

# Urządzenia mobilne poza kontrolą

Smartfony i tablety szpiegują bezustannie, przesyłając olbrzymie ilości informacji na temat ich właścicieli. I prywatności **nie zagwarantują** nawet najlepsze przepisy prawne

**Sławomir Wikariak**  
slawomir.wikariak@infor.pl

Kontakty zapisane w komórce, adresy e-mail znajomych, liczona z dokładnością do kilku metrów lokalizacja, w której przebywał użytkownik o konkretnej godzinie – to tylko przykładowe informacje, które są przesyłane – często bez naszej wiedzy – z naszych smartfonów.

– Tych urządzeń jest coraz więcej, używane są coraz powszechniej, a my tak naprawdę nie wiemy, co one robią z naszymi danymi – tłumaczył dr Wojciech Rafał Wiewiórowski, generalny inspektor ochrony danych osobowych, podczas debaty zorganizowanej przez Dziennik Gazetę Prawną.

– Przy czym mam na myśli nie tylko smartfony czy tablety. Dla przykładu – nowoczesne samochody są także urządzeniami mobilnymi. Przesyłają informacje nie tylko o swoim położeniu czy usterkach. Mało kto zdaje sobie sprawę, że synchronizując komputer pokładowy ze smartfonem, po to by np. posłuchać muzyki, jednocześnie kopiowana jest książka adresowa i wiele innych informacji, do których może mieć później dostęp punkt serwisowy – dodawał.

## Permanentna inwigilacja

Chociaż uczestnicy debaty nie byli zgodni, czy nową rzeczywistość można skutecznie uregulować prawnie, to co do jednego nikt nie miał wątpliwości. Mało kto z nas zdaje sobie sprawę z tego, jak głębokiej infiltracji podlegamy w każdej chwili.

– Nawet z pozoru najmniej groźna aplikacja instalowana w smartfonie może naruszać naszą prywatność. Okazało się np., że zwykła latarka, poza tym, że świeci, równocześnie transferuje dane z książki adresowej telefonu – zauważył Maciej Groń, dyrektor departamentu społeczeństwa informacyjnego w Ministerstwie Administracji i Cyfryzacji.

– Były przypadki aplikacji dużych i znanych firm, takich jak chociażby Twitter, które

cichaczem przesyłały całe książki adresowe na serwer. Teoretycznie robiły to po to, by ułatwić ludziom życie. Jeśli za jakiś czas okaże się, że ktoś z tego samego e-maila, który mieliśmy w swej skrzynce, zarejestruje się na Twitterze, to serwis będzie mógł nam zasugerować, że jest to ktoś znajomy. W efekcie nawet dane osób, które celowo nie korzystają z takich serwisów, by chronić swą prywatność, i tak są gromadzone na serwerach – relacjonuje Piotr Konieczny, ekspert z serwisu Niebezpiecznik.pl.

Informacje na temat użytkowników są coraz atrakcyjniejszym towarem. To one pozwalają na profilowanie np. konsumentów. Dzięki nim firma, która zna nasze zachowania w sieci, może chociażby zaproponować nam towary, którymi możemy być zainteresowani.

To jedynie wierzchołek góry lodowej. Dane na nasz

## Najlepszym sposobem na zmniejszenie zagrożenia jest edukacja

temat przedstawiają coraz większą wartość dla coraz szerszej grupy odbiorców.

– Nie jest tajemnicą, że firmy oferujące ubezpieczenia na życie odchodzą od obowiązkowych badań zdrowotnych właśnie na rzecz pozyskiwania informacji na nasz temat z sieci. Okazuje się, że na podstawie naszego zachowania w internecie można równie skutecznie przewidzieć ryzyko zachorowania na określone choroby. A pozyskanie tych danych jest wielokrotnie tańsze od badań lekarskich – zauważył dr Arwid Mednis, partner w kancelarii Wierzbowski Eversheds i Wykładowca Uniwersytetu Warszawskiego.

## Identyfikowanie zagrożeń

Opisane praktyki bez wątpienia mogą naruszać prywatność użytkowników. Dlatego

też czas odpowiedzieć sobie na pytanie, czy w tę sferę nie powinno wkroczyć prawo. Dyskusja na temat urządzeń mobilnych jest jednym z elementów tegorocznego VIII Dnia Ochrony Danych Osobowych, który obchodzony będzie 28 stycznia. Z tych samych względów DGP zorganizował debatę poświęconą temu zagadnieniu.

– Jesteśmy dopiero na początku drogi i raczej identyfikujemy potencjalne problemy, niż je rozwiązujemy. Przed nami konieczność uzyskania odpowiedzi na wiele pytań, jak choćby te, za co jest odpowiedzialny operator, a za co dostawca oprogramowania, jaki model ich odpowiedzialności przyjąć. To tylko najbardziej podstawowe z nich – podkreśla dr Wojciech R. Wiewiórowski.

Wiele smartfonów klienci kupują u operatorów. Dostają urządzenie z wgranym systemem i pewnymi aplikacjami. Zaraz po włączeniu może więc ono przysłać wiele danych na temat użytkowników. Może więc to operator powinien zadbać o naszą prywatność?

– Trudno by mu było brać odpowiedzialność za to, co robi urządzenie. Przychodzi ono do operatora z zainstalowanym oprogramowaniem. Smutna prawda jest taka, że operator nie ma możliwości sprawdzić, co w nim się znajduje. Nie wie nawet, dokąd tak naprawdę są transferowane dane ze smartfonów – wyjaśnił dr Wacław Iszkowski, prezes Polskiej Izby Informatyki i Telekomunikacji.

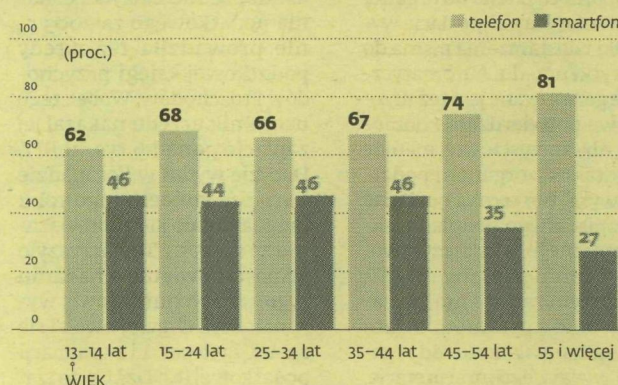
– Dlatego też uważam, że jakiegokolwiek próby nałożenia odpowiedzialności na operatorów są z góry skazane na niepowodzenie. To po prostu będzie martwe prawo – zaznaczył.

GIODO uważa zaś, że operator ma pewne zobowiązania wobec nabywcy smartfonu.

– Operator już teraz odpowiada za sprzedawane wraz z pakietem usług urządzenie na podstawie przepisów o ochronie konsumentów, podobnie jak sprzedawca

## Coraz więcej użytkowników smartfonów

### 13,5 MLN SMARTFONÓW POSIADAJĄ POLACY



Chociaż na razie większość telefonów używanych przez Polaków wciąż stanowią urządzenia starego typu, to już ten rok w grupie wiekowej 25-44 lata może przynieść odwrócenie tego trendu i przewagę smartfonów. Największe przywiązanie do komórek starego typu wykazują starsi użytkownicy, zwłaszcza z grupy powyżej 55 lat.

**56 MLN** kart SIM (zarówno abonamentowych, jak i przedpłaconych) działa w Polsce

**54 PROC.** użytkowników korzysta z kart przedpłaconych

**5,9 MLN** abonentów ma polska sieć telefonii stacjonarnej

**8,3 PROC.** o tyle potaniały w ub.r. usługi związane z łącznością

Źródło: raport Generation Mobile 2013, dane Głównego Urzędu Statystycznego na koniec III kwartału 2013 r.

każdego innego produktu – polemizował dr Wojciech Wiewiórowski.

Nikt nie ma jednak wątpliwości, że operator nie może odpowiadać za aplikacje instalowane przez użytkownika. Tu pewne obowiązki powinien mieć dostawca oprogramowania. Problem w tym, że najczęściej jest to firma zagraniczna mająca siedzibę w USA czy Chinach. Nawet, gdy producentem jest polska firma, to też zazwyczaj sprzedaje aplikacje za pośrednictwem sklepów działających pod rządami obcego prawa. Dlatego też polskie ustawodawstwo na niewiele się tu zda.

– Spore nadzieje pokładam w projektowanym rozporządzeniu unijnym o ochronie danych osobowych. Jednolite przepisy mające zastosowanie w całej Unii Europejskiej będą miały dużo większą wagę niż

odrębne w każdym z krajów z osobna. Inna też będzie pozycja negocjacyjna przy konstruowaniu ewentualnych porozumień z krajami takimi jak USA czy Chiny, gdy partnerem będzie cała UE, a nie każdy z jej członków osobno – zaznacza Maciej Groń z MAiC.

Patrząc realistycznie, nie ma jednak szans na to, by nowe unijne przepisy zostały przyjęte w obecnej kadencji Parlamentu Europejskiego.

## Przed wszystkim edukacja

Pojawia się zresztą pytanie, czy prawo jest w stanie zapewnić nam prywatność w dobie powszechnego korzystania ze smartfonów.

– Oczywiście, że nie. Zakusy uregulowania tego są z góry skazane na niepowodzenie – ocenił dr Wacław Iszkowski.

Doktor Arwid Mednis również powątpiewał w skuteczność regulacji prawnych. Co jednak, jego zdaniem, nie oznacza, że przepisy nie powinny nakładać pewnych obowiązków, chociażby informacyjnych. Konsument ma prawo wiedzieć, że jakieś dane z używanego przez niego urządzenia będą gdzieś przesyłane.

Innym ze sposobów na cywilizowanie branży urządzeń mobilnych mogłyby być dobrowolne certyfikaty. Klienci wiedzieliby, że instalując certyfikowane oprogramowanie, mają przynajmniej prawo do informacji, kto i jakie dane na ich temat będzie zbierał.

– Dokładne sprawdzenie aplikacji pewnie byłoby trudne, niemniej jednak w jakimś zakresie możliwe – przyznał Piotr Konieczny.

– Porównałbym to do oprogramowania pozwalającego na dostęp do bankowości internetowej. Już dzisiaj banki weryfikują je po kątem bezpieczeństwa, gdyż ewentualne błędy mogłyby narazić je na spore koszty – wyjaśnił.

Najważniejsza jest jednak edukacja. To użytkownicy ostatecznie bowiem decydują, jakie dane trafiają do usługodawców. Muszą pamiętać, że chodzi nie tylko o informacje na ich temat, ale także o osobach, z którymi utrzymują kontakt.

Zdaniem GIODO uświadamianie należy zacząć już w szkołach.

– Chodzi przy tym o edukację rozumianą nie jako kolejne pogadanki, tylko pokazanie problemu od strony jak najbardziej praktycznej. Na lekcji języka angielskiego możemy omawiać dany czas zarówno na przykładzie Big Bena, jak i tego, jakie informacje na nasz temat są gromadzone i przekazywane przez urządzenia mobilne oraz jakie to rodzi zagrożenia – zauważył dr Wojciech R. Wiewiórowski.

**Czytaj też na**  
**www.gazetaprawna.pl**

**Szerszy zapis debaty ukaże się w jednym z najbliższych wydań Prawnika – tygodnika dla prenumeratorów**