



DR WOJCIECH RAFAŁ WIEWIÓROWSKI
generalny inspektor ochrony danych osobowych



MACIEJ GROŃ
dyrektor Departamentu społeczeństwa informacyjnego w Ministerstwie Administracji i Cyfryzacji



PIOTR KONIECZNY
kierownik zespołu bezpieczeństwa Niebezpiecznik.pl



DR WACŁAW ISZKOWSKI
prezes Polskiej Izby Informatyki i Telekomunikacji



DR ARWID MEDNIS
partner w kancelarii Wierzbowski Eversheds, pracownik Wydziału Prawa i Administracji Uniwersytetu Warszawskiego

Ludzie mają prawo wiedzieć, czy telefon ich szpieguje



Kto ponosi odpowiedzialność za to, co robi smartfon? Jakie dane i dokąd mogą być transferowane? Czy prawo jest w stanie nadążyć za technologią? Zastanawiali się nad tym uczestnicy debaty DGP. Prowadził ją Sławomir Wikariak

Dlaczego dyskutujemy o smartfonach?

Wojciech Rafał Wiewiórowski Rzecznicy ochrony danych osobowych zajęli się tematem aplikacji i urządzeń mobilnych z prostego powodu. Są one już używane powszechnie, a wciąż tak naprawdę nie wiemy, co robią z naszymi danymi. Zastanawialiśmy się nad tym na zorganizowanej w minionym roku w Warszawie 35. Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności. I przyznajemy się do tego, że posiadamy zbyt małą ilość informacji, by zrozumieć świat aplikacji mobilnych. Na razie stawiamy pytania. Szczegrze mówiąc, zastanawiamy się, dlaczego dotychczas nikt ich nie sformułował. Wydaje się, że np. operator telekomunikacyjny powinien być zainteresowany tym, co robią aplikacje zainstalowane w telefonie sprzedawanym przez niego wraz z usługą telekomunikacyjną.

Arwid Mednis Rzeczywiście w tej chwili najważniejsze jest zrobienie swego rodzaju inwentaryzacji i sprawdzenie, jak działają aplikacje mobilne, bo na razie tak naprawdę jeszcze mało o nich wiemy. Przede wszystkim musimy się upewnić, jakie dane zbiera się za ich pomocą i kto

ma do tych danych dostęp. Dopiero wtedy będziemy mogli zastanawiać się na ujęciem tego w normy prawne.

Wiemy już jednak, że problem bez wątpienia istnieje. Urządzenia, którymi się posługujemy, gromadzą na nasz temat naprawdę olbrzymią ilość informacji, które mogą zostać wykorzystane do najróżniejszych celów. Na przykład 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 sieci można równie skutecznie przewidzieć ryzyko zachorowania na określone choroby, jak na podstawie testów DNA czy badania krwi. A pozyskanie tych danych jest wielokrotnie tańsze od badań lekarskich. Wszystko więc, co trafia do sieci na nasz temat, może być wykorzystane do celów, których nie możemy przewidzieć w chwili, gdy te dane udostępniamy, również za pomocą aplikacji mobilnych.

Maciej Groń Problem ten jest z jednej strony nowy, z drugiej jednak – jest kontynuacją tych wszystkich zagadnień, z jakimi mamy do czynienia od wielu

lat, używając internetu. Teraz zaczyna być o tyle istotny, że liczba używanych w Polsce smartfonów czy tabletów rośnie bardzo szybko. A to rzeczywiście oznacza, że trzeba się będzie zmierzyć z tym zjawiskiem od strony prawnej i zaproponować sposób jego uregulowania. Przy czym nowe technologie wymagają od nas odejścia od pozytywistycznego podejścia do prawa. Chodzi o to, by przepisy nie były zbyt szczegółowe. Chociaż w pewnym sensie mogłoby to być wygodniejsze dla użytkowników i administratorów danych osobowych, to jednocześnie takie prawo natychmiast by się dezaktualizowało. Prawo nie jest w stanie przewidzieć każdej nowej technologii, która za chwilę się pojawi. Dlatego bardziej powinno opierać się na analizie ryzyka i uwzględniać samo zagadnienie ochrony danych, niż to, w jaki sposób są one przetwarzane.

Kto i za co odpowiada?

Wojciech Rafał Wiewiórowski Pierwsze pytanie, jakie my, rzecznicy ochrony danych osobowych, musimy sobie postawić jako regulatorzy, brzmi: kto odpowiada za dane przekazywane przez urządzenia mobilne. W jakim zakresie odpowiada za

nie operator telekomunikacyjny, u którego najczęściej kupujemy te gadżety, jakimi są smartfon czy tablet. W jakim zakresie ten, który stworzył system operacyjny lub aplikację, a w jakim wreszcie sam użytkownik. To zresztą dopiero początek drogi, jaką pokonują dane wysyłane z urządzeń mobilnych. Bo często są one przekazywane dalej. Komu i za co ten ktoś odpowiada? To kolejne pytania.

Wacław Iszkowski Operatorzy, którzy rzeczywiście często sprzedają te urządzenia razem z usługą, tak naprawdę nie mają i nie mogą mieć pojęcia o tym, co te urządzenia mają w środku. Dlatego obarczanie ich odpowiedzialnością jest z góry pozbawione sensu. Oni zwyczajnie nie mają informacji o działaniu fabrycznie zainstalowanych aplikacji – czy przy okazji widocznych funkcji nie dokonują jeszcze tajemnego gromadzenia informacji, przesyłając je następnie na serwer ich producenta.

Dodatkowo większość użytkowników prawie natychmiast instaluje nowe aplikacje oraz uaktualnia te już przez nich używane. Czy operator ma kontrolować każdego ze swoich abonentów jak ten korzysta z dostarczonego smartfona czy tabletu?

Wojciech Rafał Wiewiórowski Pozwolę sobie nie zgodzić się z tym poglądem. Na tym pierwszym etapie sytuacja jest prosta. Za urządzenie odpowiada ten, kto je sprzedaje. Podobnie jak z komputerem – jeśli jest na nim zainstalowane jakieś oprogramowanie, to również odpowiada za nie sprzedawca. Ta odpowiedzialność wynika nawet nie z przepisów o ochronie danych osobowych, tylko z regulacji o ochronie konsumentów. Zgodzę się natomiast, że za to, co robi każda aplikacja zainstalowana później przez

użytkownika, operator nie ponosi już odpowiedzialności. Podobnie jak za urządzenie, które jest kupione od innego sprzedawcy niż operator, do którego ktoś następnie włoży kartę SIM.

Wacław Iszkowski Za oprogramowanie zainstalowane na komputerze, tablecie czy smartfonie odpowiada przede wszystkim producent tego oprogramowania. Oczywiście za oprogramowanie zainstalowane fabrycznie jakąś część odpowiedzialności bierze producent urządzenia i może nawet sprzedawca. Ale warto pamiętać, że z innego prawa – prawa autorskiego nie wolno dokonywać de-assembly oprogramowania – inaczej mówiąc – samodzielnie go analizować bez zgody jego autora i producenta. Nie wspomnę tutaj o kosztach takiej weryfikacji.

Dlatego nie widzę sensu w czynieniu producenta, sprzedawcy czy operatora odpowiedzialnym za coś, na co nie tylko nie ma wpływu, ale nawet nie jest w stanie tego zweryfikować. A tak naprawdę o tym, co rzeczywiście robi dane urządzenie, mają wiedzę jedynie Chińczycy, którzy mieli do niego – jako ostatni – dostęp podczas produkcji. Nikt z nas nie wie, czy leżące teraz przed nami telefony nie wysyłają gdzieś danych i to nawet jeśli je odłączymy od sieci i nawet wyłączymy.

Piotr Konieczny To prawda, że generalnie nie wiadomo, co się dzieje w telefonie, ale jeśli ktoś chce, to może się tego dowiedzieć. Aplikacje, które szyfrują przesyłane dane, mogą być problematyczne, ale nawet przy całym zamieszaniu związanym ze Snowdenem nadal zdecydowana większość producentów nie korzysta z szyfrowania. A to oznacza, że stosunkowo łatwo można sprawdzić, jakie dane przesyła konkretna aplikacja. Zresztą nawet jeśli aplikacja szyfruje dane, to i tak pewne informacje są możliwe do odczytania. Adres IP serwera na jaki przesyłane są dane, zawsze jest widoczny dla operatora. Innymi słowy, może on nie wiedzieć, jakie dane są przesyłane, ale wie, dokąd, kiedy i jak często trafiają.

Dokąd trafiają informacje?

Arwid Mednis Zgadzam się z poglądem, że nie jest potrzebne tworzenie osobnych regulacji dla urządzeń mobilnych. Podobne aplikacje mogą działać na komputerach, smartfonach czy tabletach. Liczy się to, kto te dane de facto zbiera i do czego je wykorzystuje. Główny problem to oczywiście skala. Dawniej dane z naszych urządzeń gromadzili przede wszystkim operatorzy telekomunikacji. Teraz zdecydowanie więcej zbierają dostawcy oprogramowania, twórcy aplikacji itp. Zresztą niekoniecznie związani, przynajmniej na pierwszy rzut oka, z komputerami czy nawet urządzeniami mobilnymi. Niedawno duży amerykański koncern motoryzacyjny prezentując nowe modele samochodów, przyznał, że będą one zbierać różne dane, np. na temat prędkości, bo chce wiedzieć, jakie grzechy popełniają kierowcy. Wszystko to jest pewnie robione w złośliwym celu, niemniej może to budzić pewien niepokój.



Okazuje się, że na podstawie naszego zachowania w sieci można równie skutecznie przewidzieć ryzyko zachorowania na określone choroby, jak na podstawie testów DNA czy badania krwi. A pozyskanie tych danych jest wielokrotnie tańsze. I firmy ubezpieczeniowe z tej drogi korzystają

Piotr Konieczny Na danych z samochodów firmy już teraz zarabiają. Znany producent nawigacji samochodowej Tom Tom przyznał niedawno, że sprzedaje policji dane dotyczące prędkości, z jaką poruszają się kierowcy. Ta zaś dzięki nim decyduje, gdzie stawiać radary. Oczywiście firma zapewnia, że dane te są zanonimizowane, niemniej jednak pokazuje to wyraźnie, jak wiele informacji zbierają na nasz temat różne urządzenia.

Były przypadki aplikacji bardzo znanych, poważnych firm, typu Twitter lub Facebook, które cichaczem przesyłały całe książki adresowe na serwery. Teoretycznie robiły to po to, by ułatwić ludziom wyszukiwanie ich znajomych. Jeśli ktoś z tego samego e-maila, który mieliśmy w swej książce adresowej, zarejestrował się w serwisie, to aplikacja mogła nam zasugerować nawiązanie kontaktu z tym znajomym. Tylko że przy takim modelu działania, nawet dane osób, które celowo nie korzystają z Twittera czy Facebooka, by chronić swą prywatność, i tak są gromadzone na jego serwerach. Nawet jeśli unikamy Facebooka, to z dużym prawdopodobieństwem można założyć, że i tak ma on nasze dane, bo ktoś inny je mu udostępnił. Albo świadomie, albo nieświadomie.

Wojciech Rafał Wiewiórowski Rzeczywiście, chociaż najczęściej mówimy o smartfonach czy tabletach, to problem jest dużo szerszy. Dla przykładu – nowoczesne samochody są także mobilnymi urządzeniami wysyłającymi i odbierającymi dane. Przesyłają informacje nie tylko o położeniu czy usterkach. Mało kto zdaje sobie sprawę, że gdy synchronizujemy 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.

Maciej Groń 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. Po co producentowi aplikacji, która zamienia smartfona w latarkę, te informacje? Możemy się jedynie domyślać.

Takie przykłady można mnożyć. Bez wątplenia pokazuje to, że problem wymaga rozwiązań prawnych.

Arwid Mednis Niestety nie bardzo wierzę w ich skuteczność. Nawet jeśli w Unii Europejskiej wejdzie w życie rozporządzenie dotyczące ochrony danych osobowych, o którym tak długo już słyszymy, to jakie ono będzie miało znaczenie dla firm z Chin? Żadne. Dane z naszych telefonów nadal będą do nich przesyłane i nic nie będziemy mogli na to poradzić. Jeśli przyjdzie zagłada dla naszej prywatności, to będzie ona wynikać z efektu skali. Po prostu podmiotów zbierających dane z naszych telefonów będzie tak wiele i będą pochodzić z tak różnych miejsc na świecie, że żadna regulacja prawna nie będzie w stanie nad tym zapanować.

Maciej Groń Właściwym kierunkiem są bez wątpienia umowy międzynarodowe, a zwłaszcza takie, które obejmą jak największą grupę państw. Niemniej jednak powinniśmy zacząć od Unii Europejskiej. Mam duże oczekiwania zwłaszcza co do rozporządzenia unijnego dotyczącego ochrony danych osobowych, nad którym prace trwają już zresztą dwa lata. Nie chodzi tylko o to, że to rozporządzenie ujednolici standardy w całej Unii Europejskiej. Chodzi o to, by Unia Europejska mogła w rozmowach z państwami trzecimi mówić jednym głosem i promować swoje rozwiązania. Poszczególne kraje Unii nie są bowiem wystarczająco silnymi partnerami do rozmów, które mogłyby narzucić innym krajom pewne standardy dotyczące ochrony prywatności. Cała Unia Europejska jest już natomiast równorzędnym partnerem do rozmów nawet z USA czy Chinami. A to te kraje nadają ton, jeśli chodzi o nowe technologie.



Nowe rozporządzenie unijne dotyczące ochrony danych osobowych będzie kładło spory nacisk na certyfikaty. A najgorsze, co mogłoby się wydarzyć, to gdyby nie istniały one na polskim rynku i nasi przedsiębiorcy musieliby certyfikować się np. w Luksemburgu

Wojciech Rafał Wiewiórowski Ja jednak tak do końca nie deprecjonowałbym prawa krajowego. Są pewne elementy, które właśnie przepisy krajowe regulują i powinny regulować. Mam na myśli zwłaszcza zasady przekazywania informacji służbom takim jak policja czy prokuratura, a nawet sądy. Zasady te są regulowane głównie przez prawo krajowe. To ono decyduje, jakie informacje mogą być przekazane w procesie karnym, a jakie w procesie cywilnym. To ono reguluje, co i komu wolno.

Czy prawo coś zmieni?

Piotr Konieczny Warto postawić sobie pytanie o skuteczność regulacji prawnych. Przykładem mogą być cookies, o których od pewnego czasu muszą nas informować strony internetowe. Być może nieco zwiększyło to świadomość obywateli, do czego są one wykorzystywane, jednak zdecydowana większość ludzi po prostu automatycznie kilka „OK”, tylko po to, by informacja o cookies, która przysłania pół ekranu, jak najszybciej zniknęła. Powiem coś, co może niektórych zaskoczy, ale i bez cookies firmy marketingowe mogą zbierać dokładnie te same informacje na nasze temat – da się to zrobić, nie pozostawiając niczego w naszych komputerach, a zatem nie podpadając pod przepis, który wymaga informowania o tym. Dlatego też zdecydowanie zgadzam się z tezą, że prawo nie nadąża za technologią. I to chyba nigdy nie będzie nadążać.

Wacław Iszkowski Od razu dopowiem, że żadne prawo nic tu nie zmieni. Możemy mnożyć nakazy i zakazy, ale zostaną one martwe. Czy producent z Chin albo firm z USA przejmie się nimi? Oczywiście, że nie. Z kolei polscy operatorzy zwyczajnie nie mogą być obciążani odpowiedzialnością za to, co robią urządzenia. I mówię to, chociaż sam doświadczyłem sytuacji, gdy mój smartfon po włączeniu po przylocie do Kanady bez mojej świadomości przetransferował 59 MB danych. I niestety nie ma takiego prawa, które zmusiłoby operatora kanadyjskiego do poinformowania mnie, kto i po co to zrobił – a musiałem za to zapłacić coś ponad 1500 zł.

Wojciech Rafał Wiewiórowski Dlatego raczej nie szedłbym w stronę zwiększania nakazów i zakazów, a rozwiązanie widziałbym w samoregulacji rynku. Jednym ze sposobów mogą być certyfikaty poświadczające zachowywanie pewnych standardów ochrony prywatności. Oczywiście trzeba się zastanowić, kto miałby wydawać takie certyfikaty. Dyskusji wymaga też kwestia, co powinno być badane podczas procesu certyfikacyjnego.

Wacław Iszkowski Taka certyfikacja jest zwyczajnie niewykonalna. Co miałaby ona dawać? Jakie znaczenie miałby taki certyfikat? Jak długo byłby ważny, skoro przy kolejnej aktualizacji oprogramowania mogłoby ono już mieć dodatkowe funkcje, których nie miało podczas procesu certyfikacji?

Poza tym proszę pamiętać, że te urządzenia, które dzisiaj mamy, już za chwilę będą wyglądać i działać zupełnie inaczej. Gdy przed kilkunastu laty oglądaliśmy film „Raport mniejszości” to myśleliśmy, że scenarzyści mieli bogatą wyobraźnię – między innymi pokazując identyfikowanie osób w centrum handlowym. A te technologie już wtedy były już używane. Trudno mówić o możli-

wości certyfikowania czegoś, co zmienia się w takim tempie. Jedynie możemy tutaj korzystać z zaufania do firmy sprzedającej nam daną aplikację, że nie wykorzysta ona nas czy naszych danych przeciwko nam. Ale ze sprawy Snowdena wiemy, że nawet bardzo zaufane firmy musiały udostępniać dane NSA.

Piotr Konieczny Certyfikacja, przynajmniej w pewnym zakresie, jest jednak możliwa, co pokazuje chociażby przykład Apple. Aplikacje, które trafiają do sprzedaży w sklepie tej firmy, muszą przejść przez proces weryfikacji, chociażby po to, by sprawdzić, czy nie dublują funkcji programów produkowanych przez samo Apple i nie podkopują ich pozycji rynkowej. Skoro już teraz firma to robi, to nie widzę przeciwwskazań, aby również wymóc na niej weryfikację pewnych, określonych prawem zasad ochrony prywatności. Zresztą Google, chociaż w mniejszym zakresie, także bada oprogramowanie, głównie pod kątem tego, czy nie jest złośliwe – niestety opisanie reguł dotyczących ochrony danych osobowych jest pewnie o kilka stopni bardziej skomplikowane niż wyszukanie konkretnego złośliwego fragmentu w kodzie aplikacji. Sama certyfikacja jest jednak wykonalna, czego dobrym przykładem są banki, które dostarczają oprogramowanie mobilne do obsługi kont. Gdyby aplikacje te nie dochowywały prawnych obowiązków nałożonych na banki, to groziłoby im wysokie kary i negatywna prasa. Między innymi z tego powodu starają się drobiazgowo weryfikować wypuszczane przez siebie oprogramowanie.

Czy certyfikować dobrowolnie, czy z przymusu?

Arwid Mednis Certyfikacja jest pewnym rozwiązaniem, przy czym ja raczej opowiadałbym się za dobrowolnością niż narzucaniem obowiązków certyfikacyjnych. Oczywiście certyfikaty te mogłyby mieć różny zakres i potwierdzać spełnienie różnych norm. To jednak również pozostawiłbym do uregulowania przez sam rynek, licząc na to, że różnego rodzaju bonusy związane chociażby z możliwością wejścia do sklepu certyfikowanego oprogramowania nakłonią jego producentów do tego, by sami chcieli przechodzić taką weryfikację.

Wojciech Rafał Wiewiórowski Certyfikacja to jedno z poważniejszych wyzwań, jakie staną przed GIODO w najbliższych latach. Wspominane już tutaj nowe rozporządzenie unijne dotyczące ochrony danych osobowych będzie bowiem kładło spory nacisk właśnie na certyfikaty. A najgorsze, co mogłoby się wydarzyć, to gdyby nie istniały one na polskim rynku i nasi przedsiębiorcy musieliby certyfikować się np. w Luksemburgu.

Dlatego teraz jest dobry moment na dyskusję o tym, jak taka certyfikacja ma wyglądać. Czy idziemy w stronę homologacji? Przy czym od razu mówię, że Biuro GIODO absolutnie nie jest przygotowane do tego, by takie homologacje wydawać. Czy raczej pozostawiamy to izmom gospodarczym lub tworzymy sieć audytorów? Na razie nie znam odpowiedzi na te pytania, ale musimy je znaleźć, gdyż przedsiębiorcy bez wątplenia będą zainteresowani uzyskiwaniem certyfikatów.

Jak zwiększyć świadomość użytkowników?

Wacław Iszkowski Będę się upierał, że ani obowiązki prawne, ani dobrowolna certyfikacja nic nie zmieniają. Dane są i będą zbierane, bo mają wartość marketingową. Firmy są skłonne za nie płacić, najlepiej za już odpowiednio sprofilowane zbiory danych, gdyż dzięki temu mogą dotrzeć ze swym produktem do klientów. Skuteczną ochronę przed zbieraniem informacji na temat użytkowników urządzeń mobilnych mógłby dać wyłącznie całkowity zakaz reklamy, gdyż wówczas nie byłoby już powodów do gromadzenia danych o nas.

Dokończenie na str. 6

Dokończenie ze str. 5

Jest to oczywiście postulat nierealny, gdyż coraz bardziej cały biznes uzależnia się od skuteczności reklamy. A więc to do reklamodawców i agencji reklamowych powinniśmy apelować, aby dbali o dobro danych osobowych konsumentów i wzięli odpowiedzialność za to, co z tymi danymi czynią. A jak tego nie będą robić, to powinni odpowiadać prawnie za skutki swoich zaniedbań. Zawsze najbardziej powinien odpowiadać ten, który na „przestępstwie” najwięcej zyskał.

A my powinniśmy realnie zadbać o interes użytkowników – uświadamiając ich, że sami muszą dbać o ochronę swoich danych poprzez rozsądne korzystanie z urządzeń i unikanie kontaktów z podejrzanymi aplikacjami. Odpowiedź na wszystkie pytania, które padły podczas tej debaty, jest prosta – edukacja i jeszcze raz edukacja.

Maciej Groń Co jednak da mi sama świadomość, że mój telefon może mnie szpiegować, skoro nie będę mógł nic z tym zrobić? Edukacja bez wątpienia jest ważna, niemniej jednak narzucenie pewnych obowiązków prawnych jest niezbędne. Za absolutne minimum uważam konieczność informowania użytkowników, że jakieś dane na jego temat będą przetwarzane, przez kogo i w jakim celu. Tylko wtedy możemy mówić o świadomym korzystaniu przez użytkowników z aplikacji mobilnych, kiedy będą oni mieli pełną wiedzę. Obecnie jedynym wyjściem użytkownika, który nie zgadza się na wykorzystanie jego danych w dowolny sposób, jest nieskorzystanie z danej aplikacji. A nie o to nam przecież chodzi, żeby zniechęcać ludzi do korzystania z rozwiązań, jakie oferują im obecnie nowe technologie, tylko aby nie naruszało to pewnych standardów.

Wacław Iszkowski A później mamy wkurzonych ludzi, którym ta informacja nie jest do niczego potrzebna, tylko utrudnia im życie. Tak jak z cookies. Ludzie wchodzący na stronę internetową Dziennika Gazety Prawnej są wściekli, że informacja o cookies zasłania im tekst. I nikt jej nie czyta, tylko patrzy, jak ją zamknąć.

Arwid Mednis Niemniej nie możemy przesuwąć granicy do tego stopnia, że ludzie nie będą mieli prawa wiedzieć, co dzieje się z ich danymi. To podstawowe prawo. Ja mogę się zgodzić, że dzięki temu otrzymam lepiej dopasowaną do siebie ofertę, ale muszę mieć świadomość tego, że jestem profilowany, i chciałbym mieć wybór, czy chcę otrzymywać oferty dopasowane do swojego gustu. Nie chcę być uszczęśliwiany na siłę. Chociaż przyznaję, że nie widzę dużej potrzeby wprowadzania dodatkowych obowiązków. Uważam, że te, które dzisiaj istnieją, czy to w prawie unijnym, czy też polskim, są wystarczające. Trzeba je co najwyżej dostosować do tych nowych urządzeń i aplikacji.

Wojciech Rafał Wiewiórowski Zgadzam się, że edukacja jest dzisiaj kluczowa. Trzeba dotrzeć z informacją na temat zagrożeń dla prywatności zarówno do młodzieży, jak i ludzi starszych, którzy również mogą nie mieć tej świadomości. Dodatkowo taka edukacja musi być dostosowana do ról społecznych różnych grup. Inaczej edukujemy cyfrowo nauczycieli, inaczej urzędników, a inaczej adwokatów czy lekarzy.

GIODO stara się to robić, przy czym zdajemy sobie sprawę, że pogadanki w szkole nie są dobrym pomysłem. Chodzi o pokazanie problemu od strony jak najbardziej praktycznej. Na lekcji języka angielskiego możemy omawiać gramatykę zarówno przy okazji czytanki o Big Benie, jak i materiału o tym, jakie informacje na nasz temat są gromadzone i przekazywane przez urządzenia mobilne oraz jakie to rodzi zagrożenia.

Debata odbyła się w redakcji Dziennika Gazety Prawnej w ramach obchodów VIII Europejskiego Dnia Ochrony Danych Osobowych