

**PRAWO** Nowa dyrektywa Unii Europejskiej nakazuje operatorom śledzić e-maile oraz internetowe rozmowy

# Internet pod ścisłą kontrolą

**Ilona Blicharz**  
dziennikarka działu kraj

Od poniedziałku dostawcy internetu mają obowiązek zapisywać, z kim kontaktujemy się przez sieć. A w szczególnych przypadkach będą musieli gromadzić e-maile i nagrywać rozmowy z komunikatorów głosowych.

Wszystko przez unijną dyrektywę telekomunikacyjną, która narzuca krajom członkowskim zaostrezone zasady bezpieczeństwa. Chodzi o lepsze możliwości śledzenia terrorystów, którzy wykorzystują nowe technologie do komunikacji. Jednak eksperci w sprawach ochrony danych osobowych obawiają się nowych rozwiązań.

Polskie władze w dużym pośpiechu nowelizują prawo telekomunikacyjne. Wprowadzenie nowych przepisów, ale tylko nieznacznie. Teoretycznie już w poniedziałek operatorzy mogą zacząć inwestować w serwery, które mają archiwizować dane spływające od milionów internautów w Polsce. – Nowelizacja ustawy Prawo telekomunikacyjne z Senatu trafiła do Sejmu. Jeśli proces legislacyjny będzie przebiegał sprawnie, zostanie zaraz przyjęta – mówi rzecznik

**Każdy dostawca internetu musi gromadzić dane o tym, kto i do kogo wysyłał e-maile lub z kim rozmawiał przez komunikatory**

Ministerstwa Infrastruktury Mikołaj Karpiński.

Dzięki wprowadzeniu nowego prawa odpowiedzialne za bezpieczeństwo służby dostaną nową broń w walce z przestępcami. Będą miały dostęp do baz danych, pokazujących kto, do kogo i kiedy wysłał e-maila. Będą mogły zmusić operatorów do składowania treści tych e-maili i nagrywania rozmów prowadzonych np. przez Skype'a.

– Mogą zażądać historii e-mailowej korespondencji bez nakazu sądowego – mówi mec. Wacław Knopkiewicz, specjalista od prawa telekomunikacyjnego w kancelarii Grynhoff Woźny Maliński. – Dotyczy to wszystkich przestępstw. Nie tylko poważnych, jak mówi o tym dyrektywa – dodaje.

Każdy dostawca internetu będzie musiał archiwizować dane przez 12 miesięcy. Podniesie to koszt działania operatorów, który w konsekwencji zostanie przerzucony na klientów. – Takie bazy będą

kosztować operatorów setki milionów złotych – mówi rzecznik Urzędu Komunikacji Elektronicznej Jacek Strzałkowski. – Potrzebne będą dodatkowe serwery, trzeba będzie rozbudować pomieszczenia i stworzyć odpowiednie zabezpieczenia – tłumaczy rzecznik Grupy TP Wojciech Jabczyński.

Właśnie te zabezpieczenia budzą największe kontrowersje. Zresztą dyrektywa budzi wątpliwości nie tylko w Polsce. Szwecja stanowczo sprzeciwia się nowym przepisom, a w Niemczech wytyczne trafiły już nawet do sądu.

Skąd te sprzeciwy? – Dyrektywa jest niebezpieczna, bo zagraża prywatności – mówi nam Michał Serzycki, generalny inspektor ochrony danych osobowych. – Od zamachu na World Trade Center walczyliśmy między prawem do prywatności a do bezpieczeństwa. Najczęściej wygrywa to drugie. Ale w tym przypadku mam wątpliwości. Co to znaczy, że dane będą wykorzystywane w przypadku poważnych przestępstw? Jakiego organu będą mogły z nich korzystać? Czy zabezpieczenia są wystarczające? Czy kolejna władza nie rozszerzy przepisów tak, żeby dać dostęp do nich szerszemu gronu? Na te pytania nie ma odpowiedzi – mówi Serzycki.

*usłópraca Barbara Sowa*

## Hakerzy mogą przejąć dane

**ILONA BLICHARZ:** Od poniedziałku każdy operator internetowy będzie musiał przez rok gromadzić informacje o wysyłanych przez nas e-mailach. Czy rodzi to jakieś niebezpieczeństwo?

**PAWEŁ ODOR\*:** Tak, i to bardzo duże. Taką bazą zainteresowane będą nie tylko nasze służby specjalne. To są cenne dane, na których można nieźle zarobić. Chętni na nie mogą być np. spamerzy, którzy będą mieli dostęp do milionów adresów e-mailowych, czy też firmy, dla których takie informacje byłyby marketingową żyłą złota. Nie wykluczam też zainteresowania ze strony służb bezpieczeństwa innych krajów.

**Jakie jest zagrożenie wycieku e-mailowych adresów?**

Ryzyko jest większe niż w przypadku papierowych danych, bo te można zamknąć w sejfie, do którego klucz ma tylko jedna osoba. Gromadzenie informacji o kontaktach internetowych będzie odbywać się w czasie rzeczywistym, dlatego istnieje możliwość ich przechwycenia np. podczas przesyłania lub gromadzenia. Zawsze może też dojść do ataku hakerów. Im



**Paweł Odor**

tańsze i gorsze zabezpieczenia, tym o taki wyciek łatwiej. A nawet najbardziej skuteczne zabezpieczenia nie pomogą, jeśli któryś z pracowników nadzorujących bazę zdecyduje wykraść te informacje.

**Jak wobec tego można je zabezpieczyć?**

Zwykły użytkownik nic nie może zrobić. Cała odpowiedzialność spada na operatorów. Potrzebni są profesjonalnie przeszkoleni pracownicy oraz specjalne programy zabezpieczające.

**Ile kosztuje cała baza?**

Samo „złapanie” adresów nie jest zbyt dużym problemem finansowym. Koszty pojawiają się w chwili, gdy trzeba je będzie zmagazynować, zabezpieczyć i udostępnić, a później

jeszcze odpowiednio skasować. Trzymanie naszych adresów e-mailowych przez rok wydaje się krótkim czasem, ale pomyślmy, ile przez ten czas wysyłamy e-maili. Można oszacować, że na same dyski trzeba będzie wydać około 10 złotych na tysiąc użytkowników sieci. To nie wszystko. Trzeba będzie również zapłacić za zabezpieczenia oraz oprogramowanie, które pozwoli szybko wyszukiwać i ewentualnie wyjąć potrzebne adresy. Poza tym ktoś tym musi zarządzać i tego pilnować. No i na koniec dane muszą być tak skasowane, żeby nikt niepowołany nie mógł ich odzyskać.

**Czy można liczyć na to, że stworzenie takiej bazy wystraszy np. spamatorów?**

Niestety nie. Po wysyłanych e-mailach jest praktycznie niemożliwością sprawdzenie, kim jest spamer i skąd wysłał niechciane informacje. Zresztą, o ile wiem, ta ustawa na razie nie będzie wykorzystywana do zwalczania tego typu przestępstw...

\*Paweł Odor, główny specjalista firmy Kroll Ontract w Polsce, ekspert od bezpieczeństwa w sieci