RODO ma nadal pierwszoplanową rolę – mówi prof. Arwid Mednis

Posted on 2026-05-31

Ubolewam nad tym, że nadal dominuje podejście, iż celem RODO jest ochrona danych dla samej ochrony. Tymczasem ja zawsze przypominam, że tak naprawdę głównym celem RODO jest ochrona różnych praw i wolności, które mogą zostać naruszone w związku z przetwarzaniem naszych danych – mówi dr hab. Arwid Mednis, radca prawny, członek Społecznego Zespołu Ekspertów przy Prezesie UODO, kierownik Zakładu Administracji Publicznej i Transformacji Cyfrowej na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego, partner w KLM LAW.

W maju tego roku przypada rocznica przyjęcia RODO (10 lat) i rozpoczęcia jego realnego stosowania (8 lat). Jako praktyk czy może Pan powiedzieć, że przepisy te już faktycznie przyjęły się w firmach, czy też musimy poczekać na jakieś kolejne „kamienie milowe”?

Arwid Mednis: Dzisiaj mało kto pamięta, że przed RODO mieliśmy ustawę o ochronie danych osobowych, której dużą część rozwiązań RODO powieliło. Oczywiście było też sporo zmian, ale w gruncie rzeczy większość praw osób, których dane dotyczą, była już w poprzedniej ustawie. Podobnie jak przepisy dotyczące bezpieczeństwa danych czy podejmowania

zautomatyzowanych decyzji itd. Z jakiegoś powodu tamte przepisy przyjęły się średnio, delikatnie mówiąc. Ustawa obowiązywała od 1998 do 2018 r. i pomimo tak długiego okresu obowiązywania ochroną danych osobowych nie przejmowano się w takim stopniu jak za czasów RODO.

Dopiero RODO przyczyniło się do tego, że większa liczba przedsiębiorców zaczęła się tą ochroną danych przejmować. Jest takie podejrzenie, z którym się w znacznym stopniu zgadzam, że to wysokie kary spowodowały wzrost świadomości u przedsiębiorców. Chociaż pamiętajmy, że sankcje w starej ustawie też były, ale „jedynie" w zakresie prawa karnego. Były przewidziane kary pozbawienia wolności, ale realnie nikogo nie ukarano niczym poważniejszym niż grzywna, większość spraw umorzono, zatem nie ma się co dziwić, że ustawę z 1997 r. nazwano „bezzębnym tygrysem". Wydaje się więc, że świadomość tych przepisów jest dziś duża. Większość ludzi już wie, że jest coś takiego jak RODO, ale zdarzają się jeszcze firmy, które RODO traktują czysto formalnie, na zasadzie „kupujemy dokumentację, bo wiemy, że musi być polityka ochrony danych, test równowagi itp. – i udajemy, że mamy to wdrożone". Natomiast zdecydowana większość ma świadomość, że trzeba te zasady porządnie wdrożyć i że musi to być stale kontrolowane, bo ochrona danych jest procesem ciągłym.

Czy wiąże się to też ze zrozumiem roli. jaką odgrywają dane osobowe we współczesnym świecie?

Ubolewam nad tym, że nadal dominuje podejście, iż głównym celem RODO jest ochrona danych dla samej ochrony. Tymczasem ja zawsze przypominam – również na wykładach dla studentów i przy okazji różnych wystąpień – że tak naprawdę głównym celem RODO jest ochrona różnych praw i wolności, które mogą zostać naruszone w związku z przetwarzaniem danych osobowych. To nawet wynika z pełnego tytułu RODO, bo jest to rozporządzenie o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych itd. Oczywiście prawo do ochrony danych osobowych czy prawo do prywatności są również prawami

podstawowymi, ale RODO ma też chronić np. przed dyskryminacją, czyli zapewniać równe traktowanie, a także chronić autonomię woli jednostki itp.

A więc gdy egzekwujemy RODO, to naszą rolą nie jest wyłącznie zapewnienie, że nie będzie wycieków danych, bo tak naprawdę z samego sposobu przetwarzania danych również mogą wynikać zagrożenia, np. wadliwa metoda profilowania może się przyczynić do nierównego traktowania ludzi. Trzeba więc nadal szerzyć świadomość, że RODO chroni różne prawa i wolności, które mogą zostać naruszone w związku z przetwarzaniem danych osobowych.

Jakie są największe problemy w stosowaniu przepisów RODO w polskich firmach?

Ja może nie mam pełnego przeglądu, bo pracuję dla dużych firm, i to głównie z sektora finansowego. Jednak wydaje mi się, że problemem, który ostatnio wielu przedsiębiorców zgłasza, jest kwestia funkcjonowania inspektora ochrony danych. Nadal pojawiają się pytania, jak „ustawić" status IOD i jego pozycję w organizacji, bo to się zmieniało także w praktyce organu nadzorczego. Były już liczne postępowania w tej sprawie, a nawet kary z tego tytułu. Nadal istnieje jednak niezrozumienie, kim inspektor ma być, że nie powinien co do zasady wykonywać funkcji administratora, że jego rolą jest kontrola poprawności przetwarzania danych w instytucji.

Zawsze powtarzam, że za ochronę danych w instytucji czy organizacji odpowiadają wszyscy pracownicy, choć oczywiście ważna jest zarządcza rola centralnego kierownictwa. W dużych organizacjach tworzy się odrębne komórki lub stanowiska odpowiedzialne za realizację obowiązków z RODO, niezależne od IOD. Inspektor jest od tego, żeby patrzeć, czy jest to dobrze robione, monitorować, zwracać uwagę, kontrolować, edukować itd. I to wydaje się nadal problemem w wielu firmach.

Problemem na pewno jest też kwestia łączenia funkcji IOD z innymi zadaniami. Rodzi to problem konfliktu interesów. RODO mówi też, że IOD ma podlegać bezpośrednio kierownictwu danej instytucji, ale czy jeśli wykonuje on też inne zadania ,to może w tym

zakresie podlegać komuś innemu. Jest też problem podległości funkcjonalnej w zakresie prawa pracy.

Kolejną rzeczą, o której warto wspomnieć, bo także dość często się pojawia, jest transfer danych za granicę UE – do państw trzecich. Gdy dokonujemy takiego transferu, musimy w większości przypadków przeprowadzić ocenę jego wpływu na ochronę danych (transfer impact assessment). I to jest nadal rzecz, która wzbudza sporo wątpliwości. Nie każdy wie, jak powinna funkcjonować taka ocena ryzyka, mimo że mamy sporo instytucji, które wydały wytyczne w tej sprawie, jak choćby EROD czy francuski CNIL. Wiele firm ma również problemy z takimi zagadnieniami jak zgłaszanie naruszeń, podstawy marketingu bezpośredniego, a więc jak stosować przepisy RODO i Prawa komunikacji elektronicznej. Wątpliwości budzi również kwestia możliwości przechowywania danych o kliencie po zakończeniu umowy, tj. czy można je przechowywać dla celów obrony przed roszczeniami, bo, jak wiadomo, NSA w ostatnich wyrokach stwierdził, że nie ma do tego podstaw. Te orzeczenia dotyczyły głównie banków, ale problem mogą mieć wszyscy przedsiębiorcy, którzy zawierają umowy z konsumentami.

Powiedział Pan o rosnącej świadomości przepisów RODO, ale czy wciąż panuje swego rodzaju strach przed tymi przepisami, myślenie na zasadzie, że „nie da się, bo RODO?" Chociaż wiadomo, że wiele rzeczy da się zrobić w ramach tej regulacji, tylko trzeba je odpowiednio przeprowadzić…

Wciąż spotykamy się z odpowiedziami „nie da się, bo RODO". Jest to często przejaw zwykłego oportunizmu, by odmówić podania danych osobowych, podczas gdy faktyczną podstawą odmowy jest niechęć do działania. Odmawia się np. dostępu do informacji publicznej „bo RODO" nawet jeśli ktoś domaga się informacji o osobie pełniącej funkcję publiczną. To jest nieporozumienie, podobnie jak swoista nadinterpretacja RODO. Pamiętamy nadawanie pseudonimów pacjentom, szafki zgodne z RODO i szereg innych absurdów, które z rozporządzeniem nie miały nic wspólnego. Faktem jest, że w RODO jest

sporo rozwiązań o charakterze ocennym. Np. zastosowanie jako podstawy prawnej przetwarzania przesłanki prawnie uzasadnionego interesu z art. 6 ust. 1 f. RODO wymaga identyfikacji tego interesu, oceny niezbędności oraz testu równowagi. To wydaje się skomplikowane, więc ludzie utwierdzają się w przekonaniu, że RODO to „czarna magia" i trzeba zwrócić się do specjalisty, który nie zawsze jest specjalistą… Znajoma lekarka jeszcze całkiem niedawno kupiła do gabinetu „szafki zgodne z RODO".

Co jest większym motywatorem do przestrzegania RODO – strach przed karami czy jednak przed stratami wizerunkowymi w przypadku wycieku danych? Czy te straty wizerunkowe to rzeczywiście jest coś, co dzisiaj może poważnie dotknąć firmę, i czy klienci, społeczeństwo, obywatele rzeczywiście zwracają na to uwagę?

Wydaje mi się, że to jest bardzo ważny aspekt. Kary to jedno, ale obawa przed stratą wizerunkową – i to nie taką ogólnikowo traktowaną, tylko taką, która sprawi, że np. duży bank, zakład ubezpieczeniowy, portal społecznościowy, czy duży sklep internetowy okażą się w oczach klientów miejscem niewiarygodnym, jest tu ważnym czynnikiem. A jeśli w wyniku wycieku wiele osób straci jeszcze pieniądze, to taka firma staje się po prostu mało bezpieczna. Więc wydaje się, że to bardzo ważny motywator, bo klienci powinni czuć się bezpiecznie, szczególnie gdy korzystają z narzędzi cyfrowych – różnych aplikacji czy stron internetowych.

Czyli także świadomość społeczeństwa dotycząca wartości danych wzrosła?
Zdecydowanie tak, bo po każdym takim wycieku powstaje ryzyko, że dane zostaną użyte do podszycia się pod kogoś albo wykradzenia pieniędzy. RODO przewiduje tu bardzo ważny mechanizm, bo w przypadkach, gdy ryzyko takie jest wysokie, należy zawiadomić osoby, których dane dotyczą – zarówno o samym wycieku, jak i o podjętych środkach. Na tej podstawie podmiot danych może sam również podjąć odpowiednie środki, by ograniczyć skutki wycieku. RODO przewiduje także prawo do odszkodowania z tytułu naruszenia. Co prawda liczba samych pozwów cywilnych wobec firm, które nie „upilnowały" danych

osobowych moim zdaniem nie wzrosła, ale wiemy, że one się zdarzają. Ludzie się tymi sprawami coraz bardziej interesują, a po wycieku dzwonią i pytają, co się stało z ich danymi i jakie są sposoby zabezpieczenia się. Np. jeśli wyciekły dane z dokumentów tożsamości, można wykupić odpowiednie usługi ostrzegające przed próbą ich użycia albo zastrzec ten dokument czy numer PESEL.

Skoro mamy już świadomość wartości danych osobowych, jak to się przekłada na system stworzony przez DGA? Niedawno weszła w życie ustawa wdrażająca ten akt w Polsce. Czy Pana zdaniem możemy się spodziewać jakiegoś większego zainteresowania dzieleniem się danymi w ramach altruizmu danych czy spółdzielni danych?

Odnoszę się do tego sceptycznie od samego początku. Byli nawet tacy, którzy uważali, że to jest w ogóle bez sensu – zarówno DGA, jak i Data Act. Ja bym aż tak daleko idącego wniosku nie formułował, natomiast nie wydaje mi się, żeby była duża chęć do takiej formy dzielenia się danymi. Rozmawiałem z wieloma osobami, w tym ze studentami, i świadomość tych przepisów nie jest jeszcze zbyt duża. Szersze zastosowanie znajdzie pewnie Akt o danych (Data Act), ponieważ firmy mogą wykazywać zainteresowanie korzystaniem z różnych danych zgromadzonych przez urządzenia podłączone do internetu. Natomiast jeśli chodzi o altruizm danych, to nie sądzę, żeby zainteresowanie było ogromne, chociaż jest to inicjatywa na pewno potrzebna. Między innymi pandemia pokazała to, że udostępnianie niektórych rodzajów danych może się okazać społecznie istotne.

Wspomniał Pan DGA i Data Act, ale przepisów, nazwijmy to „nowotechnologicznych" jest cały pakiet. Należą do niego także AI Act, DSA, DMA i inne. Czy one wzmocnią ochronę danych, czy jednak są miejscami sprzeczne między sobą i z RODO, więc finalnie ta ochrona będzie słabsza, bo nie da się wszystkich tych aktów przestrzegać jednocześnie?

Często te akty wymienia się jednym tchem, co nie jest do końca uzasadnione, bo chociaż tworzą one „pakiet cyfrowy", to trzeba pamiętać, że mają różne funkcje. DSA to regulacja uprawnień użytkowników w stosunku do platform, która stanowi uzupełnienie RODO, a w

szerszym wymiarze oba akty mają na celu zapewnienie użytkownikom bezpieczeństwa w środowisku cyfrowym. DMA to z kolei regulacja bardziej horyzontalna, która ma zapewnić uczciwą konkurencję i przejrzystość na rynku cyfrowym.

DGA z kolei tworzy ramy proceduralne i organizacyjne dla udostępniania danych, ale w zakresie danych osobowych nie narusza RODO i nie stanowi samoistnej podstawy ich przetwarzania. Data Act reguluje dostęp do danych generowanych przez urządzenia Internetu Rzeczy i większym stopniu skupia się na danych przemysłowych. Ale tam, gdzie w grę wchodzą dane osobowe pochodzące z urządzeń, Data Act nie modyfikuje RODO. AI Act ma w odniesieniu do systemów sztucznej inteligencji podobną funkcję do RODO, ma zapewniać ochronę praw podstawowych, ale też zdrowia i bezpieczeństwa, jednak przede wszystkim promuje zorientowaną na człowieka i godną zaufania sztuczną inteligencję. Ponadto akt ten zawiera pewne mechanizmy mające wspierać innowację – co stanowi jego drugi cel. To przede wszystkim tzw. piaskownice regulacyjne.

Nie wymieniliśmy tu wszystkich aktów z ostatniego okresu, które też będą miały obszary wspólne z RODO (jak choćby przepisy o cyberbezpieczeństwie), ale warto podkreślić, że to RODO wciąż pozostaje fundamentem, jeśli chodzi o ochronę naszych danych. Pod tym względem właściwie nic się nie zmienia, choć wiele osób miało nadzieję na jakieś odstępstwa od RODO w innych aktach cyfrowych. Procedowana jest obecnie inicjatywa Digital Omnibus, która ma m.in. ułatwić korzystanie z danych na potrzeby trenowania modeli sztucznej inteligencji. Ułatwienie to ma dotyczyć m.in. próby określenia podstawy prawnej takiego przetwarzania.

Digital Omnibus w zakresie AI przesuwa terminy wejścia w życie głównych przepisów AI Actu. Czy to nie osłabi za bardzo ochrony praw obywateli? A może paradoksalnie przez to, że firmy będą mieć więcej czasu na dostosowanie się, a rygory nie będą aż tak ścisłe, realnie wzmocni to tę ochronę?

Postawiłbym na to drugie – po prostu okazało się, że mamy za mało czasu na wdrożenie

obowiązków. Nawet Komisja Europejska dopiero niedawno opublikowała wytyczne w sprawie systemów wysokiego ryzyka. Mam więc nadzieję, że przesunięcie tego terminu i pewne modyfikacje niektórych wymogów przyczynią się do tego, że rynek będzie lepiej przygotowany na nowe przepisy. Nie wydaje mi się też, żeby przez te zmiany stopień ochrony został jakoś znacząco zmniejszony. Dlatego uważam, że to dobrze, iż przesunięto niektóre terminy.

Jeśli mówimy o technologii, to nie zawsze jest ona wykorzystywana w słusznym celu. Prezes UODO dużo czasu i uwagi poświęcił na tematy związane z rozwojem deepfake'ów i na walkę z tym zdecydowanie szkodliwym zjawiskiem. Czy Pana zdaniem silniejsze egzekwowanie przepisów ochrony danych wystarczy do ograniczenia tego zjawiska? Czy potrzebne są zupełnie nowe regulacje w tym zakresie, aby chronić obywateli?

Mnie uczono, że prawo z natury rzeczy nie nadąża za życiem, za zmianami, zwłaszcza technologicznymi. Trzeba się pewnym nowościom najpierw przyjrzeć, żeby zobaczyć, w jakim kierunku idą, i dopiero jak to troszkę okrzepnie, można je regulować. I z deepfake'ami chyba też tak jest, ale jednocześnie już wiemy, że deepfake jako manipulacja może nieść szczególne zagrożenia.

Z jednej strony jest to oczywiście wykorzystanie czegoś wizerunku, i już to samo w sobie wpływa bardzo niekorzystnie na tę osobę, bo deepfake może być użyty np. w filmie pornograficznym. Ale są jeszcze inne skutki. Jeżeli mamy deepfake, na którym osoba publiczna, np. prezydent państwa albo jakiś celebryta, coś reklamuje albo wypowiada treści, które są ewidentną manipulacją czy dezinformacją, to niesie to z sobą trudne do oszacowania skutki społeczne. I mam wrażenie, że obecne regulacje prawne mogą się okazać niewystarczające. Dzisiaj na pewno bałbym się wypowiadać na temat tego, w jakim kierunku takie regulacje powinny pójść.

W dużym stopniu jest to także kwestia wykrywalności takich czynów i stworzenia technologii, którą można by do tego wykorzystać. Osobną sprawą jest również

identyfikowanie deepfake'ów. Przeciętny człowiek, którego wizerunek został wykorzystany w taki sposób, ma mocno ograniczone możliwości udowodnienia, że to jest deepfake, gdyż materiały są coraz bardziej przekonywające – zawierają jego wizerunek i jego głos i coraz mniej anomalii wskazujących na sztuczne wykreowanie.

Warto też edukować (choć być może jest już za późno), że pochopne wrzucanie danych do serwisów społecznościowych kończy się tym, że na podstawie kilkusekundowego nagrania ktoś może stworzyć właśnie taki deepfake. I to praktycznie każdy, bo jeszcze jakiś czas temu technologia ta dostępna była tylko dla specjalistów, a dziś już każdy ma dostęp do takich narzędzi. Co prawda niektóre z nich odmawiają tworzenia filmu z prawdziwą osobą, ale są też dostępne takie, które stworzą tego typu materiały. Dlatego dużym wyzwaniem jest zwalczanie tego typu zjawisk na gruncie technologicznym i prawnym.

Czyli nie tylko to, żeby twórcy musieli oznaczać tego typu materiały, ale też, żeby odbiorcy mieli możliwość zidentyfikowania, że dana treść została stworzona przez AI?

Obawiam się, że obowiązek oznaczania treści wygenerowanych przez AI nie będzie skuteczny, szczególnie tam, gdzie chodzi o celową dezinformację na masową skalę. Zresztą zdjęcie znaku wodnego z filmu nie jest dużym problemem.

Powstaje pytanie, czy państwo nie powinno w tym względzie zachowywać się bardziej proaktywnie i zostać wyposażone w narzędzia umożliwiające bezpośrednią ingerencję w określone treści. I jak to wyważyć z oskarżeniami o cenzurę. Proszę zauważyć, że dzisiaj szczególnie w sferze cyfrowej państwo cofa się do roli nadzorcy; to przedsiębiorcy, platformy, sklepy itd. mają oceniać ryzyko i wprowadzać odpowiednie środki mitygujące. Państwo tylko sprawdza, czy zrobili to dobrze.

Samo RODO przecież opiera się na takim mechanizmie, w przeciwieństwie do poprzednich przepisów, które wprost mówiły, np. że hasło dostępowe ma zawierać określoną liczbę znaków itd. Oczywiście dziś regulowanie w prawie długości hasła byłoby bez sensu bo

zmiany technologiczne są tak szybkie, że to, co dziś jest skutecznym zabezpieczeniem, jutro nim nie będzie. Ale obecnie odpowiedzialność jest przerzucana w większym stopniu na podmioty kontrolowane, a często taki przedsiębiorca nie dostaje od ustawodawcy konkretnych kryteriów lub narzędzi do takiej oceny. To jest dla mnie, jako administratywisty, pewien problem. Weźmy przykład DSA, gdzie szczególnie na bardzo duże platformy i wyszukiwarki przerzuca się odpowiedzialność za identyfikowanie ryzyk systemowych, jak bezpieczeństwo nieletnich czy zagrożenia dla dyskursu politycznego oraz wprowadzenie odpowiednich środków. Organy same takich ocen nie dokonują, jedynie weryfikują, czy skutek został osiągnięty.

Mieliśmy ostatnio konferencję o administratorze danych bez zdolności prawnej. Chodziło o sytuacje, kiedy ten administrator jest, ale niekoniecznie można od niego egzekwować jakieś zobowiązania na drodze cywilnej. Czy to jest w praktyce częsty i poważny problem, czy raczej zagadnienie akademickie?

Rzeczywiście kwestia osobowości prawnej, co potwierdziliśmy podczas tej konferencji, nie jest kryterium decydującym o uznaniu za administratora. Zresztą z samej definicji wynika, że administratorem może być osoba fizyczna, prawna, jednostka organizacyjna itd. Więc, mówiąc krótko, nie musisz mieć osobowości prawnej, żeby być administratorem, bo kryterium wyróżnienia administratora to władztwo nad danymi – czyli to, kto decyduje o celach i środkach przetwarzania danych. Ale też – i ja starałem się na to zwrócić uwagę – bywają takie sytuacje, kiedy jednak to, kto ma osobowość prawną, szczególnie w przypadku rozbudowanych struktur organizacyjnych czy raczej tego, na jakim poziomie w organizacji jest ta osobowość prawna, może mieć znaczenie.

Na konferencji podawałem przykład organizacji, która jest osobą prawną, ale ma oddziały (np. bank). Teoretycznie można sobie wyobrazić, że to ten oddział, który nie ma osobowości prawnej, faktycznie decyduje o celach i środkach przetwarzania danych. To jest przykład hipotetyczny, bo obecnie to raczej się nie zdarza, ale teoretycznie oddział spółki czy

organizacji może mieć własnych klientów i odrębne systemy.

I pojawia się np. taki problem: co w sytuacji, kiedy ten oddział chciałby zawrzeć umowę powierzenia? Przecież we własnym imieniu nie może tego zrobić, może jedynie na podstawie upoważnienia od kierownictwa spółki, ale wtedy robi to w imieniu spółki, a nie swoim. A więc z jednej strony fakt posiadania osobowości prawnej nie ma znaczenia, ale w konkretnych przypadkach, o jakich mówię, może to mieć jednak znaczenie ze względu choćby właśnie na kwestie zaciągania zobowiązań.