GRUPA ROBOCZA ART. 29

01189/09/PL
WP 163

Opinia 5/2009 w sprawie portali społecznościowych

przyjęta w dniu 12 czerwca 2009 r.

Spis treści

Streszczenie

Niniejsza opinia skupia się na tym, jak portale społecznościowe mogą działać zgodnie z wymogami wspólnotowego prawodawstwa w zakresie ochrony danych. Zasadniczo ma ona służyć przekazaniu dostawcom sieciowych serwisów społecznościowych (SNS) wskazówek dotyczących środków, które należy wprowadzić, aby zapewnić zgodność z prawem UE.

W opinii zwraca się uwagę, że dostawcy SNS oraz, w wielu przypadkach, zewnętrzni dostawcy aplikacji są administratorami danych i mają odpowiadające tej funkcji obowiązki wobec użytkowników SNS. W opinii wskazano, że wielu użytkowników działa jedynie w sferze czysto prywatnej, kontaktując się z innymi osobami w ramach załatwiania swoich spraw osobistych, rodzinnych lub domowych. W opinii uznano, że w takich przypadkach stosuje się „wyłączenie do celów domowych", a przepisy dotyczące administratorów danych nie mają zastosowania. Opinia określa również okoliczności, w których czynności użytkownika SNS nie są objęte „wyłączeniem do celów domowych". Rozpowszechnianie i użycie informacji dostępnych w SNS do innych, wtórnych i niezamierzonych, celów są głównymi przedmiotami zainteresowania Grupy Roboczej Art. 29. W całej opinii zaleca się stosowanie ustawień domyślnych zdecydowanie chroniących i wspierających prywatność jako doskonałego punktu wyjścia dla wszystkich oferowanych usług. Kluczowym obszarem zainteresowania jawi się dostęp do informacji ujętych w profilu. Opisane są również takie tematy, jak przetwarzanie danych szczególnie chronionych i wizerunków, reklama i marketing bezpośredni w SNS oraz kwestie związane z zatrzymywaniem danych.

Główne zalecenia skupiają się na obowiązkach dostawców SNS w zakresie przestrzegania przepisów dyrektywy o ochronie danych oraz wspierania i umacniania praw użytkowników. Zasadnicze znaczenie ma, aby dostawcy SNS od początku informowali użytkowników o swojej tożsamości oraz przedstawiali im wszystkie różnorodne cele, dla których przetwarzają dane osobowe. Dostawcy SNS powinni zachować szczególną staranność w odniesieniu do przetwarzania danych osobowych małoletnich. W opinii zaleca się, aby użytkownicy przesyłali zdjęcia lub informacje o innych osobach fizycznych wyłącznie za zgodą danej osoby, oraz uznaje się, że SNS mają również obowiązek informowania użytkowników o prawach do 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 art. 30 ust. 1 lit. a) i ust. 3 powyższej 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 oraz 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 swój regulamin,

PRZYJMUJE NINIEJSZY DOKUMENT:

1. Wprowadzenie

Rozwój społeczności sieciowych i usług dostarczanych przez firmy hostingowe, takich jak sieciowe serwisy społecznościowe („SNS"), jest stosunkowo nowym zjawiskiem, przy czym liczba użytkowników takich stron internetowych wciąż rośnie w gwałtownym tempie.

Informacje osobowe przesyłane *on-line* przez użytkowników, wraz z danymi opisującymi działania użytkowników i ich interakcje z innymi osobami, mogą tworzyć bogaty profil opisujący zainteresowania i działania danej osoby. Dane osobowe publikowane na portalach społecznościowych mogą być wykorzystywane przez osoby trzecie w bardzo różnych celach, w tym celach komercyjnych, co może stwarzać poważne zagrożenia, związane między innymi z kradzieżą tożsamości, stratami finansowymi, utratą perspektyw biznesowych lub zatrudnienia czy ze szkodami fizycznymi.

Berlińska międzynarodowa grupa robocza ds. ochrony danych w sektorze telekomunikacji przyjęła w marcu 2008 r. Memorandum rzymskie[2]. W memorandum zawarta jest analiza zagrożeń dla prywatności i bezpieczeństwa stwarzanych przez sieci społeczne oraz wskazane są wytyczne dla organów regulacyjnych, dostawców i użytkowników. Niedawno przyjęta Rezolucja w sprawie ochrony prywatności w sieciowych serwisach społecznościowych[3] również ustosunkowuje się do wyzwań związanych z SNS. Grupa robocza uwzględnia również dokument strategiczny opublikowany w październiku 2007 r. przez Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA) pod tytułem "Kwestie i zalecenia związane z bezpieczeństwem w odniesieniu do sieci społecznych *on-line*"[4], skierowany do organów regulacyjnych i dostawców sieci serwisów społecznościowych.

---

1 Dziennik Urzędowy L 281 z dnia 23.11.1995 r., 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 na 30. Międzynarodowej konferencji organów ds. ochrony danych i prywatności w Strasburgu dnia 17.10.2008 r., http://www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_social_networks_en.pdf .

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

2. Definicja „sieciowego serwisu społecznościowego (SNS)” i model biznesowy

Sieciowe serwisy społecznościowe (SNS) można ogólnie określić jako platformy komunikacyjne *on-line* umożliwiające osobom fizycznym przystępowanie do lub tworzenie sieci użytkowników o wspólnych upodobaniach. W sensie prawnym serwisy społecznościowe są usługami społeczeństwa informacyjnego w rozumieniu art. 1 ust. 2 dyrektywy 98/34/WE zmienionej dyrektywą 98/48/WE. SNS posiadają pewne cechy wspólne:

- użytkowników zachęca się do przekazania danych osobowych w celu stworzenia opisu swojej osoby lub swojego „profilu”;

- SNS obejmują również narzędzia, które umożliwiają użytkownikom przesyłanie swoich własnych materiałów (treści generowanych przez użytkowników, na przykład fotografii lub wpisu do pamiętnika, pliku muzycznego lub wideo lub łączy do innych stron[5]);

- możliwe jest “tworzenie sieci kontaktów towarzyskich” dzięki wykorzystaniu narzędzi, które pozwalają stworzyć każdemu użytkownikowi listę kontaktów oraz za pomocą których użytkownicy mogą wchodzić w interakcje.

Dużą część swoich przychodów SNS generują poprzez usługi reklamowe, które są świadczone na stronach internetowych stworzonych i odwiedzanych przez użytkowników. Użytkownicy, którzy w ramach swoich profili przesyłają duże ilości informacji o swoich zainteresowaniach, stanowią doskonały rynek dla reklamodawców chcących przekazywać ukierunkowane reklamy w oparciu o te informacje.

Dlatego ważne jest, aby SNS działały z poszanowaniem praw i wolności użytkowników, którzy z uzasadnionych powodów mogą oczekiwać, że ujawniane przez nich dane osobowe będą przetwarzane zgodnie z europejskimi i krajowymi przepisami w zakresie ochrony danych i prywatności.

3. Zastosowanie dyrektywy o ochronie danych

Przepisy dyrektywy o ochronie danych mają zastosowanie do większości dostawców SNS, nawet jeżeli ich siedziby znajdują się poza EOG. Grupa Robocza Art. 29 odsyła do swojej wcześniejszej opinii dotyczącej wyszukiwarek, gdzie znajdują się dalsze wskazówki dotyczące kwestii prowadzenia działalności gospodarczej i wykorzystania środków jako czynników warunkujących stosowanie dyrektywy o ochronie danych oraz dotyczące reguł mających w związku z tym zastosowanie odnośnie do przetwarzania adresów IP i użycia plików typu „cookies”[6].

3.1 Kto jest administratorem danych?

Dostawcy SNS

Dostawcy SNS są administratorami danych na mocy dyrektywy o ochronie danych. Zapewniają oni środki przetwarzania danych użytkownika i świadczą wszystkie „podstawowe” usługi związane z zarządzaniem kontami użytkowników (na przykład rejestracja i usuwanie kont). Dostawcy SNS określają również sposób wykorzystania danych

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

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

użytkownika w celach reklamowych i marketingowych – włączając w to usługi reklamowe świadczone przez osoby trzecie.

Dostawcy aplikacji

Dostawcy aplikacji mogą być również administratorami danych, jeżeli tworzą aplikacje, które funkcjonują obok aplikacji SNS, a użytkownicy zdecydują się na używanie danej aplikacji.

Użytkownicy

W większości przypadków, użytkownicy są uznawani za osoby, których dane dotyczą. Dyrektywa nie nakłada obowiązków administratora danych na osobę fizyczną, która przetwarza dane osobowe „w trakcie czynności o czysto osobistym lub domowym charakterze" – co stanowi tak zwane „wyłączenie do celów domowych". W niektórych przypadkach „wyłączenie do celów domowych" może nie obejmować czynności użytkownika SNS i można uznać, że użytkownik przejmuje część obowiązków administratora danych. Niektóre przykłady są opisane poniżej.

3.1.1. Cel i charakter

Wśród SNS obserwuje się narastającą tendencję do „przechodzenia od »Web 2.0 dla zabawy« do »Web 2.0 na potrzeby zwiększenia wydajności i świadczenia usług«”[7], w skutek czego czynności niektórych użytkowników SNS mogą wykraczać poza działania o czysto osobistym lub domowym charakterze, na przykład gdy SNS jest stosowane jako platforma współpracy w ramach stowarzyszenia lub przedsiębiorstwa. Jeżeli użytkownik SNS działa w imieniu przedsiębiorstwa lub stowarzyszenia lub wykorzystuje SNS głównie jako platformę służącą osiąganiu celów komercyjnych, politycznych lub charytatywnych, wspomniane wyłączenie nie ma zastosowania. W tym przypadku użytkownik przyjmuje pełnię obowiązków administratora danych ujawniającego dane osobowe innemu administratorowi danych (SNS) lub osobom trzecim (innym użytkownikom SNS lub potencjalnie nawet innym administratorom danych mającym dostęp do danych). W takich okolicznościach użytkownik musi uzyskać zgodę osób zainteresowanych lub wskazać inną podstawę prawną przewidzianą w dyrektywie o ochronie danych.

Zazwyczaj dostęp do danych (danych ujętych w profilu, wpisów, opowiadań itp.) przekazanych przez użytkownika jest ograniczony do samodzielnie wybranych kontaktów. Jednakże w niektórych przypadkach użytkownicy mogą mieć wiele kontaktów z osobami trzecimi, z których nie wszystkich mogą faktycznie znać. Duża ilość kontaktów mogłaby wskazywać, że „wyłączenie do celów domowych” nie obowiązuje, a więc użytkownika można byłoby uznać za administratora danych.

3.1.2. Dostęp do informacji ujętych w profilu

SNS powinny zadbać o takie ustawienia domyślne, które chronią prywatność i są bezpłatne oraz ograniczają dostęp do samodzielnie wybranych kontaktów.

Gdy dostęp do informacji ujętych w profilu mają osoby spoza grona samodzielnie wybranych kontaktów, na przykład gdy dostęp do profilu jest zapewniony dla wszystkich członków SNS[8] lub dane są indeksowane przez wyszukiwarki, dostęp wykracza poza sferę osobistą lub domową. Podobnie jeżeli użytkownik podejmie świadomą decyzję o rozszerzeniu dostępu poza samodzielnie wybranych „przyjaciół”, aktualizują się obowiązki administratora danych. W rzeczywistości w tej sytuacji będą miały zastosowanie te same przepisy, co w przypadku gdy jakakolwiek osoba wykorzystuje inne platformy technologiczne do publikacji danych osobowych w sieci[9]. W kilku państwach członkowskich brak ograniczeń dostępu (czyli charakter publiczny) oznacza, że dyrektywa o ochronie danych ma zastosowanie w taki sposób, że użytkownik Internetu przyjmuje obowiązki administratora danych[10].

Należy pamiętać, że nawet jeżeli wyłączenie do celów domowych nie obowiązuje, użytkownik SNS może korzystać z innych wyłączeń, na przykład wyłączenia na potrzeby

---

7 „Internet przyszłości: Europa musi być kluczowym graczem” przemówienie europejskiej komisarz ds. społeczeństwa informacyjnego i mediów Viviane Reding, wygłoszone podczas spotkania Rady Lizbońskiej w ramach inicjatywy „Przyszłość Internetu”, Bruksela, 2 lutego 2009 r.

8 Lub gdy można wykazać, że nie prowadzi się faktycznie żadnej selekcji przy akceptacji kontaktów, tj. użytkownicy akceptują „kontakty” bez względu na posiadane powiązania

9 Tak jak w przypadku platform zajmujących się publikacją, które nie są SNS, lub w przypadku oprogramowania umieszczonego na własnym serwerze (*self-hosted*).

10 W wyroku w sprawie Satamedia ETS orzekł w przeciwny sposób w pkt 44: „Z powyższego wynika, że to drugie odstępstwo powinno być interpretowane jako obejmujące jedynie działania wchodzące w zakres życia prywatnego lub rodzinnego podmiotów indywidualnych (zob. ww. wyrok w sprawie Lindqvist, pkt 47). W sposób oczywisty nie ma to miejsca w przypadku działalności Markkinapörssi i Satamedia, polegającej na przekazaniu zebranych danych nieograniczonej liczbie osób”.

dziennikarskie, artystyczne lub literackie. W takich przypadkach należy znaleźć równowagę pomiędzy swobodą wypowiedzi i prawem do prywatności.

3.1.3 Przetwarzanie danych osób trzecich przez użytkowników

Stosowanie wyłączenia do celów domowych jest również ograniczone potrzebą zagwarantowania praw osób trzecich, w szczególności w odniesieniu do danych szczególnie chronionych. Ponadto należy zauważyć, że nawet jeżeli obowiązuje wyłączenie do celów domowych, użytkownik może ponosić odpowiedzialność na mocy ogólnych przepisów danego krajowego prawodawstwa cywilnego lub karnego (na przykład z tytułu zniesławienia, odpowiedzialności deliktowej za naruszenie dóbr osobistych, odpowiedzialności karnej).

3.2 Bezpieczeństwo i domyślne ustawienia prywatności

Bezpieczne przetwarzanie informacji jest kluczowym czynnikiem zaufania do SNS. Administratorzy danych muszą stosować odpowiednie środki techniczne i organizacyjne, „zarówno przy opracowywaniu systemu przetwarzania danych, jak i podczas samego ich przetwarzania", w celu utrzymania bezpieczeństwa i zapobiegania bezprawnemu przetwarzaniu danych, przy uwzględnieniu zagrożeń związanych z przetwarzaniem i charakterem danych[11].

Ważnym elementem ustawień prywatności jest dostęp do danych osobowych publikowanych w ramach profilu. Jeżeli nie istnieją żadne ograniczenia dostępu do tych danych, osoby trzecie mogą pozyskać wszelkiego rodzaju intymne informacje dotyczące użytkowników, czy to będąc członkiem SNS czy poprzez wyszukiwarki. Jednakże jedynie mała część użytkowników rejestrujących się do serwisu dokonuje jakichkolwiek zmian w ustawieniach domyślnych. Dlatego też SNS powinny oferować ustawienia domyślne chroniące prywatność, które pozwalają użytkownikom na swobodne i wyraźne wyrażanie zgody na dostęp do treści profilu osobom nienależącym do samodzielnie wybranych kontaktów, tak aby ograniczyć ryzyko bezprawnego przetwarzania przez osoby trzecie. Nie powinno być możliwości odnalezienia profili z ograniczonym dostępem przez wewnętrzne wyszukiwarki, w tym narzędzia służące wyszukiwaniu według parametrów, na przykład wieku lub lokalizacji. Decyzje o rozszerzeniu dostępu nie mogą być dorozumiane[12], na przykład poprzez zastosowanie przez administratora danych SNS wariantu wycofania zgody (*opt-out*).

3.3 Informacje, które mają przekazywać SNS

Dostawcy SNS powinni informować użytkowników o swojej tożsamości oraz o różnych celach przetwarzania danych osobowych zgodnie z przepisami określonymi w art. 10 dyrektywy o ochronie danych, do których należą między innymi:

- wykorzystanie danych w celach marketingu bezpośredniego;
- możliwa wymiana danych z określonymi kategoriami osób trzecich;
- przegląd dotyczący profili: ich tworzenia i głównych źródeł danych;

---

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

[12] W Sprawozdaniu i wskazówkach dotyczących prywatności w sieciowych serwisach społecznościowych („Memorandum rzymskim") wymienione są zagrożenia, takie jak „błędnie rozumiane pojęcie społeczności", s. 2, „ujawnianie większej ilości danych osobowych niż się danej osobie wydaje", s. 3. Firma zajmująca się bezpieczeństwem komputerów ostrzega znaczący SNS o istnieniu domyślnego dostępu dla członków w ramach jednej lokalizacji geograficznej: http://www.sophos.com/pressoffice/news/articles/2007/10/facebook-network.html.

- wykorzystanie danych szczególnie chronionych.

Grupa robocza zaleca:

- aby dostawcy SNS przekazywali użytkownikom odpowiednie ostrzeżenia o zagrożeniach dla prywatności stwarzanych sobie i innym poprzez przesyłanie informacji do SNS;

- użytkownikom SNS należy również przypomnieć, że przesyłanie informacji o innych osobach fizycznych może naruszać ich prywatność i prawa w zakresie ochrony danych;

- SNS powinny informować swoich użytkowników, że jeżeli zamierzają przesyłać zdjęcia innych osób fizycznych lub informacje o nich, powinno się to odbywać za zgodą tych osób[13].

3.4 Dane szczególnie chronione

Za szczególnie chronione uznaje się dane ujawniające pochodzenie rasowe lub etniczne, opinie polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych lub dane dotyczące zdrowia lub życia seksualnego. Szczególnie chronione dane osobowe mogą być publikowane w Internecie jedynie za wyraźną zgodą osoby, której dane dotyczą, lub jeżeli osoba, której dane dotyczą, sama w wyraźny sposób upubliczniła te dane[14].

W niektórych państwach członkowskich UE, wizerunki osób, których dane dotyczą, są uznawane za specjalną kategorię danych osobowych, jako że mogą być wykorzystane do rozpoznania pochodzenia rasowego / etnicznego lub mogą być użyte do ustalenia przekonań religijnych lub informacji o zdrowiu. Grupa robocza zasadniczo nie uznaje wizerunków publikowanych w Internecie za dane szczególnie chronione[15], chyba że wizerunki te są w wyraźny sposób wykorzystane do ujawnienia szczególnie chronionych danych o osobach fizycznych.

Będąc administratorami danych, SNS nie mogą przetwarzać szczególnie chronionych danych o członkach SNS lub osobach niebędących członkami SNS bez ich wyraźniej zgody[16]. Jeżeli SNS umieszcza w formularzu profilu dla użytkowników jakiekolwiek pytania dotyczące danych szczególnie chronionych, SNS musi dobitnie zaznaczyć, że odpowiadanie na te pytania jest całkowicie dobrowolne.

3.5 Przetwarzanie danych osób niebędących członkami SNS

Wiele SNS umożliwia użytkownikom uzupełnianie danych o innych osobach, na przykład poprzez dodanie imienia / nazwiska pod zdjęciem, ocenę danej osoby, wymienienie „osób, które spotkałem / chcę spotkać" w czasie imprez. Takie oznaczenia mogą również przyczynić się do identyfikacji osób niebędących członkami SNS. Jednakże SNS mogą przetwarzać takie

---

[13] Można to ułatwić poprzez wprowadzenie w ramach portali społecznościowych narzędzi zarządzania oznaczeniami, na przykład poprzez udostępnienie w profilu osobowym miejsc wskazujących obecność imienia / nazwiska użytkownika na oznaczonym zdjęciu lub pliku wideo, które oczekują na zgodę na ujawnienie, lub poprzez ustalenie terminów ważności dla oznaczeń, które nie uzyskały zgody ze strony opisanej osoby.

[14] Państwa członkowskie mogą ustanowić odstępstwa od tej zasady; zob. art. 8 ust. 2 lit. a) zdanie drugie oraz art. 8 ust. 4 dyrektywy o ochronie danych.

[15] Jednakże publikowanie wizerunków w Internecie wzbudza coraz większe obawy w zakresie ochrony prywatności, ponieważ technologie rozpoznawania twarzy są coraz lepsze.

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

dane o osobach niebędących członkami jedynie w przypadkach, gdy spełnione jest jedno z kryteriów określonych w art. 7 dyrektywy o ochronie danych.

Ponadto podstawy prawnej nie ma tworzenie wstępnie opracowanych profili osób niebędących członkami poprzez zestawianie danych zamieszczanych niezależnie przez użytkowników SNS, w tym informacji o kontaktach uzyskanych na podstawie umieszczonych w serwisie książek adresowych[17].

Nawet jeżeli SNS miałby możliwość skontaktowania się z określoną osobą niebedącą członkiem i poinformowania jej o istnieniu dotyczących jej danych osobowych, to ewentualne przesłane e-mailem zaproszenie do przystąpienia do SNS w celu uzyskania dostępu do tych danych osobowych stanowiłoby naruszenie zakazu określonego w art. 13 ust. 4 dyrektywy o prywatności i łączności elektronicznej, dotyczącego wysyłania niezamówionych wiadomości elektronicznych w celach marketingu bezpośredniego.

3.6 Dostęp osób trzecich

3.6.1 Dostęp za pośrednictwem SNS

Oprócz głównej usługi świadczonej przez SNS, większość SNS oferuje użytkownikom dodatkowe aplikacje tworzone przez dostawców zewnętrznych, które również przetwarzają dane osobowe.

SNS powinny posiadać środki pozwalające dopilnować, aby aplikacje dostarczane przez osoby trzecie były zgodne z dyrektywą o ochronie danych oraz dyrektywą o prywatności i łączności elektronicznej. Oznacza to w szczególności, że aplikacje te zawierają wyraźne i szczegółowe informacje skierowane do użytkowników dotyczące przetwarzania ich danych osobowych i że mają one dostęp jedynie do niezbędnych danych osobowych. Dlatego też SNS powinny oferować dostawcom zewnętrznym dostęp modułowy, tak aby mogli oni wybrać tryb dostępu, który z założenia jest bardziej ograniczony. Ponadto SNS powinny zapewnić użytkownikom możliwość łatwego zgłaszania wątpliwości dotyczących aplikacji.

3.6.2 Dostęp osób trzecich za pośrednictwem użytkowników

SNS czasami umożliwiają użytkownikom dostęp do ich danych oraz ich aktualizację z wykorzystaniem innych aplikacji. Na przykład użytkownicy mogą mieć możliwość:

- odczytywania i przesyłania wiadomości do sieci ze swoich telefonów komórkowych;
- synchronizowania danych kontaktowych swoich przyjaciół w SNS z książką adresową na komputerze stacjonarnym;
- automatycznego uaktualniania swojego statusu lub lokalizacji w SNS z wykorzystaniem innej strony internetowej.

SNS publikuje informacje o sposobie, w jaki takie oprogramowanie może być napisane, w formie „programistycznego interfejsu aplikacyjnego” („API”). Umożliwia on osobom trzecim napisanie programu wykonującego określone czynności, a użytkownikom zapewnia

[17] Motyw 38 dyrektywy o ochronie danych wyjaśnia, że: „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 uzyskiwane od niej, musi otrzymać dokładne i pełne informacje, uwzględniające okoliczności pozyskiwania danych”. W przypadku niektórych SNS publikacja profili osób niebędących członkami SNS stała się przypuszczalnie istotnym sposobem reklamowania „usług” tych SNS.

swobodny wybór między kilkoma różnymi dostawcami zewnętrznymi[18]. Oferując API umożliwiający dostęp do danych osób kontaktowych, SNS powinien:

- zapewnić poziom szczegółowości umożliwiający użytkownikowi wybór poziomu dostępu dla osoby trzeciej, który jest wystarczający tylko do wykonania danego zadania.

Uzyskując w imieniu użytkownika dostęp do danych osobowych poprzez interfejs API dla osób trzecich, zewnętrzni dostawcy usług nie powinni:

- przetwarzać i przechowywać danych dłużej niż jest to konieczne do wykonania konkretnego zadania;

- wykonywać żadnych innych operacji na danych z importowanych kontaktów użytkownika niż osobiste ich wykorzystanie przez użytkownika przekazującego dane.

3.7 Podstawy prawne marketingu bezpośredniego

Marketing bezpośredni jest kluczową częścią biznesowego modelu SNS, które mogą wykorzystywać różne sposoby marketingu. Jednakże marketing wykorzystujący dane osobowe użytkowników powinien być zgodny z odpowiednimi przepisami dyrektywy o ochronie danych oraz dyrektywy o prywatności i łączności elektronicznej[19].

Marketing kontekstowy jest dostosowany do treści, które przegląda lub do których uzyskuje dostęp użytkownik[20].

Marketing segmentacyjny polega na dostarczaniu reklam oznaczonej grupie użytkowników[21]; użytkownik zostaje umieszczony w danej grupie na podstawie informacji, które bezpośrednio przekazał do SNS[22].

Wreszcie *marketing behawioralny* wybiera reklamy w oparciu o obserwację i analizę działań użytkowników w czasie. Techniki te mogą podlegać różnym wymogom prawnym, w zależności od stosowanych podstaw prawnych i cech wykorzystywanych technologii. Grupa robocza zaleca, aby nie wykorzystywać danych szczególnie chronionych w behawioralnych modelach reklamy, o ile nie zostaną spełnione wszystkie wymogi prawne.

Niezależnie od zastosowanego modelu lub zastosowanej kombinacji modelów, reklamy mogą być dostarczane bezpośrednio przez SNS (dostawca SNS działa w tym przypadku jako pośrednik) albo przez zewnętrznego reklamodawcę. W pierwszym przypadku dane osobowe użytkowników nie muszą być ujawniane osobom trzecim. Jednak w drugim przypadku zewnętrzny reklamodawca może przetwarzać dane osobowe dotyczące użytkowników, na przykład jeżeli przetwarza adres IP użytkownika i plik *cookie* umieszczony w komputerze użytkownika.

---

[18] Choć „API" jest ogólnym terminem technicznym, tutaj API odnosi się do dostępu w imieniu użytkownika, tj. użytkownicy muszą podać swoje dane identyfikacyjne do programu, tak aby mógł on działać w ich imieniu.

[19] W najbliższej przyszłości grupa robocza zamierza odnieść się w oddzielnym dokumencie do różnych aspektów reklamy *on-line*.

[20] Na przykład jeżeli wyświetlana strona zawiera słowo „Paryż", reklama może dotyczyć restauracji w tym mieście.

[21] Przy czym każda grupa jest zdefiniowana na podstawie zestawu kryteriów.

[22] Na przykład gdy zarejestrował się w serwisie.

3.8 Zatrzymywanie danych

SNS wykraczają poza zakres definicji usług łączności elektronicznej zawartej w art. 2 lit. c) dyrektywy ramowej (2002/21/WE). Dostawcy SNS mogą oferować dodatkowe usługi mieszczące się w zakresie usług łączności elektronicznej, na przykład ogólnodostępną usługę poczty e-mail. Taka usługa będzie podlegała przepisom dyrektywy o prywatności i łączności elektronicznej oraz dyrektywy w sprawie zatrzymywania danych.

Niektóre SNS umożliwiają swoim użytkownikom wysyłanie zaproszeń osobom trzecim. Zakaz wykorzystywania poczty elektronicznej w celach marketingu bezpośredniego nie dotyczy komunikacji osobistej. Aby realizować warunki wyłączenia do celów komunikacji osobistej, SNS musi spełniać następujące kryteria:

- ani wysyłający, ani odbiorca nie otrzymuje żadnych zachęt;
- dostawca usługi nie wybiera odbiorców wiadomości[23];
- tożsamość użytkownika wysyłającego musi być wyraźnie określona;
- użytkownik wysyłający musi znać pełną treść wiadomości, która zostanie wysłana w jego imieniu.

Niektóre SNS zatrzymują również dane identyfikacyjne użytkowników, którym zakazano korzystania z usługi, aby uniemożliwić im ponowną rejestrację. W takim przypadku użytkownicy ci muszą zostać poinformowani, że takie przetwarzanie danych ma miejsce. Ponadto zatrzymane mogą być jedynie dane identyfikacyjne, a nie informacje o przyczynach nałożenia zakazu na takie osoby. Takie dane nie powinny być zatrzymane dłużej niż przez jeden rok.

Dane osobowe przekazane przez użytkownika podczas rejestracji w SNS powinny zostać usunięte, gdy tylko użytkownik lub dostawca SNS zdecyduje się na usunięcie konta[24]. Na podobnej zasadzie nie powinny być zatrzymywane informacje usunięte przez użytkownika w trakcie aktualizacji konta. Przed podjęciem takich kroków SNS powinien powiadomić użytkowników za pomocą instrumentów, które ma do dyspozycji w celu informowania użytkowników, o okresach zatrzymania danych. Ze względu na bezpieczeństwo i przepisy prawne, w szczególnych przypadkach uzasadnione może być przechowywanie zaktualizowanych lub usuniętych danych i kont przez pewien określony czas, aby zapobiegać wrogim działaniom będącym następstwem kradzieży tożsamości i innych wykroczeń lub przestępstw.

Gdy użytkownik nie korzysta z usługi przed pewien określony czas, profil powinien zostać ustawiony jako nieaktywny, tj. niewidoczny dla innych użytkowników lub osób z zewnątrz, a po upływie kolejnego okresu dane znajdujące się w porzuconym koncie powinny zostać usunięte. Przed podjęciem takich kroków SNS powinny powiadamiać użytkowników za pomocą instrumentów, które mają do dyspozycji.

---

[23] Tj. zabroniona jest praktyka stosowana przez niektóre SNS polegająca na wysyłaniu zaproszeń bez wyjątku do wszystkich osób z książki adresowej użytkownika.

[24] Zgodnie z art. 6 ust. 1 lit. e) dyrektywy o ochronie danych dane muszą być "przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez czas nie dłuższy niż jest to konieczne do celów, dla których dane zostały zgromadzone lub dla których są dalej przetwarzane."

3.9 Prawa użytkowników

SNS powinny respektować prawa osób fizycznych objętych przetwarzaniem danych zgodnie z przepisami określonymi w art. 12 i 14 dyrektywy o ochronie danych.

Prawa użytkowników do dostępu do danych i ich sprostowania nie są ograniczone do użytkowników danej usługi, ale dotyczą każdej osoby fizycznej, której dane są przetwarzane[25]. Członkowie i osoby niebędące członkami SNS muszą posiadać środki realizacji swoich praw do dostępu, poprawiania i usuwania. Strona główna portalu SNS powinna wyraźnie wspominać o istnieniu „biura skarg i reklamacji" utworzonego przez dostawcę SNS, aby zajmować się ochroną danych i kwestiami prywatności oraz skargami składanymi przez członków i osoby niebędące członkami SNS.

Artykuł 6 ust. 1 lit. c) dyrektywy o ochronie danych nakazuje, aby dane były „prawidłowe, stosowne oraz nienadmierne ilościowo w stosunku do celów, dla których zostały zgromadzone i/lub dalej przetworzone". W tym kontekście warto zauważyć, że SNS może wymagać rejestracji pewnych danych identyfikacyjnych dotyczących członków, ale nie musi publikować prawdziwych tożsamości członków w Internecie. Dlatego też SNS powinny starannie rozważyć, czy mogą uzasadnić zmuszanie użytkowników do występowania pod własnym nazwiskiem, a nie pod pseudonimem. Istnieją mocne argumenty za pozostawieniem użytkownikom możliwości wyboru w tej kwestii, a przynajmniej w jednym państwie członkowskim jest to wymogiem prawnym. Argumenty te są szczególnie mocne w przypadku SNS z dużą ilością członków.

Artykuł 17 dyrektywy o ochronie danych wymaga, aby administrator danych wprowadził odpowiednie techniczne i organizacyjne środki bezpieczeństwa w celu ochrony danych osobowych. W szczególności, takie środki bezpieczeństwa obejmują kontrolę dostępu i mechanizmy uwierzytelniania, które można wdrażać, nawet jeżeli stosowane są pseudonimy.

4. Dzieci i małoletni

Duża część usług SNS jest wykorzystywana przez dzieci / małoletnich. W opinii WP147[26] grupa robocza skupiła się na zastosowaniu zasad ochrony danych w szkole i środowisku edukacyjnym. W opinii tej podkreślono potrzebę uwzględnienia dobra dziecka, co również wskazano w konwencji ONZ o prawach dziecka. Grupa robocza pragnie podkreślić znaczenie tych zasad również w kontekście SNS.

Organy ochrony danych na całym świecie podejmują ciekawe inicjatywy[27], które skupiają się głównie na zwiększaniu świadomości na temat SNS i możliwych zagrożeń. W celu skuteczniejszego sprostania opisanym wyzwaniom, grupa robocza zachęca do prowadzenia dalszych badań dotyczących tego, jak radzić sobie z trudnościami związanymi z prawidłową weryfikacją wieku i dowodem wyrażenia świadomej zgody.

Opierając się na dotychczasowych rozważaniach grupa robocza uważa, że odpowiednim środkiem w zakresie ochrony danych dzieci w kontekście SNS byłaby strategia wielowymiarowa. Strategia taka mogłaby zostać stworzona w oparciu o:

---

[25] Na przykład wtedy, gdy adres e-mail danej osoby został użyty przez serwis SNS do wysłania tej osobie zaproszenia.

[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/, duński program „Chat Check Badge", http://www.fdim.dk/ .

- inicjatywy mające na celu zwiększanie świadomości, które mają zasadnicze znaczenie dla zapewnienia aktywnego zaangażowania dzieci (poprzez szkoły, włączenie podstaw ochrony danych do programów edukacyjnych, tworzenie doraźnych instrumentów edukacyjnych, współpracę właściwych organów krajowych);

- rzetelne i zgodne z prawem przetwarzanie danych dotyczących małoletnich, na przykład brak pytań o szczególnie chronione dane w formularzach zgłoszeniowych, zaniechanie marketingu bezpośredniego skierowanego konkretnie do małoletnich, konieczność uzyskania wcześniejszej zgody rodziców przed zarejestrowaniem i odpowiednie poziomy logicznej separacji między społecznościami dzieci i dorosłych;

- wprowadzenie technologii ochrony prywatności (PET), na przykład domyślnych ustawień chroniących prywatność, komunikatów wyskakujących okienkach zawierających ostrzeżenia, pojawiających się na stosownych etapach, oprogramowania weryfikującego wiek);

- samoregulację ze strony dostawców, zachęcanie do przyjmowania kodeksów praktyk, które powinny zawierać skuteczne środki wykonawcze, również o charakterze dyscyplinarnym;

- w razie potrzeby, doraźne środki legislacyjne, które mają zniechęcać do nieuczciwych lub oszukańczych praktyk w kontekście SNS.

5. Podsumowanie obowiązków / praw

Stosowanie dyrektyw WE

1. **Dyrektywa o ochronie danych ma zasadniczo zastosowanie do przetwarzania danych osobowych przez SNS, nawet jeżeli ich siedziby znajdują się poza terytorium EOG.**

2. **Dostawców SNS uznaje się za administratorów danych w rozumieniu dyrektywy o ochronie danych.**

3. **Dostawcy aplikacji mogą być uznani za administratorów danych w rozumieniu dyrektywy o ochronie danych.**

4. **Użytkowników uznaje się za osoby, których dane dotyczą, w kontekście przetwarzania ich danych przez SNS.**

5. **Przetwarzanie danych osobowych przez użytkowników w większości przypadków podlega wyłączeniu do celów domowych. Istnieją sytuacje, w których czynności użytkownika nie są objęte tym wyłączeniem.**

6. **SNS wykraczają poza zakres definicji usługi łączności elektronicznej i dlatego dyrektywy w sprawie zatrzymywania danych nie stosuje się do SNS.**

Obowiązki SNS

7. **SNS powinny informować użytkowników o swojej tożsamości oraz przekazywać pełne i wyraźne informacje o celach i różnych sposobach, w jakich zamierzają przetwarzać dane osobowe.**

8. **SNS powinny oferować ustawienia domyślne chroniące prywatność.**

9. SNS powinny przekazywać użytkownikom zamieszczającym dane w SNS informacje i odpowiednie ostrzeżenia o zagrożeniach dla prywatności.

11. SNS powinny informować użytkowników, że zdjęcia innych osób fizycznych lub informacje o nich mogą być przesyłane wyłącznie za zgodą danej osoby.

12. Strona główna SNS powinna przynajmniej zawierać łącze do biura skarg i reklamacji, zajmującego się kwestiami ochrony danych zgłaszanymi przez członków i osoby niebędące członkami SNS.

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

14. SNS muszą ustalić maksymalne okresy zatrzymywania danych w odniesieniu do użytkowników nieaktywnych. Konta porzucone należy usuwać.

15. Jeżeli chodzi o małoletnich, SNS powinny podejmować odpowiednie działania służące ograniczeniu zagrożeń.

<u>Prawa użytkowników</u>

16. Zarówno członkowie, jak i osoby niebędące członkami SNS posiadają w odpowiednich przypadkach prawa osób, których dane dotyczą, zgodnie z przepisami art. 10-14 dyrektywy o ochronie danych.

17. Członkowie i osoby niebędące członkami SNS powinni mieć dostęp do łatwej w użyciu procedury rozpatrywania skarg / reklamacji stworzonej przez SNS.

18. Użytkownicy powinni mieć zasadniczo możliwość przyjmowania pseudonimów.

Sporządzono w Brukseli dnia 12 czerwca 2009 r.

W imieniu grupy roboczej
Przewodniczący
Alex TÜRK