Jakub Styczyński,
dziennikarz Dziennika Gazety Prawnej
zajmujący się nowymi technologiami
oraz ochroną danych osobowych

- Czy systematycznie publikując materiały obejmujące problematykę ochrony prywatności dostrzega Pan potencjalnie groźne zjawiska dla jej poszanowania?

Nie da się ukryć, że pandemia koronawirusa dobitnie pokazała, że w kryzysowych sytuacjach, kwestie ochrony danych osobowych są przez wielu spychane na dalszy plan. A spełnianie obowiązków wynikających z rozporządzenia RODO znów zaczęło poważnie doskwierać przedsiębiorcom. Najlepiej widać to na przykładzie Węgier, które na czas pandemii postanowiły zawiesić pewne obowiązki nałożone przez unijne rozporządzenie. W Polsce również pojawiały się takie pomysły. I choć formalnie nikt RODO u nas nie zawiesił, to i tak zauważyłem pewne rozprężenie wśród przedsiębiorców w zakresie spełniania norm wynikających z przepisów.

- Jak sytuacja przedstawia się Pana zdaniem podczas epidemii? Z czym Administratorzy mają obecnie problemy?

Z początku spore problemy sprawiła administatorom organizacja pracy zdalnej i wiążąca się z tym konieczność wdrożenia odpowiednich zabezpieczeń. W ostatnich tygodniach, w związku z odmrażaniem gospodarki przez rząd i otwieraniem na nowo lokali usługowych oraz zakładów pracy, pojawia się jednak inny kłopot. Wśród administratorów zaczęły bowiem krążyć informacje o tym, że w ramach przeciwdziałania rozprzestrzenianiu się koronawirusa, należy swoim pracownikom oraz gościom zakładu pracy, mierzyć temperaturę, a także wdrożyć ankiety o stanie zdrowia. Sugerował to nawet resort rozwoju w swoich wytycznych, niekonsultowanych z Urzędem Ochrony Danych Osobowych. Tymczasem takie działania mogą stanowić poważne naruszenie przepisów RODO w zakresie przetwarzania szczególnej kategorii danych osobowych. Gromadzenie informacji o stanie zdrowia przez wiele podmiotów, w tym przez galerie handlowe, zakłady pracy, salony fryzjerskie itd., może zaś prowadzić do poważnych w skutkach, wycieków danych.

- Czy można, dostrzegając próby wprowadzania nowych narzędzi [Internetu rzeczy], mieć wątpliwości co do ich zastosowania w odniesieniu do ochrony danych lub dóbr osobistych? W czym dostrzega Pan największe zagrożenia?

Będąc dużym fanem rozwoju technologii, jednocześnie bardzo sceptycznie podchodzę do tematu Internetu Rzeczy. Pomysł, aby do globalnej sieci podłączona była lodówka, pralka, suszarka, budzik, czy reszta elektroniki użytkowej, budzi moje obawy – głównie o ich bezpieczeństwo. Wiadomo bowiem, że producenci konsumenckich urządzeń typu RTV i AGD dążą do maksymalizacji zysku. A ten osiąga się między innymi obniżając jakość komponentów. Myślę, że największe oszczędności będą poczynione na zabezpieczeniach urządzeń z Internetem Rzeczy. Już dziś widzę, że tania elektronika użytkowa (np. popularne smartwatche czy opaski fitness) jest tania przede wszystkim dlatego, iż jej użytkownicy płacą za nie dodatkowo własnymi danymi osobowymi. I to nie byle jakimi – wszak smartwatche mogą zbierać dane o lokalizacji, tętnie, wadze czy jakości snu. To sprawia, że producenci, a także podmioty z nimi współpracujące, wiedzą o dużej grupie ludzi czasem więcej, niż wie o nich lekarz.

Oczywiście można gdybać, czy przy zbieraniu tak dużej ilości danych, chińskie czy amerykańskie koncerny technologiczne w ogóle interesują się tym, że typowy Kowalski codziennie wychodzi na spacer na Mokotowie. Entuzjaści technologii przekonują, że Kowalski jest dla nich jedynie bitem informacji, punktem w statystyce. I że nikogo nie obchodzi, że akurat ten człowiek spaceruje w tym konkretnym miejscu oraz czasie. Jednocześnie trzeba jednak pamiętać, że posiadając tak szczegółowe dane, zawsze można po nie sięgnąć. I potencjalnie wykorzystać w nieetycznym celu. Ważna jest świadomość. Warto zatem urządzeń używać, ale nie nadużywać.

- Jakie nowe kierunki lub regulacje prawne/etyczne powinny być rozwijane w związku z prywatnością w cyfrowym świecie?

Myślę, że Unia Europejska wyznacza trendy w tym zakresie. Amerykanie pozazdrościli nam RODO, kiedy na jaw wyszła afera Cambridge Analityca. W niektórych stanach zaczęto wręcz myśleć nad przyjęciem rozwiązań prawnych na modłę RODO. Debata nad legislacją dotyczącą sztucznej inteligencji trwa zaś na forum europejskim już od dłuższego czasu. Powstał nawet specjalny zespół zajmujący się etycznymi aspektami SI. Wśród głównych jego

postulatów jest „odczarowanie" systemów z SI. Tych „czarnych skrzynek", które firmy „karmią" danymi i uzyskują dzięki temu dokładne analizy np. zachować czy oczekiwań klientów. Chodzi o to, żeby regulatorzy czy organy nadzorcze miały możliwość wglądu w to, jakie algorytmy przyjęły firmy przetwarzające dane, a także jakiego rodzaju dane były przez system analizowane. Dzięki temu można by sprawdzić, czy napisane algorytmy nie dyskryminują żadnej grupy społecznej, podczas realizacji narzuconych im celów.

- Czy warto podejmować Pana zadaniem tematy o zagrożeniach Sztucznej Inteligencji i czego powinny dotyczyć?

Na pewno bezcelowa jest na razie dyskusja na temat etyki robotów – na humanoidalne postacie z cybernetycznym umysłem musimy jeszcze bowiem zaczekać. Póki co z wykorzystania SI płyną zupełnie innego rodzaju zagrożenia, niz potencjalna zagłada ludzkości dokonana przez maszyny.

Zamiast wyznaczać konkretne kierunki, powinniśmy dążyć do ustalenia granic etycznych, których nie należy za nic w świecie przekraczać. Chodzi tu np. o szalenie kontrowersyjne używanie powszechnego monitoringu wizyjnego wykorzystującego systemy SI. Zwolennicy tej technologii przekonują, że mogłaby ona pomóc zapewnić obywatelom większe bezpieczeństwo. W pewnym zakresie, na pewno mają rację. Natomiast takie rozwiązanie chyba nigdy nie przejdzie testu proporcjonalności z RODO. Bo zawsze powszechna inwigilacja w rękach państwa jako administratora danych osobowych, może doprowadzić do wdrażania systemów oceny społecznej i nadużyć, znanych z Chin. A tego, póki co, Europejczycy nie chcą.

W zakresie ochrony danych osobowych, wydaje mi się, że wciąż bardzo naiwni są internauci. Z jednej bowiem strony deklarują, że informacje o nich, powinny być odpowiednio zabezpieczone. A z drugiej strony ochoczo oddają swoje dane osobowe firmom oferującym w zamian niewielkie rabaty. Albo korzystają z chińskich serwisów społecznościowych wykorzystujących systemy SI na dużą skalę, łącznie z analityką cech biometrycznych twarzy. A wszechobecne w sieci „memy", czy „challenge" sprawiają, że manipulowanie emocjami ludzi przez firmy stojące socjotechnikę, stało się łatwiejsze, niż kiedykolwiek. W tym zakresie może nas uratować wyłącznie edukacja. Ale nie taka tradycyjna, opierająca się na wkuwaniu treści w stylu „Słowacki wielkim poetą był". Trzeba patrzeć na rozwiązania

wdrażane np. w Finlandii, gdzie dzieci uczy się krytycznego myślenia i obiektywnego podejścia do przyswajanych treści.

- Jakie grupy ekspertów powinniśmy angażować do działań wyprzedzających nowe zagrożenia?

Chyba takich, jak w każdej dyskusji – przeciwnych sobie. Bo tylko wtedy istnieje szansa, że wypracowane rozwiązanie będzie możliwie najbliższe nieuchwytnego „złotego środka". Czyli w tym przypadku powinniśmy mieć zwolenników technologii, którzy chcą zmieniać świat i informatyków, którzy zachłystują się ilością danych oraz możliwościami, jakie daje wykorzystanie SI. A po drugiej stronie etycy i socjologowie. Może to brzmi banalnie, ale przecież ostatecznie z rozwiązań technologii mają korzystać ludzie. A informatycy – zresztą nie tylko oni – nie są w stanie przewidzieć dziwnych zagrożeń, jakie może nam sprawić technologia. Ciekawy przykład podał mi w wywiadzie dla DGP Michał Kosiński z Uniwersytu Stanforda, specjalista w dziedzinie psychometrii, sztucznej inteligencji i big data, który bada ludzi na podstawie ich śladów cyfrowych. Wyjaśniał on, że przykładowo Facebook kontroluje to, co czytamy, podsuwając nam treści najbardziej angażujące i atrakcyjne. Przez to spędzamy na portalu coraz więcej czasu. Jeśli algorytm odnotuje, że pokazywanie użytkownikom wielkich, tłustych kotletów powoduje, iż w następnym dniu poświęcą więcej czasu Facebookowi, to uparcie będzie im wyświetlać hamburgery. Maszyna nie przewidzi, że ci ludzie danego dnia zjedzą hamburgera, zapiją go coca-colą i przez to następnego dnia będą spędzać więcej czasu przy komputerze, bo się będą czuć zbyt ociężali, by wyjść na siłownię. W sposób niezamierzony może to doprowadzić do wzrostu epidemii otyłości wśród internautów. Na tej samej zasadzie, jeśli użytkownicy czytują skrajnie prawicowe lub lewicowe artykuły zawierające teorie spiskowe, będą takimi treściami zalewani. Być może ktoś się przez to zradykalizuje, odda głos w wyborach niezgodnie z sumieniem albo zrobi coś jeszcze głupszego.

- Jak sytuację Sztucznej Inteligencji widzą specjaliści z innych państw UE?

Europejscy specjaliści są znani na świecie z tego, że zaciekle walczą o naszą prywatność. To między innymi dzięki nim europejskie firmy musiały zacząć być konkurencyjne w innym zakresie niż te zza Wielkiego Muru. Rozwiązania z UE może nie są najtańsze, ale zapewniają najwyższą jakość ochrony danych osobowych. Bo przecież wiele europejskich firm musi

przestrzegać nie tylko RODO, ale też dyrektywy PSD2, rozporządzenia AML IV, czy innych restrykcyjnych aktów prawnych.

Dostrzegam jednak, że na forum UE pojawiają się głosy mówiące o tym, aby starać się nieco luzować podejście do ochrony danych osobowych. Specjaliści wiedzą, że przez nie firmy z UE zostają daleko w tyle, jeżeli chodzi o wdrażanie nowoczesnych rozwiązań. Jednocześnie jednak mają dylemat, bo nie chcą pozwolić na tak głęboką ingerencję w życie obywateli, jak w USA, Indiach czy Chinach.

- Czy prasa Pana zdaniem podejmuje szczegółowe tematy w zakresie Sztucznej Inteligencji i Internetu rzeczy?

Myślę, że niewystarczająco często. W wielu przypadkach media są jedynie tubą marketingową dla informacji podsyłanych im przez działy PR. W praktyce rozwiązania, szumne nazwane Sztuczną Inteligencją, to mrzonki - zbiór prostych algorytmów, które robią niewiele więcej, niż oprogramowanie sprzed kilku dekad.

Z kolei Internet Rzeczy wciąż jest przedstawiany w mediach jako ciekawostka, pieśń przyszłości. Na łamach Dziennika Gazety Prawnej od kilku lat staramy się poruszać bardzo pogłębione materiały dotyczące nie tylko aspektów prawnych dotyczących SI oraz Internetu Rzeczy, ale również aspektów etycznych. Myślę, że brakuje w mediach poważnej prasy na ten temat. Nawet jeśli ktoś zaczyna pisać na temat przyszłości SI, to wciąż analizuje ją przez pryzmat kiczowatych filmów science-fiction sprzed dziesiątek lat.

- Jak ocenia Pan wzrost świadomości społeczeństwa w zakresie ochrony prywatności?

„Nie wolno, bo RODO" – to zdanie chyba już na stałe zagościło w głowach dużej części Polaków. Wypowiedź dość zabawna, zwłaszcza, że wielu ludzi w zasadzie nie ma pojęcia, o czym mówi. Nie zmienia to faktu, że świadomość obywateli w zakresie praw wynikających z RODO jest i tak większa, niż w zakresie jakiegokolwiek innego aktu prawnego. Widać to na przykładzie rosnącej liczby skarg wpływających do prezesa UODO. Wciąż mam jednak wrażenie, że Polacy bardzo krytycznie podchodzą do kwestii przetwarzania danych osobowych przez administrację publiczną, jednocześnie pozwalając na dużo więcej podmiotom prywatnym.

- Co myśli Pan o rozwiązaniu zaproponowanym przez Ministerstwo Cyfryzacji – ProteGO Safe?

Podzielam zdanie specjalistów, że to narzędzie ma niewielkie szane, aby spełnić założone przez siebie cele. Wystarczy spojrzeć na przykład Singapuru, którego to aplikacja TraceTogether była inspiracją dla stworzenia ProteGO Safe. Z tego narzędzia korzysta zaledwie 5 proc. wszystkich obywateli. W Indiach, jej odpowiedniczkę – Aarogya Setu – pobrało 50 mln osób z 500 mln użytkowników smartfonów. I populacji 1,3 mld. Tymczasem najnowsze brytyjskie i amerykańskie badania wskazują, że aby tego typu aplikacje były skuteczne, to powinno z nich korzystać co najmniej 70 proc. populacji. Potencjalną efektywność ProteGO Safe oceniam zatem jako nikłą.

Jednocześnie absolutnie nie apeluję o to, aby narzędzie było dla obywateli obowiązkowe. Niebezpieczeństwo związane z potencjalnymi wyciekami danych czy możliwością inwigilacji obywateli oceniam bowiem jako bardzo wysokie. Wątpliwości ekspertów budzi również fakt, że dane z ProteGO Safe są umieszczane w chmurze obliczeniowej usługodawcy z USA, gdzie służby specjalne mają możliwość wglądu w dane przetwarzane przez tamtejsze firmy. A także chęć rządu, aby w monitorowaniu obywateli pomogli amerykańscy giganci technologiczni jak Apple oraz Google. Idealnym rozwiązaniem byłoby, gdyby tego typu narzędzie było administrowane przez niezależną instytucję i opierało się na wymianie danych w rejestrze rozproszonym (blockchain).

Poza tym myślę, że pandemia koronawirusa nie wymaga podejmowania dużej ingerencji w analizę przemieszczania się obywateli. Chyba, póki co, powinniśmy pozostać przy sprawdzonej i bezpiecznej technologii – myciu rąk mydłem i noszeniu maseczek.

- Czy w ostatnim czasie słyszał Pan informacje o wyciekach danych? Jeśli tak, to czy informacje te uznał Pan za wystarczające w kontekście wyjaśnień co do podjętych działań związanych z odpowiedzialnością i ewentualnymi sankcjami?

W ostatnim czasie nie było zbyt wielu doniesień o wyciekach danych z firm. Czy faktycznie ich nie było? Cóż, żyjemy w świecie, w którym gigantyczne wycieki danych z Google'a, Amazona, Ubera, Facebooka czy chmury Microsoftu, nie miały żadnych negatywnych konsekwencji dla tych koncernów. I w kraju, gdzie dane o wyborcach pozyskuje się w formie niezabezpieczonego, zbiorczego pliku tekstowego. Praktyka pokazuje, że organy nadzorcze

mające stać na straży ochrony danych osobowych, nie mają żadnych jurysdykcji ani odwagi do podejmowania działań względem gigantów technologicznych. A w stosunku do organów państwowych wystarczy lipna podstawa prawna w ustawie pisanej na kolanie, aby wyciszyć ewentualne zastrzeżenia prezesa UODO.

- Jak długo Pana zdaniem specjaliści z zakresu ochrony danych będą jeszcze budować świadomość Administratorów w zakresie odpowiedzialności, która na nich spoczywa w związku z wyznaczaniem kompetentnych fachowców?

To chyba jedna z tych „syzyfowych prac". Tak jak w polskich filmach obcina się budżety na rejestrację dźwięku, bo przecież ludzie przychodzą dla gwiazd, tak samo w firmach ważniejsza jest marka, bieżące wynagrodzenia i maksymalizacja zysków. Póki organ nadzorczy nie ma problemu z tym, żeby Inspektorzy Ochrony Danych w firmach pozostawali w większości przypadków zależni od swoich pracodawców, a na rynku można znaleźć usługi IOD, którzy pełnią tę funkcję w kilkudziesieciu podmiotach na raz, póty sytuacja nie będzie normalna. Przedstawiciele firm wciąż myślą o RODO jak o kolejnym, nikomu niepotrzebnym, obowiązku. I póki nie przydarzy im się jakiś włam hakerski, albo dotkliwa kara od organu nadzorczego, to nie będą inwestować w zwiększanie zabezpieczeń. Wciąż łudzę się, że certyfikaty zgodności z RODO mogłyby sprawić, że firmy zaczną ze sobą konkurować jakością ochrony danych osobowych. Niestety certyfikacja w Polsce nadal nie istnieje, tak samo jak kodeksy branżowe.

- Jak Pana zdaniem i czy możemy w jakiś sposób dochodzić swoich praw w kontekście udostępniania naszych danych (np. z rejestru PESEL) podmiotom do tego nieupoważnionym?

Takie możliwości oczywiście istnieją. Teoretycznie naszym sprzymierzeńcem powinien być Urząd Ochrony Danych Osobowych. Jego podejście w zakresie ochrony danych z rejestru PESEL czy spisu wyborców, wciąż jednak pozostawiają wiele do życzenia. Wygląda więc na to, że powinniśmy dochodzić swoich praw, jeżeli nie w sądach krajowych, to w unijnych trybunałach.

Dziękujemy za rozmowę Zarząd SIODO

Rozmowę przeprowadzili D. Czerw i P. Kitela