

DEBATA DGP Rządowy projekt ustawy o prawie telekomunikacyjnym: blokowanie nielegalnych stron www

W internecie nikt nie jest anonimowy, ale mamy prawo do prywatności

Bezpieczeństwo danych w internecie powinno być zapewnione przez pełną informację o prawach użytkowników i możliwościach przetwarzania danych.

Kto i kiedy może wykorzystywać nasze cyfrowe ślady w internecie?

MINISTER

MICHAŁ SERZYCKI, GŁOŚ: Rozwój nowych technologii i upowszechnienie internetu powodują, że coraz bardziej aktualne stają się pytania dotyczące naszego bezpieczeństwa w sieci. Uważam, że choć w internecie nie jesteśmy anonimowi, to mamy prawo do prywatności i powinniśmy o nią walczyć. Tym bardziej że ogromna ilość danych osobowych jest pozyskiwana bez naszej wiedzy i zgody. Dla przykładu wymienię stosowany przez wyszukiwarki mechanizm umożliwiający rejestrację odwiedzanych przez użytkownika stron www i tworzenie na tej podstawie profili osobowościowych. Tymczasem ta informacja w połączeniu z innymi, którymi dysponuje dostawca usług, może stanowić dane osobowe, które powinny podlegać ochronie. Dlatego jako organ do spraw ochrony danych osobowych będę zabiegał, by zgodnie z wypracowanym w Unii Europejskiej stanowiskiem, dostawcy usług internetowych, w tym operatorzy wyszukiwarek, dopełniali obowiązku informacyjnego, czyli zawiadamiali, kto, w jakim zakresie i po co zbiera nasze dane. A z chwilą, gdy przestają one służyć określonej i uzasadnionej celowi – były usuwane.

ZBIGNIEW STAWARZ, ZASTĘPCA DYREKTORA BIURA KRYMINALNEGO, Z KOMENDY GŁÓWNEJ POLICJI: Internetu nie da się opanować. Nawet Chiny, gdzie jest jeden operator, nie są w stanie całkowicie kontrolować danych w internecie. Zatem uchwalanie przepisów prawnych, które mają ograniczyć tę sferę, z góry skazane jest na niepowodzenie. Jeśli bowiem istnieje przepis, to musimy mieć możliwość jego egzekwowania i zastosowania sankcji. Większość danych osobowych w sieci pochodzi od samych użytkowników. Problemem jest, jak się ustrec przed negatywnymi konsekwencjami rozpowszechniania danych prywatnych.

Do jakich naruszeń dochodzi w sieci najczęściej?

ZBIGNIEW STAWARZ: Podsywanie się pod cudzą tożsamość. Przeprowadzanie transakcji za pomocą kont, do których użytkownicy się włączają. Odnosimy też wrażenie, że coraz bardziej aktualne stają się pytania dotyczące naszego bezpieczeństwa w sieci. Uważam, że choć w internecie nie jesteśmy anonimowi, to mamy prawo do prywatności i powinniśmy o nią walczyć. Tym bardziej że ogromna ilość danych osobowych jest pozyskiwana bez naszej wiedzy i zgody. Dla przykładu wymienię stosowany przez wyszukiwarki mechanizm umożliwiający rejestrację odwiedzanych przez użytkownika stron www i tworzenie na tej podstawie profili osobowościowych. Tymczasem ta informacja w połączeniu z innymi, którymi dysponuje dostawca usług, może stanowić dane osobowe, które powinny podlegać ochronie. Dlatego jako organ do spraw ochrony danych osobowych będę zabiegał, by zgodnie z wypracowanym w Unii Europejskiej stanowiskiem, dostawcy usług internetowych, w tym operatorzy wyszukiwarek, dopełniali obowiązku informacyjnego, czyli zawiadamiali, kto, w jakim zakresie i po co zbiera nasze dane. A z chwilą, gdy przestają one służyć określonej i uzasadnionej celowi – były usuwane.

Effektem takiego włamania hakerów jest niemożność przeprowadzenia transakcji, nawet przez kilka dni. W grach komputerowych dochodzi do kradzieży niektórych jej elementów, np. świetlnych mieczy. Płaci się za takie przedmioty walutą wirtualną, ale aby je nabyć, należy zapłacić rzeczywiste pieniądze.

Przy ostatnich zmianach ustaw policja poparła wprowadzenie przepisów ułatwiających blokowanie stron. Nie możemy w przypadku fishingu w sieci banku czekać trzy dni na zezwolenie sądu. Tu trzeba działać błyskawicznie, ponieważ dochodzi do wyludzenia danych osobowych bar-



Michał Serzycki
generalny inspektor ochrony danych osobowych



Bogdan Fischer
Kancelaria Chłabas i Wspólnicy



Zbigniew Stawarz
Komenda Główna Policji



Małgorzata Kałużyńska-Jasak
rzecznik prasowy GłODO

sko, ponad 2/3 publikuje swoje zdjęcie.

MICHAŁ SERZYCKI: Ostrzegamy, że dla własnego dobra lepiej nie chwalić się posiadaniem dobrami czy zdjęciami z wakacji. Internauci mają niesłuszne przekonanie, że w sieci są anonimowi. To nieprawda. Ponadto internet jest pamiętliwy, a informacje, które tam zostają zamieszczone, bardzo trudno później usunąć, a często jest to wręcz niemożliwe.

DR BOGDAN FISCHER, KANCELARIA CHŁABAS I WSPÓLNICY: Nawet należy pójść dalej – sieć jest doskonałym miejscem gromadzenia danych osobowych.

sprawdza się. W 1997 roku wprowadzono zmiany w kodeksie karnym odnoszące się do nowych przestępstw przeciwko informacji. Adekwatnie do zagrożeń kształtuje się obecnie rozumienie tych przepisów. Świat realny i wirtualny przenikają się. Na przykład wykorzystanie środowiska gry komputerowej dla celów reklamowych rodzi wiele pytań natury prawnej w zakresie ochrony znaków towarowych wykorzystywanych w celu promocji działalności reklamodawcy. Pojawiają się usługi polegające m.in. na oferowaniu do sprzedaży (za prawdziwe pieniądze) przedmiotów funkcjonujących w świecie gry, sprzedaży stworzonej przez siebie zawartości do wykorzystania w grze bądź odpłatnego levelowania (rozbudowywania umiejętności poprzez osiągnięcie kolejnych poziomów doświadczenia) postaci innych użytkowników. Zastosowanie istniejących przepisów wymaga odpowiednich wykładni.

Czy prawne usankcjonowanie blokowania zabronionych stron internetowych jest zgodne z konstytucją?

MICHAŁ SERZYCKI: Jako organ do spraw ochrony danych osobowych uważam, że przede wszystkim to szczególne przepisy prawa muszą zezwalać na ustalanie tożsamości osób popełniających w sieci różnego rodzaju nadużycia. Niezależnie od tego, czy korzystają oni z niej jako dostawcy usług, czy jako ich użytkownicy. Gdy osoby takie dopuszczają się naruszeń obowiązujących prawa, sprawą powinny zajmować się organy właściwe do ścigania przestępstw, które działają na podstawie własnych

przepisów prawa, regulujących ich kompetencje oraz tryb prowadzenia postępowań. Jeśli zaś konieczne byłoby blokowanie stron internetowych propagujących nielegalne treści, to podejmowanie decyzji w tej sprawie przez sąd jest dobrym rozwiązaniem. Dzięki temu przed zastosowaniem tego restrykcyjnego środka dojdzie do wcześniejszego zweryfikowania prawdziwości zarzutów. Poza tym podejmowanie decyzji przez niezawisły sąd daje gwarancję rzetelnego zbadania sprawy. Niemniej trzeba też wziąć pod uwagę to, że takie blokady bardzo łatwo można obejść. Dlatego najpierw należałoby odpowiedzieć na pytanie, czy obecne przepisy nie wystarczają, by walczyć z nielegalnymi treściami w internecie. Jeśli nie, to blokowanie konkretnych stron internetowych uznalibyśmy za dopuszczalne jedynie pod kontrolą niezależnych sądów.

ZBIGNIEW STAWARZ: W świecie wirtualnym procedury blokowania administracyjnego zakładają odwołanie się do sądu. Postępowanie administracyjne w porównaniu z postępowaniem karnym jest szybsze, dlatego wydaje się skuteczniejsze.

Problem jest wyolbrzymiony. Blokowanie stron ma dotyczyć ściśle określonych poważnych przestępstw, np. tworzenia fałszywych stron bankowych. Jeśli by strony zostały zablokowane, to nie wiem, kto miałby zaskarżyć zablokowanie ich przez policję.

Obowiązkiem administratora jest zablokowanie takich treści. Przypuszczam, że przy przestępstwach internetowych w pojęciu prawa karnego trudno określić właściwość miejscową. Nie wiadomo, gdzie

przestępstwo dochodzi do skutku. Prawo karne zakłada, że przestępstwo jest ścigane, gdy nastąpi na terytorium Polski. Dowody zebrane w internecie służą sądowi w procesie o naruszenia dóbr osobistych, fałszerstwo czy wyłudzenie.

BOGDAN FISCHER: Obecnie katalog treści powodujący blokowanie jest ograniczony i nie budzi zasadniczych kontrowersji, jednak ryzyko jego rozbudowania w niedającym się przewidzieć kierunku jest znaczne. Rodzą się również dalsze pytania o aspekty techniczne utrudniania dostępu do stron i usług, problem arbitralności oceny podmiotu uprawnionego. Dyskusyjne są również inne propozycje dotyczące np. świadczenia usług drogą elektroniczną w zakresie gier hazardowych i rozszerzonej właściwości polskiego prawa.

MICHAŁ SERZYCKI: Problem prawny polega na tym, że sprawy internetowe przestępstwa trudno udowodnić winę.

Ponadto uważam, że lepiej zapobiegać, niż karać. Dlatego od chwili objęcia przeze mnie w lipcu 2006 r. stanowiska GłODO zabiegam o nawiązanie współpracy z różnymi środowiskami, dzięki której ich przedstawiciele opracowują tzw. kodeksy dobrych praktyk, czyli samoregulacji zawierających reguły postępowania dotyczące zgodnego z prawem przetwarzania danych osobowych. Kodeksy takie powstały dotychczas dla takich sektorów, jak bankowość, nieruchomości, marketing bezpośredni czy Kościół.

Dyskusję prowadziła Katarzyna Zaczekiewicz

Blokowanie stron internetowych musi odbywać się na przejrzystych zasadach i pod kontrolą sądu

dzo wrażliwych, takich jak konta, logowanie, numery kart kredytowych, które umożliwiają nielegalny przelew. Takich przestępstw będzie coraz więcej.

MAŁGORZATA KAŁUŻYŃSKA-JASAK, RZECZNIK PRASOWY GŁODO: Sondaż przeprowadzony przez PBI (Polskie Badania Internetu) wskazuje, że tylko 2 proc. internautów nie umieściło żadnych informacji w internecie na swój temat, a aż 24 proc. nie kasuje swoich nie używanych kont. Dziewięć na 10 osób podaje w internecie

Obecnie nie powinno się już dokonywać rozróżnienia na rzeczywistość realną i wirtualną, np. e-urzędy i urzędy to jest jeden świat. Przez lata zastanawiano się, czy nie uregulować w jednej ustawie zasad postępowania w internecie. Trudno nadążyć za dokonującymi się zmianami i objąć wszystko regulacjami. Stąd też może przewrotnie należało stwierdzić, iż nie należy wydzielać prawa internetu, ale starać się korzystać z tradycyjnych konstrukcji. Powinniśmy więc stosować przepisy, które już funkcjonują. Dążenie do neutralności technologicznej w tworzeniu przepisów