

Jak żyć z głową w chmurach danych

Rozmawia Paulina Szczucińska

*Wojciech Rafał Wiewiórowski, dr nauk prawnych, pełni funkcję
Generalnego Inspektora Ochrony Danych Osobowych (GIODO).*

Szerokim gestem rozdajemy informacje o sobie i swoich bliskich – w internecie, w sklepach, ankietach, hotelach. Które z tych danych podlegają ochronie?

Dane osobowe to wszystkie informacje, które pozwalają ustalić, o kogo konkretnie chodzi. W przypadku Jana Kowalskiego imię i nazwisko do tego nie wystarczą. Ale np. ja zawsze podpisuję się Wojciech Rafał Wiewiórowski – drugiego takiego zestawienia imion i nazwiska w Polsce nie ma, więc ta informacja wystarczy, żeby mnie zidentyfikować. Podobnie będzie wówczas, gdy przy nazwisku pojawi się numer PESEL. Takie dane podlegają ochronie.

Co to znaczy?

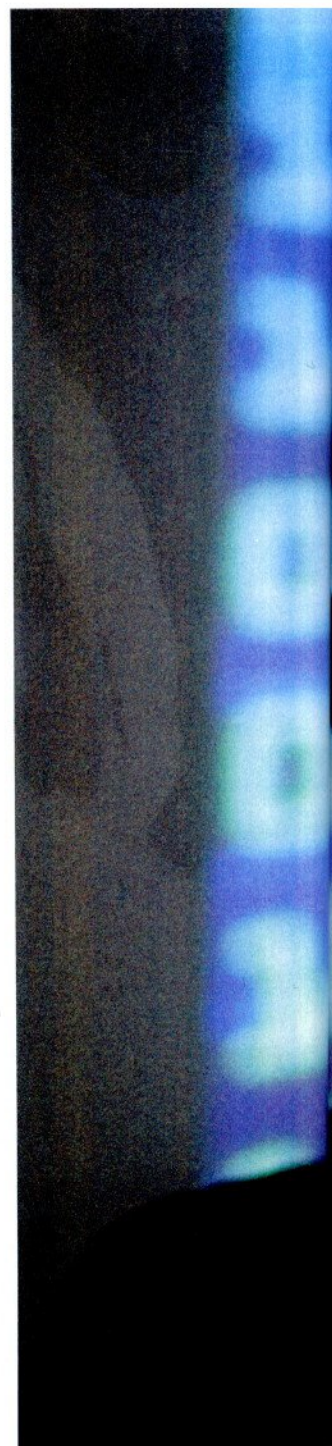
Podstawowe założenie prawa do prywatności mówi, że każdy winien sam decydować o tym, jakie informacje o nim są przekazywane na zewnątrz. Są sytuacje, gdy musimy zgodzić się na naruszenie tej prywatności, by np. umożliwić sprawne funkcjonowanie państwa, systemu ochrony zdrowia czy opieki socjalnej. We wszystkich pozostałych przypadkach dane o sobie udostępniamy dobrowolnie. Niestety, większość ludzi nie do końca wie, kiedy naprawdę musi przekazać informacje o sobie, a kiedy zgadza się na to z własnej woli.

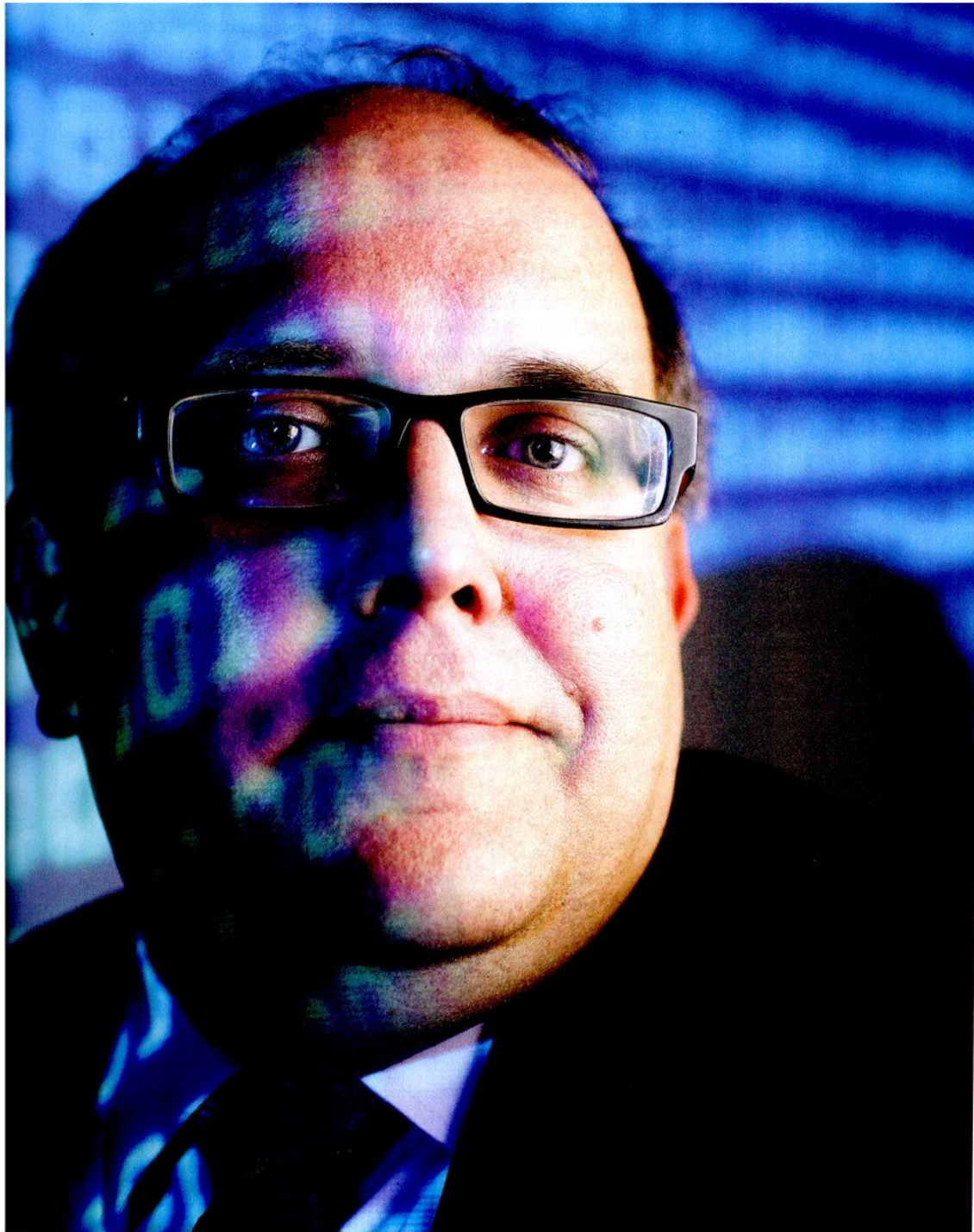
Często jesteśmy zmuszani do podania danych. Jeśli się na to nie godzimy, możemy tylko zrezygnować z usługi.

To nie jest sytuacja niezgodna z prawem. Musimy jednak zostać poinformowani, dlaczego dane są zbierane, a ich zakres nie może przekroczyć minimum potrzebnego do realizacji wskazanego celu.

Ujawnianie danych często wydaje się korzystne. Sklepy kuszą rabatami i punktami premiovymi na karcie klienta. Zapominamy o znanej regule, że nie ma obiadu za darmo.

Tak. Tymczasem informacje, które pozyskują o nas różne podmioty, mają przełożenie na realne pieniądze. Nie zawsze też zdajemy sobie sprawę, do czego dane mogą zostać użyte. Większość z nas myśli: ktoś byłby zainteresowany trzymaniem przez lata informacji o mnie? Jednak cena przechowania informacji spadła prawie do zera, więc zaczynają być gromadzone na zapas. Po co? Mam w tej chwili 41 lat. Zapewne za 35 lat będę potrzebował pomocy, której będzie mi udzielał mój inteligentny dom. Będzie wiedział o mnie wszystko. Jestem przekonany, że informacje potrzebne w 2047 r. do obsługi takiego inteligentnego domu są zbierane już dziś.





Nie jesteśmy
w stanie wyobrazić
sobie, do czego
za kilka lat zostaną
wykorzystane
informacje,
które dzisiaj
upubliczniamy.

To nie jest science fiction?

Nie jest. Gdyby dziś firmy sektora bankowego i ubezpieczeniowego mogły korzystać z danych, które zostawiałbym w sieci 20 lat temu, na pewno by to robiły. Bo tam znajdowałyby się informacje nie tylko o tym, co im deklaruje podczas podpisywania umowy ubezpieczenia czy kredytu, ale też o tym, co faktycznie się ze mną działo 20 lat temu. Nie jesteśmy w stanie wyobrazić sobie, do czego za kilka lat zostaną wykorzystane informacje, które dzisiaj upubliczniamy.

Kto, oprócz banków i ubezpieczycieli, zbiera informacje o nas?

Na pewno serwisy społecznościowe i wyszukiwarki. Za 30 lat one albo firmy, które z nich wyewoluują, będą posiadały ogromny zasób danych o zachowaniach i potrzebach wielu ludzi. Muszę też podkreślić, że trudno jednoznacznie powiedzieć, czy ta działalność jest legalna. Bo chociaż danych nie wolno zbierać na zapas, publikacja w internecie jest podobna do publikacji w gazecie. A z informacji w archiwach gazet możemy korzystać bez problemu.

Ochrona danych osobowych staje się utopią?

Niektórzy tak twierdzą. Mówią, że społeczeństwo, a zwłaszcza młodzież, nie jest zainteresowane ochroną swojej prywatności. Świadczyć ma o tym liczba śladów, które po sobie zostawiamy w internecie. Chociaż rzeczywiście jest ona ogromna, nie mogę zgodzić się z takim podejściem. W Europie przeprowadzono badania na temat stosunku do ochrony prywatności i okazało się, że 92 proc. dzieci w wieku 14–18 lat deklaruje, że stopień ochrony ich prywatności w serwisie społecznościowym jest ważnym aspektem przy podejmowaniu decyzji, czy się doń przyłączyć. Oczywiście nie twierdzę, że dzieci te potrafią chronić swoją prywatność i że faktycznie to robią. Ale czują, że jest ona ważną wartością.

Które z danych chcemy chronić najbardziej?

Lista jest długa i różni się w zależności od kraju. Oczywiście w całej Europie panuje przekonanie, że trzeba chronić dane medyczne czy dotyczące sytuacji finansowej. Z badań Eurostatu wynika np., że 70 proc. Polaków uważa, że adres zamieszkania jest daną wrażliwą (choć według prawa nią nie jest). A w Wielkiej Brytanii potrzebę chronienia tej informacji ma zaledwie 20 proc. obywateli. Z kolei według prawa daną wrażliwą są informacje o poglądach religijnych, podczas gdy wiele osób w Polsce chętnie je eksponuje, nosząc na szyi krzyżyk, koloratkę albo zakrywając głowę szalem.

To jest przejaw wolności jednostki. Lecz sytuacja może się skomplikować, gdy na ulicy przestaniemy być anonimowi. Polacy właśnie opracowali bardzo skuteczną metodę rozpoznawania ludzi za pomocą skanowania tęczówki. Taka technika zastosowana w monitoringu prowadziłaby do ograniczenia wolności obywateli. Są przewidziane jakieś regulacje prawne?

W *Raporcie mniejszości* Stevena Spielberga metodą uwolnienia się od kontroli była wymiana oczu na inne.

Czyli tylko to nam zostanie?

Żartuję. Skanowanie tęczówki oka niewątpliwie jest zbieraniem danych osobowych. W związku z tym może odbywać się tylko w szczególnych, uzasadnionych przypadkach. Przede wszystkim jednak jestem zaniepokojony brakiem w Polsce przepisów dotyczących wideomonitoringu. To duży błąd. Rzecznik Praw Obywatelskich i GODO występowali do MSWiA z wnioskiem o uregulowanie prawne tej kwestii, proponując rozwiązania. Jest to istotne, bo kiedy widzę na ulicy kamerę, nie wiem, czy należy ona do straży miejskiej, sklepu spożywczego czy wspólnoty mieszkaniowej. Brak tych regulacji jest na tle Europy wyjątkowy. Nie muszę chyba dodawać, że nie daje nam powodu do dumy.

Czy wiele jest różnic w ochronie danych osobowych w krajach UE?

Przepisy w ramach Europy są raczej zharmonizowane. Teraz w UE obowiązują dyrektywa z 1995 r., która dotyczy ochrony danych osobowych, oraz decyzja ramowa o ochronie danych osobowych w sektorach policji i wymiaru sprawiedliwości. Jednak dyrektywa ma już 17 lat. W świecie informacji jest po prostu prababcią. Gdy

Model przetwarzania danych w chmurach staje się coraz popularniejszy. A z niego zapewne w przyszłości wykluje się coś nowego, jeszcze nawet nie wiemy co. Stanowiący prawo muszą nadążać za tym postępem i cywilizować go.

była pisana, istniał co prawda internet, ale całkiem inny niż teraz. Wtedy telenetowaliśmy z serwera na serwer, mówiliśmy o serwisach gopherowych (przodkach dzisiejszego WWW). A teraz nikt nie wie nawet, co to znaczy. Postęp technologiczny jest właśnie jednym z powodów, dla którego Komisja Europejska przygotowała projekt nowych ram ochrony danych osobowych. Ma ogłosić go 25 stycznia.

A w reszcie świata jak to wygląda?

Wiele krajów, które są z UE powiązane interesami gospodarczymi lub chcą do niej przystąpić, wprowadza przepisy podobne do unijnych. Dlatego ochrona danych w prawie chorwackim, macedońskim, albańskim czy ukraińskim jest zbliżona do naszej. Jest też kilkanaście krajów, m.in. Kanada, Urugwaj, Argentyna, które przyjęły podobnego rodzaju rozwiązania, bo uznały je za słuszne. Ustawy o ochronie danych osobowych istnieją w 77 krajach.

Są też kraje, które takich przepisów nie wprowadziły.

Tak. Na przykład Stany Zjednoczone. Nie da się też porównać do europejskich standardów krajów takich jak Rosja czy Australia, do których często wybieramy się na wakacje bądź w sprawach biznesowych. Co ciekawe, one nie uważają wręcz za słuszne, by do tego systemu ochrony danych osobowych przystąpić.

Jak zatem chronione są dane, które zamieszczamy na Facebooku, który ma siedzibę w Stanach Zjednoczonych?

Prawem właściwym dla umowy, którą zawieramy, korzystając z Facebooka, jest prawo stanu Kalifornia. Jednak niedawno na terenie UE, w Irlandii, władze tego portalu założyły europejskie przedstawicielstwo oraz powołały regionalnych koordynatorów ds. prywatności, którzy działają według unijnych standardów. Właściciele portalu zdecydowali się na ten ruch, gdyż zdają sobie sprawę z groźby bycia współpozwanym w przypadku naruszeń dóbr osobistych. Jest to też sposób na utrzymanie użytkowników, bo gdyby okazało się, że z ochroną prywatności lepiej radzi sobie konkurencja, użytkownicy mogliby do niej odejść. Przecież 10 lat temu nie istniały ani Facebook, ani Google. Potęgami na rynku były serwisy Yahoo czy AOL, które dzisiaj są w drugiej, trzeciej lidze. Trzeba dbać o klienta, bo wirtualny świat błyskawicznie się zmienia.

Co dzieje się z plikami, np. zdjęciami, które wrzucam gdzieś na serwer, żeby je np. przechować? Skąd wiemy, gdzie ten serwer się znajduje i według jakich norm prawnych moje dane będą chronione?

Czytajmy informacje zawarte w polityce prywatności i regulamin, który akceptujemy przed wrzuceniem danych na serwer. Każdy podmiot świadczący usługi drogą elektroniczną powinien w nich podać, kto jest właścicielem serwisu, gdzie ma on siedzibę i jak przetwarza dane osobowe. Ale jeśli używamy poczty elektronicznej, której dostawca składa dane w chmurach (w modelu *cloud computing*), nie mamy żadnej pewności, gdzie te dane są przetwarzane: w Polsce czy np. w Laosie lub na Seszelach.

Przed publikacją w internecie zdjęcia naszego skoku ze spadochronem warto się zastanowić, czy aby we wniosku o polisę ubezpieczeniową nie wpisaliśmy, że nie uprawiamy sportów ekstremalnych.

Czy zatem cloud computing jest bezpieczny?

Systemy zabezpieczające przed włamaniem są w takim modelu zwykle bardzo dobrze skonstruowane. Nie wiemy natomiast, kto ma legalny dostęp do danych i jak się nimi zarządza. I tu mamy problem. Nie należy zakładać, że dane umieszczone na serwerze w USA lub Rosji nie będą właściwie chronione czy staną się przedmiotem handlu. Ale nie można też mieć pewności, że jego właściciele zastosują środki ochrony danych osobowych zgodne z wymaganymi w Europie oraz że będą chronić je przed dostępem służb specjalnych krajów, w których rezydują.

Co mogą zrobić? Podejrzec, wykorzystać?

Wszystko zależy od umowy, jaką zawarliśmy.

Załóżmy, że kliknęłam i zgodziłam się na wszystko.

W takim razie zapewne będą one wykorzystywane zgodnie z prawem w każdy sposób, jaki tylko wymyśli właściciel serwisu.

Gdybym wrzuciła do takiej chmury swoją księgowość?

To popełniłaby pani przestępstwo. Bo tam znajdują się dane pani klientów i współpracowników. Niedokonanie zastrzeżenia, że danych tych nie można łączyć, transferować itd. oznacza, że udostępniła pani czyjeś dane osobom do tego nieuprawnionym. A to jest przestępstwem w rozumieniu ustawy o ochronie danych osobowych. I chociaż dane te mogłyby być przetwarzane w chmurze np. w Kanadzie, to pani byłaby ścigana tutaj, w Polsce.

A jak ustalić, gdzie te dane się znajdują?

Jeśli są przetwarzane w chmurze, to możemy tylko stwierdzić, że znajdują się na jednym z serwerów, z których korzysta obsługująca nas firma. Dobrze jeśli z umowy wynika, jakie to mogą być miejsca.

Więc tak naprawdę nie wiadomo, gdzie są.

Tak, chociaż coraz więcej przedsiębiorców oferujących usługi cloud computingu zapewnia swoich klientów, że dane będą przetwarzane wyłącznie w centrach zlokalizowanych na terenie UE lub Europejskiego Obszaru Gospodarczego. Mówią: jesteście w swoim reżimie ochronnym i każde miejsce, w którym dane będą przetwarzane, podlega zasadom określonym w dyrektywie europejskiej. Ale nawet gdy to zostanie zapewnione, pojawia się jeszcze problem danych będących tajemnicami prawnie chronionymi. Przekazywanie ich do jakiegokolwiek innego kraju może być przestępstwem. W Polsce prawnie chronione są np. sekrety państwa, tajemnica lekarska, adwokacka czy spowiedzi świętej (choćby powiedziałbym, że akurat ona jest przetwarzana w całkiem innych chmurach). Organy ochrony danych osobowych proponują, by problem ten rozwiązywać, przyjmując tzw. wiążące reguły korporacyjne. Korporacja, która dostarcza chmurę, przyjmowałaby określony zestaw reguł, tworząc coś w rodzaju kraju zapewniającego ochronę naszych danych.

Czyli tworzyłaby virtualne państwo?

Tak, to trafne określenie. Oczywiście trzeba jeszcze ustalić, kto w takim wirtualnym państwie będzie organem ochrony danych osobowych i jak będzie sprawował kontrolę.

W jaki sposób mogą mi zaszkodzić dane, które udostępniłam?

Mogą być wykorzystane w innym celu, niż by sobie pani tego życzyła. Duży problem to tzw. profilowanie, czyli zbieranie danych z różnych źródeł i zestawianie ich w profile osobowe.

Kto takie profilowanie wykonuje?

Coraz więcej podmiotów, m.in. banki, firmy ubezpieczeniowe. Zbierają informacje o kliencie ze źródeł ogólnie dostępnych, np. z internetu, i uzupełniają je danymi z innych legalnych źródeł. Lecz stosuje się też inny sposób profilowania. Polega on na uzupełnianiu prawdziwych danych takimi, które są dla danej osoby statystycznie poprawne. Najbrutalniejszą odmianą takiego profilowania jest takie wnioskowanie: kilku klientów, którzy charakteryzowali się cechą A, przedwcześnie umarło. Stąd wniosek statystyczny – każdy klient odznaczający się cechą A zapewne szybko umrze. Wnioskowanie to jest zaledwie prawdopodobne, niemniej chętnie stosuje się je w wielu bankach czy firmach ubezpieczeniowych, by oszacować swoje ryzyko podczas zawierania umowy i dopasować ofertę do klienta.

Czy to jest legalne?

Jeśli się zgodziliśmy na przekazywanie informacji o nas w ramach grupy kapitałowej, to musimy zdawać sobie sprawę, że bank będzie przekazywał informację ubezpieczycielowi – i odwrotnie. Legalne jest też zbieranie danych ze źródeł, do których jest legalny dostęp. Przykład? Publikując zdjęcie skoku ze spadochronem, warto zastanowić się, czy we wniosku o polisę ubezpieczeniową nie wpisaliśmy, że nie uprawiamy sportów ekstremalnych. Zdjęcie z papierosem może zaś być sprzeczne z deklaracją, że nie palimy tytoniu. Gdy kiedyś (z zupełnie innej przyczyny) zajdzie potrzeba wypłacenia odszkodowania, firma ubezpieczeniowa wyciągnie zdjęcie i powie: „Jak to? Przecież złamała pani oświadczenie, które zostało nam kiedyś złożone”.

To się dzieje naprawdę?

Tak. Co więcej, z założenia tego typu działania nie są nielegalne. GIODO zwraca jednak uwagę, że każdy, kto dokonuje profilowania, ma obowiązek poinformowania o tym osoby profilowanej. I to – mam wrażenie – nie jest jeszcze w Polsce wykonywane. Tymczasem obowiązek ten podkreśla rekomendacja Rady Europy z listopada 2010 r.

Jak się przed tym chronić?

Każdy może wystąpić do podmiotu przetwarzającego jego dane, by zostały mu ujawnione. Te nieprawidłowe, nieaktualne, błędnie przypisane ma prawo zmienić albo choć zaznaczyć,

że ich nie potwierdza. Niedawno grupa osób z Austrii wystąpiła z takim pytaniem do irlandzkiego przedstawiciela Facebooka. Otrzymali płyty CD z kilkunastoma tysiącami stron danych o sobie.

Kto Polakom pomaga w wycofywaniu różnych danych?

To jedno z zadań realizowanych przez GIODO, który zgodnie ze swoimi ustawowymi kompetencjami może wydać np. decyzję nakazującą usunięcie danych. Czasem administrator danych się z nią nie zgadza. Wtedy sprawa trafia do sądu. Teraz mamy kilka spraw dotyczących przetwarzania danych w Krajowym Systemie Informacyjnym Policji. Zdaniem osoby zainteresowanej i GIODO dane powinny być usunięte z systemu, bo nie ma już powodu, dla którego policja miałaby je przechowywać, jednak ta odmawia ich wycofania. Ostatnio wygraliśmy dwie takie sprawy.

Czy w nowym prawie UE będziemy mieli prawo do zapomnienia?

Idea ta jest bardzo ciekawa i ważna. Rzeczywiście teraz w UE pracuje się nad jej uregulowaniem. Dzięki jej wdrożeniu zyskalibyśmy prawo do tego, aby informacja o nas nie pojawiała się w internecie i w ogóle nie była przetwarzana w dużych systemach informacyjnych. Mielibyśmy też możliwość wycofania z sieci informacji na nasz temat. Muszę jednak przyznać, że jest to trudne do realizacji, a nawet do ujęcia w przepisach.

Można jakoś samodzielnie ochronić informacje na swój temat przed niepożądanym wykorzystaniem?

Niektórzy stosują ciekawe, ale wątpliwe prawnie rozwiązanie: dołączają miniwirusy do swojego CV wysyłanego e-mailem. Te miniprogramiki po pewnym czasie mają niszczyć całą informację zapisaną w CV. Można nawet te wirusy pobrać z internetu, ale wiąże się to z pewnym niebezpieczeństwem: nie mamy pewności, czy wirus ten nie jest np. programem szpiegującym, który zamiast dane zniszczyć, wyśle je gdzieś bez naszej kontroli.

To może GIODO powinien taką aplikację napisać i udostępnić?

Może warto się nad tym zastanowić. Jednak nie mamy podstawy prawnej, żeby to robić. Nie wolno tworzyć programów niszczących dane. Kodeks karny w art. 269 b zakazuje tworzenia takich narzędzi.

To co mogę zrobić?

Powiem tak: najbezpieczniej byłoby nie umieć czytać i pisać, nie używać komputera ani telefonu i nie poruszać się w miejscach poddanych nadzorowi kamer.

Ewentualnie chodzić po ulicy w masce.

Proszę jednak pamiętać, że gdyby w tej masce weszła pani na stadion, to według nowych przepisów ustawy o bezpieczeństwie imprez masowych byłoby to już przestępstwo. Trudno się całkowicie odciąć od naszego informacyjnego świata. Najważniejsze, by mieć świadomość wagi ochrony danych osobowych. A tych, którzy proszą o ich podanie, zawsze, do znudzenia pytać: „Ale po co?”. □