędowy nr L281 z 23.11.1995, s. 31
, http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

[2] http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf

[3] Przyjęta 17.10. 2008 r. podczas XXX Międzynarodowej Konferencji Organów Ochrony Danych i Prywatności w Strasburgu,
http://www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_social_networks_en.pdf

społecznościowych"[4] skierowane do organów regulacyjnych i dostawców portali społecznościowych.

2. Definicja portalu społecznościowego (SNS) i model biznesowy

SNS można ogólnie zdefiniować jako internetową platformę komunikacyjną umożliwiającą osobom dołączenie do grupy lub stworzenie sieci podobnie myślących użytkowników. W znaczeniu prawnym, portale społecznościowe są usługami społeczeństwa informacyjnego w rozumieniu art. 1 ust. 2 dyrektywy 98/34/WE zmienionym dyrektywą 98/48/WE. SNS posiadają pewne cechy wspólne:

- użytkownicy są zachęcani do podawania swoich danych osobowych w celu stworzenia własnego opisu lub 'profilu';

- SNS są również narzędziem, które umożliwia użytkownikom zamieszczanie swoich materiałów (treści wygenerowanych przez użytkownika, takich jak zdjęcie lub zapiski z pamiętnika, muzyka lub wideoklip bądź linki do innych stron internetowych[5]);

- możliwe jest tworzenie sieci znajomych z wykorzystaniem narzędzi, które pozwalają każdemu użytkownikowi stworzyć listę kontaktów – osób, z którymi użytkownik ma możliwość interakcji.

Większość zysków związanych z SNS pochodzi z reklam wyświetlanych na stronach tworzonych lub odwiedzanych przez użytkowników. Użytkownicy, którzy zamieszczają w profilach dużo informacji o swoich zainteresowaniach, stanowią dobry rynek dla reklamodawców, którzy chcą skierować do określonych użytkowników reklamy w oparciu o te informacje.

Dlatego ważne jest, aby SNS działały z poszanowaniem praw i wolności użytkowników, którzy w sposób uprawniony i uzasadniony mogą oczekiwać, że udostępnione przez nich dane osobowe będą przetwarzane zgodnie z europejskimi i krajowymi przepisami o ochronie danych osobowych i prywatności.

3. Zastosowanie dyrektywy o ochronie danych

Przepisy dyrektywy o ochronie danych mają zastosowanie do dostawców wyszukiwarek w większości przypadków, nawet wówczas gdy siedziba dostawcy znajduje się poza obszarem EOG. W zakresie dalszych wytycznych dotyczących kwestii siedziby i wykorzystywania środków, czyli wyznaczników zastosowania dyrektywy o ochronie danych oraz zasad, które mogą być wykorzystane w związku z przetwarzaniem adresów IP i wykorzystywaniem plików cookies Grupa Robocza Artykułu 29 odwołuje się do swojej poprzedniej opinii w sprawie wyszukiwarek.[6]

3.1 Kto jest administratorem danych?

Dostawcy SNS

---

[4] http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

[5] W przypadkach, gdy SNS zapewniają usługi komunikacji elektronicznej, zastosowanie mają także przepisy dyrektywy o prywatności i łączności elektronicznej 2002/58.

[6] WP148, „Opinia 1/2008 dotycząca zagadnień ochrony danych związanych z wyszukiwarkami".

Zgodnie z dyrektywą o ochronie danych administratorami danych są dostawcy SNS. Zapewniają oni środki przetwarzania danych użytkownika oraz wszystkie ”podstawowe” usługi związane z zarządzaniem kontem użytkownika (np. rejestracja i usuwanie kont). Dostawcy SNS określają również, w jaki sposób działania reklamowe i marketingowe mogą być wykorzystane w celach reklamowych i marketingowych, w tym reklamie zapewnianej przez strony trzecie.

Dostawcy aplikacji

Dostawcy aplikacji mogą być również administratorami danych, o ile opracowują aplikacje dodatkowe poza tymi z SNS, a użytkownicy mogą dowolnie zdecydować o wykorzystaniu takich aplikacji.

Użytkownicy

W większości przypadków użytkowników uważa się za osoby, których dane dotyczą. Dyrektywa nie nakłada obowiązków administratora danych na osobę fizyczną, która przetwarza dane osobowe „w ramach czynności o czysto osobistym lub domowym charakterze” – tzw. „wyłączenie do celów domowych”. Istnieją jednak sytuacje, w których działalność użytkownika SNS nie jest objęta takim wyłączeniem, i uznaje się, że użytkownik przejmuje część obowiązków administratora danych. Niektóre z tych sytuacji zostały omówione poniżej:

3.1.1. Cel i charakter

Wśród SNS można zauważyć rosnącą tendencję, jeśli chodzi o *„przejście od „Web 2.0 dla zabawy” do „Web 2.0 dla wydajności i usług”*[7], gdzie działania niektórych użytkowników SNS wykraczają poza czynności o czysto osobistym lub domowym charakterze, na przykład jeśli wykorzystują oni portal jako platformę współpracy dla stowarzyszenia lub firmy. Jeżeli użytkownik SNS działa w imieniu stowarzyszenia lub firmy, lub wykorzystuje SNS głównie do celów reklamowych, politycznych lub charytatywnych, wyłączenie nie ma zastosowania. W takich przypadkach użytkownik w pełni przejmuje zobowiązania administratora danych udostępniającego dane innemu administratorowi (SNS) i stronom trzecim (inni użytkownicy SNS, a potencjalnie również inni administratorzy posiadający dostęp do danych). W takich okolicznościach użytkownik musi uzyskać zgodę zainteresowanych osób, których dane dotyczą, lub wykazać inną podstawę prawną na mocy dyrektywy.

Zwykle dostęp do danych (dane profili, posty, opowiadania…) zamieszczonych przez użytkownika jest ograniczony do grona zaproszonych przez niego znajomych, jednak zdarza się, że użytkownicy mają wielu znajomych również pośród osób trzecich, których części mogą w rzeczywistości nie znać. Większa liczba znajomych może wskazywać, że wyłączenie do celów domowych nie ma zastosowania i w rezultacie użytkownika można uznać za administratora danych.

3.1.2. Dostęp do danych zawartych w profilu

SNS powinny zapewniać ustawienia początkowe, które będą przyjazne dla ochrony prywatności i nieodpłatne oraz będą ograniczały dostęp do grona zaproszonych przez użytkownika znajomych.

[7] „Internet przyszłości: „Europa musi być kluczowym graczem” – przemówienie pani Reding, Europejskiej Komisarz ds. Społeczeństwa Informacyjnego i Mediów wygłoszone podczas spotkania Rady Lizbońskiej w ramach inicjatywy „Przyszłość Internetu” w dniu 2 lutego 2009 r.

Jeśli dostęp do danych zawartych w profilu mają osoby spoza grona znajomych, na przykład jeśli dostęp do profilu zapewniany jest dla wszystkich członków w ramach SNS[8] lub gdy dane są indeksowane przez wyszukiwarki, dostęp wykracza poza sferę osobistą i domową. Podobnie, jeśli użytkownik podjął świadomą decyzję o nieograniczaniu dostępu do grona znajomych, zaczynają obowiązywać obowiązki administratora danych. Będą miały zastosowanie te same zasady prawne, co w przypadku wykorzystania przez osobę innych środków technicznych do publikacji danych osobowych w sieci[9]. W kilku państwach członkowskich brak ograniczeń dostępu (czyli charakter publiczny) powoduje objęcie dyrektywą o ochronie danych pod względem nałożenia na użytkownika Internetu zobowiązań administratora danych[10].

Należy również pamiętać, że nawet jeśli nie ma zastosowania wyłączenie dla czynności o czysto osobistym lub domowym charakterze, wobec użytkownika SNS mogą mieć zastosowanie inne wyłączenia, np. do celów dziennikarskich, artystycznych lub literackich. W takich przypadkach konieczne jest znalezienie równowagi między wolnością wypowiedzi i prawem do prywatności.

3.1.3. Przetwarzanie danych osób trzecich

Wyłączenie dla czynności o czysto osobistym lub domowym charakterze jest również poważnie ograniczone przez konieczność ochrony praw stron trzecich, zwłaszcza jeśli w grę wchodzą dane szczególnie chronione. Należy ponadto podkreślić, że nawet jeśli wyłączenie ma zastosowanie, użytkownicy mogą ponosić odpowiedzialność za pogwałcenie ogólnych przepisów krajowego prawa cywilnego lub karnego (np. zniesławienie, odpowiedzialność deliktowa za naruszenie praw osobistych, odpowiedzialność karna).

3.2 Bezpieczeństwo i domyślne ustawienia dotyczące ochrony prywatności.

Bezpieczeństwo przetwarzania informacji jest kluczowym elementem zapewniającym zaufanie do SNS. Administratorzy danych muszą przyjąć odpowiednie środki techniczne i organizacyjne „zarówno podczas projektowania systemów przetwarzania, jak i w czasie samego przetwarzania" w celu utrzymania bezpieczeństwa i zapobieżenia przetwarzaniu przez osoby nieuprawnione, z uwzględnieniem zagrożeń, jakie mogą wynikać z przetwarzania lub charakteru danych[11].

Istotnym elementem ustawień dotyczących ochrony prywatności jest dostęp do danych osobowych zamieszczanych w profilu. Jeżeli nie ma żadnych ograniczeń dostępu do takich danych, wówczas osoby trzecie mogą dotrzeć do wszelkiego rodzaju intymnych informacji o użytkowniku, jako członek SNS lub za pośrednictwem wyszukiwarek internetowych. Jednak jedynie niewielka liczba użytkowników zarejestrowanych na portalu wprowadza zmiany w ustawieniach początkowych. W związku z tym SNS muszą zaoferować przyjazne dla użytkownika ustawienia domyślne dotyczące dostępu do

[8] Lub gdy można dowieść, że faktycznie nie jest dokonywana selekcja przy akceptacji nowych znajomych, tj. użytkownicy akceptują 'znajomych' niezależnie od relacji, jakie z nimi posiadają.

[9] Takich jak platformy inne niż SNS, lub z wykorzystaniem niezależnego oprogramowania.

[10] Europejski Trybunał Sprawiedliwości nie podzielił tej opinii w werdykcie w sprawie Satamedia (ust. 44): *„W rezultacie wcześniej wskazane wyłączenie należy interpretować jako odnoszące się tylko do działań, które są prowadzone w ramach życia prywatnego lub rodzinnego osób (patrz sprawa Lindqvist, ust. 47). Ewidentnie nie ma to zastosowania do działań Marrkinapörssi i Satamedia, których celem jest udostępnienie zgromadzonych danych nieograniczonej liczbie osób".*

[11] Artykuł 17 i motyw 46 dyrektywy o ochronie danych.

informacji zawartych w profilu użytkownika. Użytkownik powinien swobodnie i wyraźnie zadecydować o udzieleniu zgody na dostęp do swojego profilu dla osób innych niż wskazanych przez samego użytkownika, aby zmniejszyć ryzyko niezgodnego z prawem przetwarzania przez strony trzecie. Profile o ograniczonym dostępie nie mogą być możliwe do odnalezienia przez wewnętrzne wyszukiwarki, w tym nie powinno być możliwe wyszukiwanie wedle parametrów, takich jak wiek czy lokalizacja. Decyzja o rozszerzeniu dostępu nie może być dorozumiana[12], na przykład poprzez tryb „opt-out" zastosowany przez administratora portalu społecznościowego.

3.3 Informacje, które musi podać SNS

Dostawcy SNS muszą informować użytkowników o swej tożsamości oraz o celach, dla których wykorzystują dane zgodnie z przepisani Art. 10 dyrektywy o ochronie danych, w tym (ale nie jedynie) o:

- wykorzystaniu danych do celów marketingu bezpośredniego,

- możliwości przekazywania danych do pewnych kategorii stron trzecich,

- przeglądzie profili: ich tworzeniu oraz głównych źródłach danych,

- wykorzystaniu danych szczególnie chronionych.

Grupa Robocza zaleca, by:

- dostawcy SNS ostrzegali użytkowników o zagrożeniach dla prywatności, jakie dla nich i innych niesie ze sobą publikacja danych na portalu;

- powinni przypominać użytkownikom, że zamieszczanie informacji o innych osobach może naruszać prawo tych osób do ochrony danych i prywatności.

- SNS powinny informować użytkowników, że jeśli zamierzają publikować zdjęcia lub informacje o innych osobach na swoim profilu, wymaga to zgody osoby[13].

3.4 Dane szczególnie chronione.

Dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych, jak również dane dotyczące stanu zdrowia i życia płciowego są danymi szczególnie chronionymi. Dane szczególnie chronione mogą być umieszczone w Internecie tylko na podstawie wyraźnej

---

[12] Raport i Wytyczne w sprawie Prywatności na Portalach Społecznościowych („Memorandum z Rzymu") wskazuje zagrożenia takie jak "Błędne pojęcie społeczności" s. 2, „Rozdajesz więcej informacji na swój temat niż się Tobie wydaje", s.3. Firma zajmująca się bezpieczeństwem komputerowym ostrzegła SNS przed domyślnym ustawieniem dostępu umożliwiającym taki dostęp użytkownikom z tej samej lokalizacji geograficznej: http://www.sophos.com/pressoffice/news/articles/2007/10/facebook-network.html

[13] Można to ułatwić wprowadzając na portalach społecznościowych narzędzia służące do oznaczania (tzw. tagging management tools), np. udostępniając w profilu osoby miejsce, w którym można wskazać obecność nazwy użytkownika na oznaczonych zdjęciach lub filmach wideo czekających na zgodę, bądź ustalając okres, po upływie którego oznaczenia, które nie otrzymały zgody osoby, tracą ważność.

zgody osoby, której dane dotyczą, lub jeżeli osoba, której dane dotyczą, udostępniła je w sposób oczywisty.[14]

W niektórych państwach członkowskich UE wizerunek osób, których dane dotyczą, jest uznawany za szczególną kategorię danych osobowych, ponieważ może być wykorzystany dla odróżnienia osoby na podstawie pochodzenia rasowego/etnicznego lub wyciągnięcia wniosków na temat jej przekonań religijnych lub stanu zdrowia. Grupa Robocza zasadniczo nie uważa zdjęć w Internecie za dane szczególnie chronione[15], chyba że są one w sposób wyraźny wykorzystywane w celu ujawnienia danych szczególnie chronionych widocznych na nich osób.

Jako administratorzy danych SNS nie mogą przetwarzać żadnych danych szczególnie chronionych na temat członków SNS lub osób niebędących ich członkami bez ich wyraźnej zgody[16]. Jeżeli SNS zamieszcza w formularzu profilu użytkowników jakiekolwiek pytania dotyczące danych szczególnie chronionych, SNS musi bardzo wyraźnie wskazać, że odpowiedź na takie pytania jest absolutnie dobrowolna.

3.5 Przetwarzanie danych użytkowników niebędących członkami portali

Wiele SNS pozwala użytkownikom zamieszczać dane dotyczące innych osób przez dodawanie imion na zdjęciach, ocen, list „osób, które spotkaliśmy/chcemy spotkać" podczas imprez. Dodawanie takich informacji może również przyczynić się do identyfikacji osób niebędących członkami portali. Jednak przetwarzanie takich danych osób niebędących członkami portali przez SNS może być prowadzone tylko, gdy spełnione jest jedno z kryteriów określonych w artykule 7 dyrektywy o ochronie danych.

Brak podstaw legalnego przetwarzania dotyczy również tworzenia profili osób niebędących członkami portalu poprzez agregację danych zamieszczanych niezależnie przez użytkowników SNS, włącznie z danymi o kontaktach pobranymi z wgranych książek adresowych.[17]

Nawet, jeśli SNS dysponują możliwością skontaktowania się z takimi osobami i poinformowania ich o posiadaniu związanych z nimi danych osobowych, wysłanie drogą e-mailową zaproszenia do SNS, aby zyskać dostęp do tych danych, pogwałciłoby zakaz ustanowiony w Art. 13 ust. 4 dyrektywy o prywatności i łączności elektronicznej, dotyczący przesyłania niezamówionych wiadomości elektronicznych dla celów marketingu bezpośredniego

3.6 Dostęp przez osoby trzecie.

---

[14] Państwa członkowskie mogą określać wyłączenia od tej zasady; patrz artykuł 8 ust. 2 lit. (a) oraz artykuł 8 ust. 4 dyrektywy o ochronie danych.

[15] Publikowanie zdjęć w Internecie zwiększa jednak rosnące obawy co do ochrony prywatności, wraz z ulepszaniem technologii rozpoznawania twarzy.

[16] Zgoda musi być dobrowolna, świadoma i wyraźna.

[17] Motyw 38 dyrektywy o ochronie danych precyzuje: "*Jeżeli przetwarzanie danych ma być rzetelne, osoba, której dane dotyczą musi mieć możliwość dotarcia do informacji o wystąpieniu czynności przetwarzania danych oraz, jeżeli dane są uzyskane od niej, musi otrzymać dokładne i pełne informacje uwzględniające okoliczności pozyskania danych.*". Dla niektórych SNS publikacja profili osób niebędących członkami portalu stała się przypuszczalnie istotnym sposobem wprowadzania na rynek swoich „usług".

3.6.1 Dostęp za pośrednictwem portali społecznościowych

Poza główną usługą SNS większość SNS oferuje użytkownikom dodatkowe aplikacje, tworzone przez osoby trzecie, które również przetwarzają dane osobowe.

SNS powinny mieć środki pozwalające zapewnić, że aplikacje stron trzecich będą zgodne z dyrektywą o ochronie danych oraz dyrektywą o prywatności i łączności elektronicznej. Oznacza to w szczególności, że mają dostarczać użytkownikom jasnych i konkretnych informacji na temat przetwarzania dotyczących ich danych osobowych i mieć dostęp jedynie do niezbędnych danych osobowych. Dlatego też dla dostawców aplikacji – stron trzecich należałoby wprowadzić dostęp modułowy, tak aby mogły one wybrać znacznie bardziej ograniczony sposób dostępu. SNS muszą ponadto w prosty sposób zapewnić użytkownikom możliwość zgłaszania wątpliwości dotyczących aplikacji.

3.6.2 Dostęp osób trzecich za pośrednictwem użytkowników

W niektórych przypadkach SNS dają użytkownikom możliwość dostępu do ich danych oraz uaktualniania tych danych poprzez inne aplikacje. Na przykład użytkownicy mogą:

- odczytywać i wysyłać wiadomości do sieci z telefonów komórkowych,
- synchronizować dane kontaktowe swoich znajomych z SNS z książką adresową w komputerze.
- uaktualniać automatycznie swój status oraz położenie na portalu społecznościowym korzystając z innej strony internetowej.

SNS publikują informacje na temat tego, jak można napisać tego rodzaju oprogramowanie w postaci „Interfejsów Programowania Aplikacji" („API"). Pozwala to osobom trzecim na napisanie oprogramowania, które będzie pełniło tego rodzaju funkcje, a użytkownicy mogą dowolnie wybrać dostawcę będącego osobą trzecią[18]. Oferując API umożliwiające dostęp do danych kontaktowych SNS powinny:

- zapewnić odpowiedni stopień szczegółowości umożliwiający użytkownikowi dokonanie wyboru poziomu dostępu dla osób trzecich, który byłby wystarczający do wykonania określonego zadania.

Uzyskując dostęp do danych osobowych poprzez API w imieniu użytkownika SNS osoby trzecie mają obowiązek:

- przetwarzać i przechowywać dane nie dłużej niż jest to niezbędne dla wykonania określonego zadania,
- nie wykonywania innych operacji na importowanych danych kontaktowych użytkownika, za wyjątkiem tych, które mieszczą się w zakresie osobistego wykorzystania przez użytkownika, który te dane dostarczył.

3.7 Podstawy prawne dla marketingu bezpośredniego.

[18] "API" jest szerokim pojęciem technicznym, dlatego też na potrzeby niniejszej opinii należy rozumieć je jako dostęp poprzez API w imieniu użytkownika np. użytkownik musi podać oprogramowaniu swoje dane uwierzytelniające podczas logowania, aby program mógł działać w imieniu użytkownika.

Marketing bezpośredni jest istotną częścią modelu biznesowego SNS, które mogą wykorzystywać różne rodzaje marketingu – niezależnie od tego, marketing z wykorzystaniem danych osobowych użytkowników winien być prowadzony zgodnie z odpowiednimi przepisami dyrektywy o ochronie danych i dyrektywy o prywatności i łączności elektronicznej.[19]

Marketing kontekstowy dopasowuje się do treści, które ogląda lub do których ma dostęp użytkownik[20].

Marketing segmentacyjny pozwala na dostarczanie reklam danym grupom użytkowników[21]; użytkownik jest umieszczany w grupie na podstawie informacji bezpośrednio podanych przez niego SNS[22].

Z kolei *marketing behawioralny* tworzy reklamy oparte na obserwacji i analizie zachowań użytkownika na przestrzeni czasu. Techniki te mogą podlegać różnym wymogom prawnym, w zależności od ich cech i od odpowiedniej podstawy prawnej. Grupa Robocza Artykułu 29 zaleca nieużywanie danych szczególnie chronionych do tworzenia modeli reklamy behawioralnej, o ile nie zostaną spełnione wszystkie warunki przewidziane prawem.

Niezależnie od zastosowanego modelu lub kombinacji modeli, reklamy mogą być podawane bezpośrednio poprzez SNS (który odgrywa tu rolę pośrednika) lub przez reklamodawców będących stronami trzecimi. W pierwszym z tych przypadków nie ma potrzeby ujawniania danych osobowych użytkowników stronom trzecim. W drugim reklamodawca będący stroną trzecią może przetwarzać dane osobowe użytkowników, np. gdy przetwarza ich adresy IP i pliki cookie umieszczone na ich komputerach.

3.8 Przechowywanie danych.

SNS nie wchodzą w zakres definicji usług komunikacji elektronicznej zawartej w artykule 2 lit. c dyrektywy ramowej (2002/21/WE). Dostawcy portali społecznościowych mogą jednak oferować usługi dodatkowe, które będą objęte zakresem pojęcia usług komunikacji elektronicznej, takie jak np. powszechnie dostępne usługi poczty elektronicznej, które będą podlegały przepisom dyrektywy o prywatności i łączności elektronicznej i dyrektywy o zatrzymywaniu danych.

Niektóre portale społecznościowe umożliwiają użytkownikom wysyłanie zaproszeń do osób trzecich. Zakaz wykorzystywania poczty elektronicznej dla celów marketingu bezpośredniego nie dotyczy komunikatów prywatnych. Następujące kryteria muszą być spełnione przez SNS, aby wyłączenie dotyczące komunikatów prywatnych było uprawnione:

- nie zachęca się do tego ani nadawcy ani odbiorcy,
- dostawca nie wybiera odbiorców komunikatu [23]

---

[19] W najbliższej przyszłości Grupa Robocza zamierza zająć się różnymi aspektami reklam online w odrębnym dokumencie.

[20] Na przykład jeśli na wyświetlanej stronie występuje słowo „Paryż", wyświetlać mogłaby się reklama restauracji z tego miasta.

[21] Każda grupa jest określona szeregiem kryteriów.

[22] Np. gdy zarejestrował się w usłudze.

[23] Np. zabroniona jest praktyka stosowana przez niektóre SNS polegająca na wysyłaniu zbiorczych zaproszeń do wszystkich odbiorów z książki adresowej użytkownika.

- tożsamość nadawcy musi być wyraźnie wskazana,

- nadawca musi znać całą zawartość wiadomości, która zostanie przesłana w jego imieniu.

Niektóre SNS zachowują również dane identyfikacyjne użytkowników, którzy zostali wykluczeni z usługi, aby nie mogli oni zarejestrować się ponownie. W tym przypadku należy poinformować te osoby o przetwarzaniu ich danych, a ponadto pozostawiona może być wyłącznie informacja umożliwiająca identyfikację tych użytkowników. Nie można natomiast przechowywać informacji o przyczynie wykluczenia użytkownika z usługi. Tego rodzaju informacje mogą być przechowywane nie dłużej niż rok.

Dane osobowe przekazane przez użytkownika rejestrującego się w SNS winny zostać usunięte natychmiast po usunięciu konta przez użytkownika[24]. Podobnie, informacje usunięte przez użytkownika podczas aktualizacji konta nie powinny być przechowywane. SNS powinien poinformować użytkowników przed podjęciem tych kroków za pomocą dostępnych mu środków służących do informowania użytkowników o tych okresach przechowywania. Ze względów bezpieczeństwa i względów prawnych, w pewnych przypadkach uzasadnione może okazać się przechowywanie zaktualizowanych lub usuniętych danych i kont przez pewien czas, aby pomóc zapobiec złośliwym działaniom wynikającym z kradzieży tożsamości lub innym przestępstwom.

Jeśli użytkownik nie korzysta z usługi przez konkretnie określony czas, profil powinien zostać zawieszony – byłby wówczas niewidoczny dla innych użytkowników czy oglądających, a po upływie kolejnego okresu czasu dane na porzuconym koncie powinny zostać skasowane. SNS powinny powiadomić użytkownika przed podjęciem takich kroków wszelkimi dostępnymi środkami.

3.9 Prawa użytkowników

SNS powinny przestrzegać praw osób, których dane są przetwarzane, zgodnie z artykułem 12 i 14 dyrektywy o ochronie danych.

Prawo dostępu i poprawienia danych nie jest ograniczone do użytkowników usługi, ale również przysługuje każdej osobie, której dane są przetwarzane[25]: Zarówno członkowie, jak i osoby, które nie są członkami portalu społecznościowego, powinny mieć możliwość wykonywania prawa dostępu, poprawiania i usunięcia danych. Strona główna SNS powinna zawierać wyraźne informacje o procedurze obsługi skarg ustanowionej przez SNS dla problemów związanych z ochroną danych i prywatności oraz skarg, dostępnej dla użytkowników i innych osób.

Art. 6 ust. 1 lit. c) dyrektywy o ochronie danych wymaga, aby dane były „prawidłowe, stosowne oraz nienadmierne ilościowo w stosunku do celów, dla których są gromadzone i/lub dalej przetwarzane". W tym kontekście można zauważyć, że SNS mogą mieć potrzebę zapisania niektórych danych identyfikujących członków, ale nie muszą publikować prawdziwych nazwisk członków w Internecie. Toteż SNS powinny dokładnie rozważyć kwestię, czy mogą uzasadnić zmuszanie swoich użytkowników do

[24] Zgodnie z artykułem 6 ust. 1e) dyrektywy o zatrzymywaniu danych dane *„należy przechowywać w formie, która pozwala na identyfikację osób, których dane dotyczą, przez okres nie dłuższy niż to konieczne do celów, dla których dane zostały zebrane lub w których są dalej przetwarzane"*.

[25] Np. ma to miejsce w przypadku, gdy dostawca portalu społecznościowego wykorzystał prywatne konto poczty elektronicznej tej osoby w celu wysłania jej zaproszenia.

działania z podaniem ich prawdziwej tożsamości, a nie pod pseudonimem. Istnieją silne argumenty za daniem użytkownikom wyboru w tym zakresie, a co najmniej w jednym państwie członkowskim jest to wymóg prawny. Argumenty są szczególnie silne w przypadku SNS mających wielu członków.

Artykuł 17 dyrektywy o ochronie danych wymaga, aby administrator wprowadził odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych. Do takich środków bezpieczeństwa należą w szczególności kontrola dostępu i mechanizmy uwierzytelniania, które nadal można wdrożyć, jeśli stosowane są pseudonimy.

4. Dzieci i osoby niepełnoletnie

Znaczna część usług SNS jest wykorzystywana przez dzieci / osoby niepełnoletnie. W Opinii WP 147[26] Grupa Robocza skoncentrowała się w szczególności na stosowaniu reguł ochrony danych w szkołach i środowisku szkolnym. W Opinii podkreślono konieczność uwzględnienia przede wszystkim najlepszego interesu dziecka zgodnie z Konwencją Praw Dziecka ONZ. Grupa Robocza pragnie podkreślić znaczenie tej zasady również w kontekście SNS.

Ciekawe inicjatywy[27] dotyczące zwiększania świadomości na temat SNS i ewentualnych zagrożeń zostały podjęte przez Organy Ochrony Danych na całym świecie. Grupa Robocza zachęca do dalszych badań kwestii, jak należy rozwiązać trudności związane z odpowiednią weryfikacją wieku i potwierdzeniem świadomej zgody, aby lepiej sprostać tym wyzwaniom.

W oparciu o poczynione dotychczas rozważania Grupa Robocza sądzi, że wielotorowa strategia byłaby odpowiednim rozwiązaniem kwestii ochrony danych dzieci w kontekście SNS. Tego rodzaju strategia mogłaby opierać się na:

- inicjatywach mających na celu podniesienie świadomości, niezbędnych dla zapewnienia czynnego zaangażowania dzieci (w szkołach, uwzględnienie podstawowych informacji na temat ochrony danych w programach nauczania, stworzenie doraźnych narzędzi edukacyjnych, współpraca z właściwymi organami krajowymi),

- rzetelnym i legalnym przetwarzaniu danych osób niepełnoletnich obejmującym zakaz zbierania danych szczególnie chronionych w formularzach rejestracji, zakaz marketingu bezpośredniego skierowanego do osób niepełnoletnich, konieczność uzyskania zgody osoby dorosłej przed zarejestrowaniem się, oraz odpowiednie poziomy logicznego oddzielenia środowisk dzieci i dorosłych,

- wdrożeniu PET – technologii wspierających prywatność (np. poprzez wprowadzanie ustawień początkowych bardziej przyjaznych dla użytkownika, wyskakujących okienek typu pop-up zawierających odpowiednie ostrzeżenia na poszczególnych etapach, oprogramowanie do weryfikacji wieku),

---

26 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp147_en.pdf

27 Na przykład portugalska inicjatywa "Dadus" http://dadus.cnpd.pt/, duńska Chat Check Badge http:/www.fdim.dk/

- wprowadzeniu samoregulacji przez dostawców, zachęcaniu do przyjmowania kodeksów dobrych praktyk, które powinny zawierać skuteczne środki egzekwowania prawa, również o charakterze dyscyplinarnym.

- w razie konieczności - przyjęciu środków legislacyjnych *ad hoc* w celu zniechęcenia do stosowania nieuczciwych i/lub zwodniczych praktyk w kontekście SNS.

5. STRESZCZENIE LISTY PRAW/OBOWIĄZKÓW

Zastosowanie dyrektyw WE

1. **Dyrektywa o ochronie danych co do zasady odnosi się do przetwarzania danych osobowych przez SNS, nawet jeśli jego siedziba mieści się poza EOG.**

2. **Dostawcy SNS na mocy dyrektywy o ochronie danych uznawani są za administratorów danych.**

3. **Dostawcy aplikacji mogą być uznawani są za administratorów danych na mocy dyrektywy o ochronie danych.**

4. **Użytkowników uznaje się za osoby, których dane dotyczą, w odniesieniu do przetwarzania danych w SNS.**

5. **Przetwarzanie danych osobowych przez użytkowników w większości przypadków podlega wyłączeniu jako czynności o czysto osobistym lub domowym charakterze. Istnieją jednak sytuacje, w których działalność użytkownika nie jest objęta takim wyłączeniem.**

6. **SNS nie wchodzą w zakres definicji usług komunikacji elektronicznej i w związku z tym nie ma do nich zastosowania dyrektywa o zatrzymywaniu danych.**

Zobowiązania SNS

7. **SNS winny informować użytkowników o swej tożsamości oraz zapewniać wyczerpujące i zrozumiałe informacje na temat celów i sposobów planowanego przetwarzania danych osobowych.**

8. **SNS powinny oferować przyjazne dla prywatności ustawienia domyślne.**

9. **Dostawcy SNS powinni odpowiednio ostrzegać użytkowników przed zagrożeniami dla prywatności, jakie niesie ze sobą publikacja danych na SNS.**

10. **Użytkowników należy informować, że mogą publikować zdjęcia i informacje dotyczące innych osób tylko za ich zgodą.**

11. **Strona główna SNS powinna co najmniej zawierać link do procedury obsługi skarg, ustanowionej dla problemów związanych z ochroną danych, dostępnej dla użytkowników i innych osób.**

12. **Działalność marketingowa musi być zgodna z zasadami określonymi w dyrektywie o ochronie danych oraz dyrektywie o prywatności i łączności elektronicznej.**

13. **SNS muszą określić maksymalne okresy przechowywania danych na temat użytkowników niekorzystających z usługi. Porzucone konta należy usuwać.**

14. **SNS powinny podjąć odpowiednie działania w celu ograniczenia zagrożeń w odniesieniu do osób niepełnoletnich.**

<u>Prawa użytkowników</u>

15. **Zarówno członkowie SNS, jak i osoby niebędące jego członkami, mają prawa przysługujące osobom, których dane dotyczą, na mocy art. 10-14 dyrektywy o ochronie danych – jeśli mają one zastosowanie.**

16. **Zarówno członkowie SNS, jak i osoby niebędące jego członkami, winni mieć możliwość skorzystania z łatwej w obsłudze procedury obsługi skarg ustanowionej przez SNS.**

17. **Użytkownicy powinni generalnie mieć możliwość posługiwania się pseudonimami.**

Sporządzono w Brukseli,

w dniu 12 czerwca 2009 r.

W imieniu Grupy Roboczej
Przewodniczący
Alex TÜRK