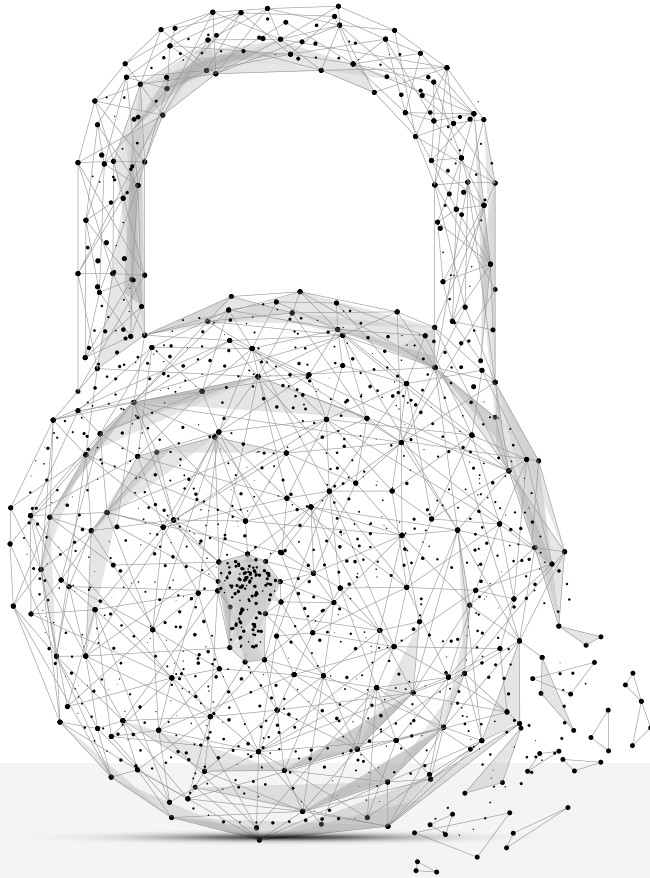
Maciej Kawecki - Doktor nauk prawnych, doradca Ministra Cyfryzacji, w latach 2015-2016 zatrudniony w Biurze Generalnego Inspektora Ochrony Danych Osobowych. Autor kilkudziesięciu publikacji z zakresu ochrony danych osobowych oraz uczestnik wielu krajowych oraz międzynarodowych konferencji naukowych z zakresu prawa nowych technologii.

Na stronie Ministerstwa Cyfryzacji 28 marca br. pojawił się projekt ustawy o ochronie danych osobowych. Jak dużo pracy czeka Ministerstwo odnośnie do zmian w przepisach?

Maciej Kawecki: Nie jestem w stanie precyzyjnie odpowiedzieć na to pytanie, jednak będą to dziesiątki albo setki ustaw. Cały czas pracujemy nad tym, żeby zidentyfikować wszystkie zmiany. W części ustaw są to zmiany techniczne (zmiana nazwy ustawy, numeru ustawy, nazwy organu – mamy termin „administrator bezpieczeństwa informacji", a będzie „inspektor ochrony danych"). Są to też zmiany techniczno-legislacyne, w pewnych przypadkach są zmiany merytoryczne. Pracujemy np. nad Kodeksem pracy i nad art. 22 indeksem 1 KP (to jest tylko przykład), szykuje się pakiet zmian w statystyce publicznej, co jest związane przetwarzaniem danych osobowych w celach statystycznych, pakiet zmian w zakresie obszaru dziedzictwa narodowego i kultury, w zakresie ochrony zdrowia itp. To są duże zmiany i założeniem pani Minister Cyfryzacji jest to, żeby były one prowadzone jednocześnie, aby system był kompletny, a tym samym skuteczniejszy.

Kiedy według Pana nowa ustawa o ochronie danych osobowych weszłaby w życie?

M.K.: Chcemy, żeby ustawa miała vacatio legis, a jednocześnie by weszła w życie w momencie, gdy rozporządzenie unijne o ochronie danych osobowych, rozpoczyna swoje stosowanie, tj. 25.5.2018 r.



Projekt przewiduje powołanie nowego urzędu, nowego prezesa, czy coś poza zmianą nazwy będzie się kryło?

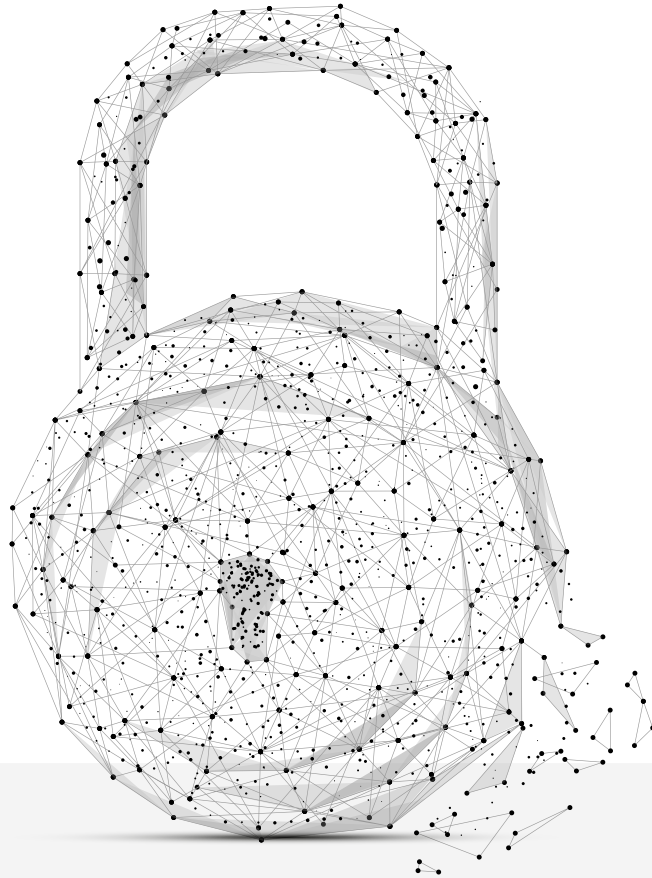
M.K.: Jeżeli chodzi o to, co się zmieni w tym organie, to na pewno chcemy wzmocnić niezależność organu ochrony danych osobowych. Tego nie ma jeszcze w projekcie, ale już mogę powiedzieć, że chcemy przyznać (dzisiaj Generalnemu Inspek-torowi statut naddaje Prezydent RP) organowi prawo do samodzielnego przyznawania sobie statutu. Obecnie GIODO ma jednego zastępcę, chcemy uprawnić organ do powoływania kilku zastępców. Wstępnie myśleliśmy o 3 zastępcach Generalnego Inspektora. Utrzymamy oczywiście tę odrębność budżetową, która jest obecnie. Ponadto utrzymamy kadencyjność organu (przesłanki odwołania wynikają wprost z rozporządzenia unijnego), w związku z czym nie oczekiwałbym tutaj żadnej rewolucji.

W uzasadnieniu projektu opisywał Pan kwestie kontroli. Czym różnią się one od kontroli, które obecnie przebiegają?

M.K.: Zmiany polegają na tym, że wprowadziliśmy 30-dniowy termin, którego dzisiaj nie ma, na przeprowadzenie kontroli. W tym właśnie okresie organ musi przeprowadzić kontrolę. Czas ten zaczyna biec od momentu zapukania do przedsiębiorcy do momentu podpisania przez niego protokołu kontrolnego. Często kontrola jest okazją do wydłużania prowadzonych postępowań. Wprowadziliśmy dodatkowo możliwość skorzystania przez inspektorów (co też wzmacnia ich pozycje) z pomocy funkcjonariuszy policji, czego dzisiaj nie ma. Przewidzieliśmy również, że inspektorzy mogą przeprowadzać niezapowiedziane kontrole (wyłączyliśmy w tym zakresie zastosowanie ustawy o swobodzie działalności gospodarczej). Celem tych zmian jest wzmocnienie ochrony danych osobowych.

Projekt przewiduje wprowadzenie kar. Jak Ministerstwo widzi te 20 milionów euro w skali polskiego przedsiębiorstwa oraz w administracji publicznej?

M.K.: Jeżeli przedsiębiorca ma gigantyczny przychód, to kara wydaje się karą racjonalną, wszystko zależy od przychodu. Jeżeli ktoś ma miliard przychodu, to kara 20 mln euro może być akceptowalna. Należy jednak wskazać, że kara to nie jedyny instrument w rękach organu. Prezes Urzędu, działając racjonalnie, ma być nie tylko egzekutorem, lecz także – a może przede wszystkim – krajowym konsultantem, ma doradzać, jak postępować, by działać zgodnie z prawem. A przedsiębiorca ma wybór – podjęcie złej decyzji może skutkować właśnie m.in. obowiązkiem pokrycia ogromnej kary finansowej. Natomiast mamy spory problem z nakładaniem kar na administrację publiczną, i to jest druga część pytania. Po opiniach, które dochodzą do nas po ukazaniu się projektu, widzimy, że są one bardzo skrajne. Jedni uważają, że nawet 100 000 zł, które



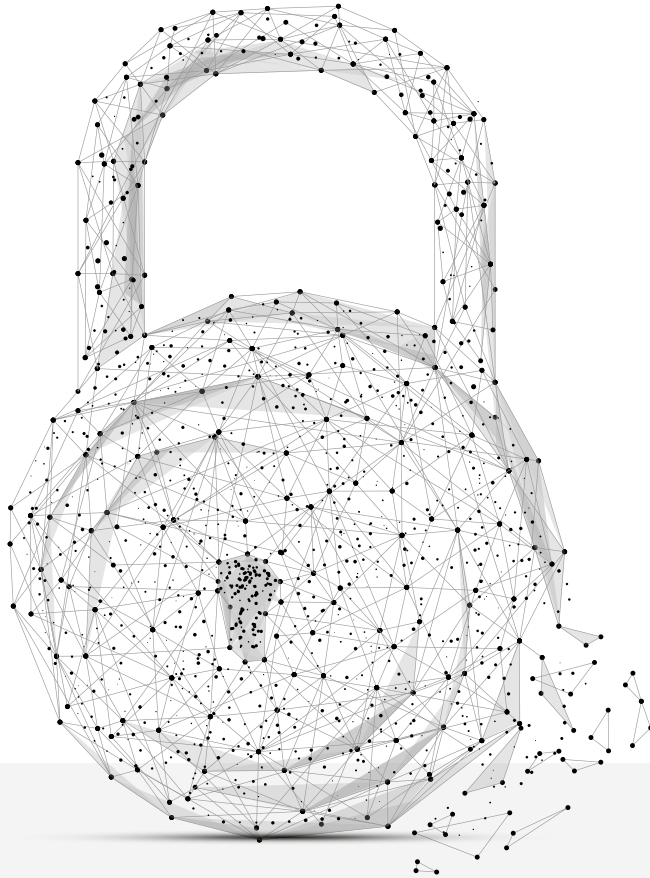
wprowadziliśmy, czyli obniżyliśmy kilkadziesiąt razy możliwość nakładania kar, jest naruszeniem interesów obywateli, bo tak naprawdę to jest pośrednio opłata, którą wnoszą obywatele za błędne działanie organu. Część osób wskazuje również, że takie rozwiązanie jest przelewaniem z tego samego budżetu, czyli z jednej części do drugiej tego samego budżetu. Z drugiej strony, pojawia się problem, w jaki sposób skutecznie egzekwować ochronę danych osobowych, w sektorze publicznym. Pani Minister Cyfryzacji zdecydowała się na zawężenie kręgu podmiotów publicznych, wobec których w ogóle można nałożyć kary, a nawet w tym przypadku tylko do 100 000 zł. A dlaczego taki wymiar? Dlatego, że uznaliśmy, iż to jest właśnie taki wymiar kary, który z jednej strony będzie odczuwalny, a z drugiej strony nie wpłynie na realizowanie zadania publicznego przez dany organ, bo kwota 20 mln euro jest kwotą, która bardzo często przekracza budżet organu państwowego, kilkakrotnie. Nie może być również tak, że obywatel za jedno naruszenie ochrony jego danych osobowych przez sektor publiczny karany jest kilkakrotnie. Po pierwsze, karą, jaką jest już sam fakt naruszenia. Po drugie, środki publiczne pochodzą z kieszeni podatników, a więc to oni pośrednio będą zobowiązani do pokrycia nałożonej na organ kary. Wreszcie, ogromna kara może wpłynąć na poziom wykonywania przez organ zadań publicznych w danym roku budżetowym, obniżając ich jakość. Chcemy takich sytuacji uniknąć. Nie można również zapominać, że administracja publiczna działa na podstawie oraz w granicach prawa, a przetwarzanie przez nią danych osobowych odbywa się wyłącznie w interesie publicznym – a nie partykularnym interesie przedsiębiorcy, jak ma to często miejsce w sektorze prywatnym. Ocena przypadków naruszeń ochrony danych osobowych w ostatnim czasie pokazuje również, że wśród tych najbardziej poważnych, a więc wycieków danych, niewiele z nich miało miejsce w sektorze publicznym. Natomiast dlaczego zawyżyliśmy krąg tych podmiotów publicznych, na które w ogóle kara może być nałożona? Staraliśmy się wskazać taki krąg podmiotów publicznych, które w największym stopniu przetwarzają dane, w tym również dane osobowe wrażliwe. Do tego kręgu należy m.in.: ZUS, NFZ, które to podmioty przetwarzają ogromne ilości danych, w tym wrażliwych.

Patrząc na listę podmiotów podlegających karze, widać, że zostały na niej państwowe i samorządowe jednostki instytucji kultury, dlaczego?

M.K.: Ponieważ jako kryterium wyłączenia przyjęliśmy administrację rządową, szeroko rozumianą (nie tylko Radę Mini-strów) i administrację samorządową. Uznaliśmy, że w przypadku i administracji rządowej, i samorządowej kształtowanie polityki państwa w rozumieniu nie politycznym, tylko w rozumieniu interesu publicznego, znajduje swoją emanację w największym stopniu w działaniach tych właśnie organów.

Zmiany dotyczą również ABI, co się najbardziej zmieni w jego pracy?

M.K.: Tak naprawdę wzmocni się jego niezależność. Rozporządzenie o ochronie danych osobowych przyznaje mu wprost gwarancje



niezależności. Na jednym ze spotkań, które odbyłem ze stowarzyszeniami administratorów bezpieczeństwa informacji, stowarzyszenie zwróciło uwagę na coś, czego ja nie zauważyłem wcześniej, że dzisiaj jednym z kryteriów kwalifikacji inspektorów ochrony danych jest wiedza. Tutaj będzie to wiedza i doświadczenie i oni rozumieją to właśnie w taki sposób, że to się zmienia, ponieważ nie tylko wiedza, lecz także dorobek zawodowy, będzie miał znaczenie na powołanie danej osoby na ABI. Natomiast jeżeli chodzi o inspektorów, zmienia się też to, że dzisiaj w ustawie administratorzy bezpieczeństwa informacji są w pewnym sensie adresatami obowiązków, natomiast w rozporządzeniu adresatami obowiązków jako takich jest tylko administrator danych bądź podmiot przetwarzający, czyli podwykonawca administratora. Tak naprawdę zakres zadań i obowiązków inspektora ochrony danych w całości będzie należał wyłącznie do administratora, to on będzie wskazywał na rolę, jaką ma odgrywać inspektor ochrony danych w danej organizacji.

Czy doświadczenie ma być zdobywane na stanowisku ABI?

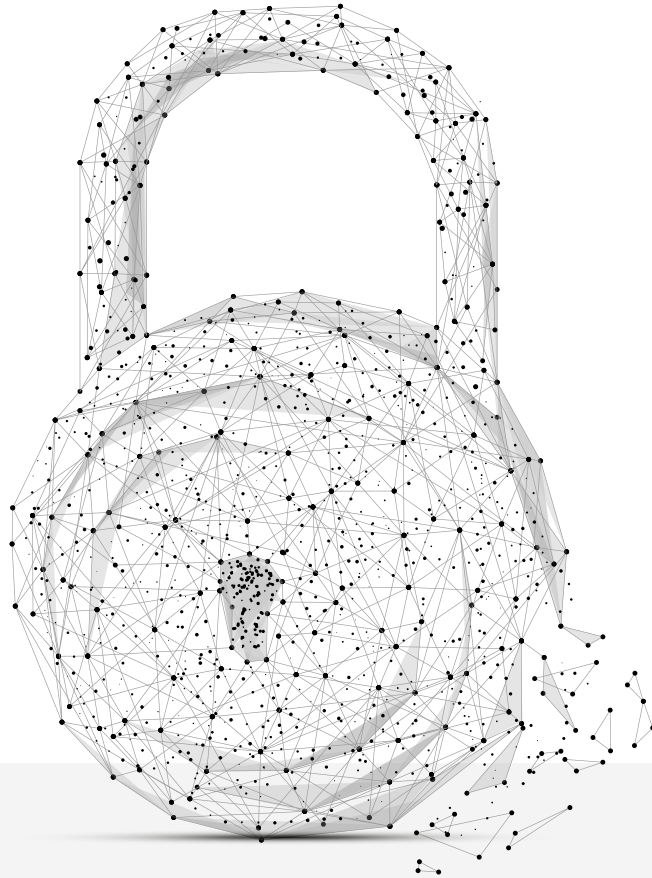
M.K.: Przepisy prawne mówią „doświadczenie w obszarze ochrony danych osobowych", więc ja rozumiałbym to szerzej.

Jak będą wyglądały procedury m.in.: zgłaszania, odwołania obecnych ABI i przyszłych inspektorów?

M.K.: Treść art. 37 ust. 7 ogólnego rozporządzenia o ochronie danych osobowych uznaliśmy za nieprecyzyjną. Na jego podstawie nie wiadomo, w jakim terminie, w jakiej formie notyfikacja powinna następować, czy organ ma możliwość prowadzenia ewidencji, czy nie ma mieć możliwości prowadzenia ewidencji notyfikacji itp. Zdecydowaliśmy się więc doprecyzować to w przepisach ustawowych.

W projekcie jest napisane, że jeżeli obecny administrator bezpieczeństwa będzie chciał zostać na swoim stanowisku, to trzeba to zgłosić?

M.K.: Tak. Obecny administrator bezpieczeństwa informacji w ciągu 3 miesięcy będzie musiał podjąć jakąkolwiek aktyw-ność, jeżeli nie podejmie, to od 1 września przestanie być inspektorem ochrony danych. Możliwość wyrażenia przez ABI swojej decyzji może być trojaka: nie podejmuje on żadnej aktywności, czyli przestanie być 1.9.2018 r. inspektorem, może wprost wystąpić do Prezesa Urzędu z żądaniem wykreślenia go, może też zawiadomić Prezesa Urzędu o swoich danych i wtedy Prezes Urzędu uzna, że dotychczasowy ABI po 1.9.2018 r. się będzie inspektorem ochrony danych osobowych.



Z punktu widzenia sektora publicznego, na co jeszcze warto zwrócić uwagę w ogólnym rozporządzeniu o ochronie danych osobowych?

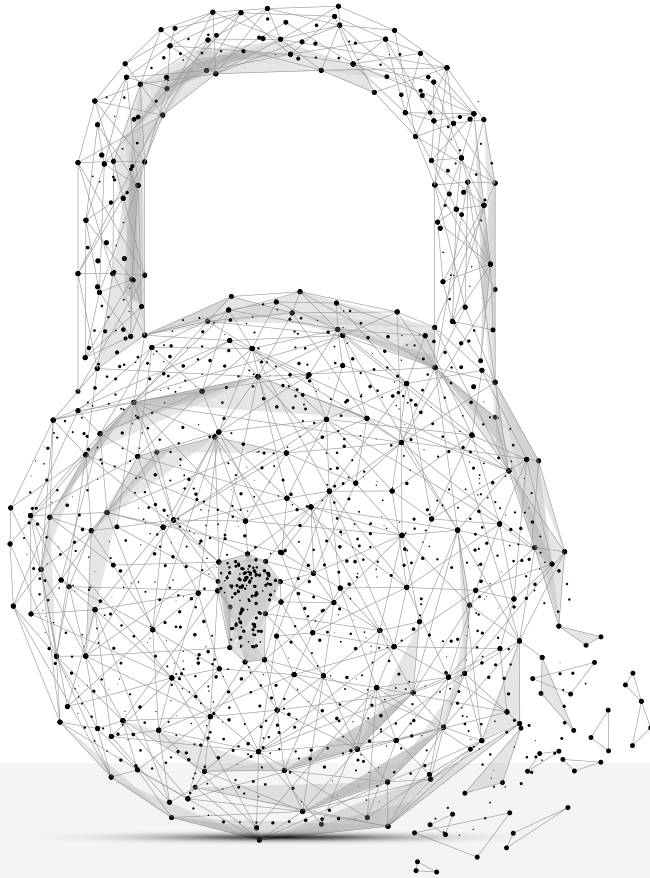
M.K.: Administracja publiczna musi zwrócić uwagę na to, że w większości przypadków adresatami norm ogólnego rozpo-rządzenia o ochronie danych osobowych są w jednakowym stopniu i administracja, i sektor prywatny. Obok kar finanso-wych, o których była już mowa, wyjątkiem są kodeksy postępowań oraz certyfikcja. Wydaje się, że są to mechanizmy, które kierowane są tylko do sektora prywatnego, nie obejmując sektora publicznego.

Na czym polegać będzie korzyść certyfikacji?

M.K.: Będzie ona polegała głównie na stymulowaniu konkurencyjności na rynku. Wykształci się pewna klasa przedsię-biorców, kancelarii, podmiotów, które ze względu na to, że posiadają certyfikat, są uważani za bardziej wyspecjalizowa-nych, za bardziej profesjonalnych. Co ważne, jednym z kryterium wymierzania w administracji publicznej kary w przypadku naruszenia zasad ochrony danych osobowych jest fakt posiadania przez przedsiębiorców certyfikatu. Nie zwalnia on w żaden sposób od niczego, jednak organ może przeprowadzić postępowanie kontrolne, ale wymierzając karę, bierze pod uwagę również to, że ktoś starał się, czyli wdrożył kodeksy, nabył certyfikat. Istotne jest to, że w naszym projekcie przewidujemy możliwość przyznawania certyfikacji tylko sektorowi prywatnemu. Rozporządzenie o ochronie danych osobowych dało nam możliwość przyznania takiej kompetencji organowi bądź sektorowi prywatnemu. My jednak uznaliśmy, że najlepszym rozwiązaniem jest przyznanie prawa do akredytacji podmiotów certyfikujących, Prezesowi Urzędu, natomiast na drugim etapie przyznanie kompetencji do certyfikacji tylko sektorowi prywatnemu. Po pierwsze, certyfikacja podejmowana przez Prezesa Urzędu stanowiłaby dla niego znaczące obciążenie administracyjne, po drugie, certyfikacja dokonywana przez sektor prywatny byłaby martwa, bo jeżeli ktokolwiek miałby wybór bycia certyfikowanym przez Prezesa Urzędu i przez sektor prywatny, wybierałby oczywiście Prezesa Urzędu, który będzie miał przecież monopol do nakładania kar administracyjnych. W pewnym sensie stworzylibyśmy więc klasyfikację certyfikatów, co nie byłoby dobre.

Na co zwracają Państwo szczególną uwagę, konstruując nowy krajowy system ochrony danych osobowych?

M.K.: Tak naprawdę na wszystko, co zbliża nas do stworzenia bardziej skutecznego systemu ochrony danych osobowych. Będziemy mieli sprawniejszy, szybszy, lepiej funkcjonujący organ ochrony danych osobowych. Założeniem Ministra Cyfryzacji jest stworzenie nowego systemu ochrony danych osobowych, co nie znaczy, że unicestwiamy to, co przez 20 lat dobrego w Polsce zostało zrobione w tym zakresie. Korzystamy



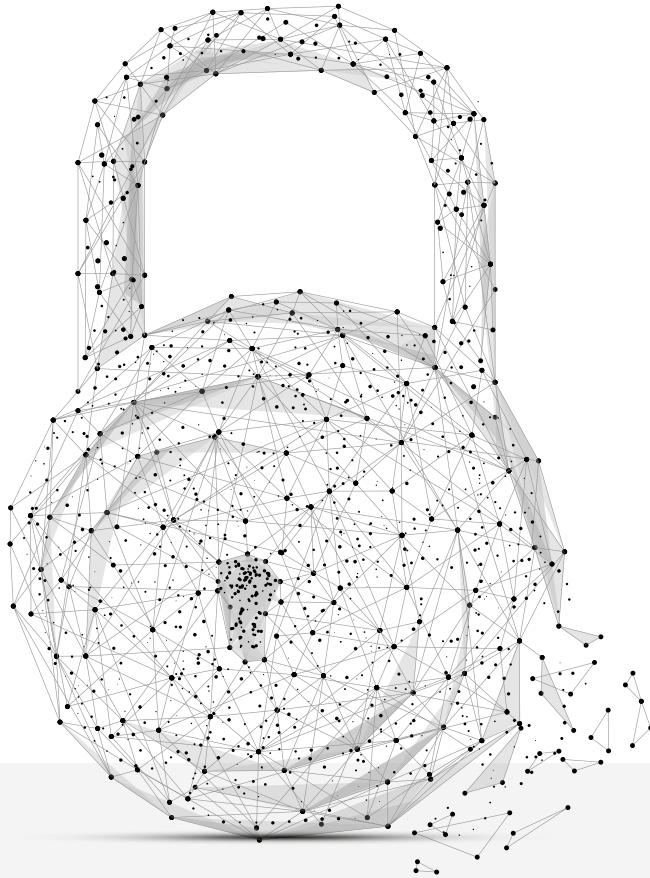
z tej tradycji, ale nie możemy, pod jej przykrywką, akcep-tować chociażby tego, że dzisiaj na wydanie rozstrzygnięcia przez GIODO czeka się 2 lata, a do wydania wyroku obywatel czeka w sporadycznych, ale jednak, przypadkach 1600 dni. Mówimy tutaj o prawach podstawowych i rozstrzygnięcie w ich przedmiocie musi być wydane w trybie natychmiastowym, stąd właśnie to postanowienie zabezpieczające, które jest wprowadzone u nas w ustawie krajowej. Powyższe powtarzam jak mantrę, bo ta mantra stanowi uzasadnienie znacznej liczby projektowanych przez nas przepisów. Trzeba też wzbudzić u obywateli świadomość, że z majem 2018 r. diametralnie zmienia się system ochrony danych osobowych.

Projekt przewiduje drogę sądową jako wzmocnienie systemu ochrony.

M.K.: Tak, jest to kolejny przykład wzmocnienia ochrony systemu ochrony danych osobowych. Obywatel, którego ochrona danych osobowych została naruszona, będzie miał kilka możliwych dróg postępowania. Będzie mógł złożyć skargę do Prezesa Urzędu na wzór skargi składanej dzisiaj do GIODO. Będzie mógł też wybrać drogę postępowania sądowego, kierując pozew bezpośrednio do sądu powszechnego – rezygnując bądź nie ze skargi do Prezesa Urzędu. Mówiąc inaczej, skarga składana do Prezesa Urzędu na kanwie projektu Ministra Cyfryzacji nie będzie wyłączała w żadnym zakresie możliwości wystąpienia z pozwem do sądu powszechnego, i odwrotnie – skarga do sądu powszechnego nie będzie wyłączała skargi do Prezesa Urzędu. Proszę zauważyć, że nie wyłączamy również możliwości wystąpienia z roszczeniem z art. 24 KC, czyli z tytułu naruszenia dóbr osobistych.

Jak inne kraje unijne przeprowadzają reformę ochrony danych osobowych?

M.K.: Mamy informacje o Niemczech, w stosunku do których ten proces legislacyjny jest bardziej zaawansowany. Istotą było, aby przed wyborami parlamentarnymi, które odbędą się jesienią w Niemczech, pakiet ten został przyjęty w parlamencie. Zapoznałem się również z projektem niemieckim i rzeczywiście rodzi poważne wątpliwości co do zgodności z rozporządzeniem o ochronie danych osobowych. Niemcy przyjęli technikę legislacyjną częściowego przepisania rozporządzenia do krajowego porządku prawnego – co rodzi poważne wątpliwości z punktu widzenia zgodności takich działań z prawem UE. Nie jest jednak moją rolą ani rolą Ministra Cyfryzacji ocena zgodności z prawem UE działań legislacyjnych podejmowanych przez inne państwa.



Jak na takiej zmianie systemu ochrony danych osobowych w całej Europie skorzysta szary obywatel?

M.K.: Korzyść będzie polegała m.in. na tym, że w razie transeuropejskiego naruszenia zasad ochrony danych osobowych obywatel będzie mógł wystąpić ze skargą do organów ochrony danych różnych państw, a te w ramach stworzonej europej-skiej sieci ochrony danych osobowych będę zmuszone do skomunikowania się między sobą. Organy uzyskują w tym zakresie chociażby uprawnienie do przeprowadzania wspólnych operacji kontrolnych.

Czy coś jeszcze ulegnie rewolucyjnej zmianie?

M.K.: Bez wątpienia zagadnienie zgody rodzica na przetwarzanie danych osobowych dziecka w internecie. Rozporządzenie unijne wprowadza w tym zakresie granicę wieku lat 16, do której to zgodę taką w imieniu dziecka udzielają rodzice. Ministerstwo chce obniżyć wiek z 16 na 13 lat, niemniej jednak niezależnie od powyższego przepis rodzi poważne wątpliwości co do tego, w jaki sposób będzie przestrzegany. Powstają chociażby pytania, w jaki sposób weryfikować tożsamość rodzica. Wydaje się, że nie można żądać podania w tym celu numeru telefonu rodzica, bo będzie to stanowiło chociażby naruszenie zasad adekwatności. Jako naruszenie takie kwalifikowane powinno być również odebranie skanu dowodu osobistego. Jak długo i w jaki sposób archiwizować zgody, w jaki sposób odbierać te zgody, co to znaczy konkretnie „usługi oferowane bezpośrednio dziecku" – czy są to usługi, które bezpośrednio oferowane są ze względu na swoją powszechną treść, czy ze względu na samą treść dedykowaną dziecku, czyli filmy, bajki, książki dla młodzieży itd. Tego wszystkiego rozporządzenie unijne nie wyjaśnia.

Jakie są pierwsze sygnały po tym, jak projekt ujrzał światło dzienne?

M.K.: Pierwsze sygnały są takie, że odbiór samego projektu jest dobry. Oczywiście docierają do nas również uwagi, za które ogromnie dziękujemy. Są one jednak bardzo często ze sobą sprzeczne. Inne oczekiwania co do krajowej reformy ma GIODO, inne oczekiwania przedsiębiorcy, a jeszcze inne organizacje pozarządowe. Każdy z tych podmiotów ocenia prze-pisy z punktu widzenia ochrony innych wartości, a rolą Ministra Cyfryzacji jest znalezienie w tym zakresie złotego środka. Cały czas go szukamy, stąd decyzja o udostępnieniu części projektu ustawy już teraz. Liczyliśmy tym samym na otwarcie dyskusji, która przerodzi się – w co wierzę, w bardzo dobrą, skuteczną legislację.