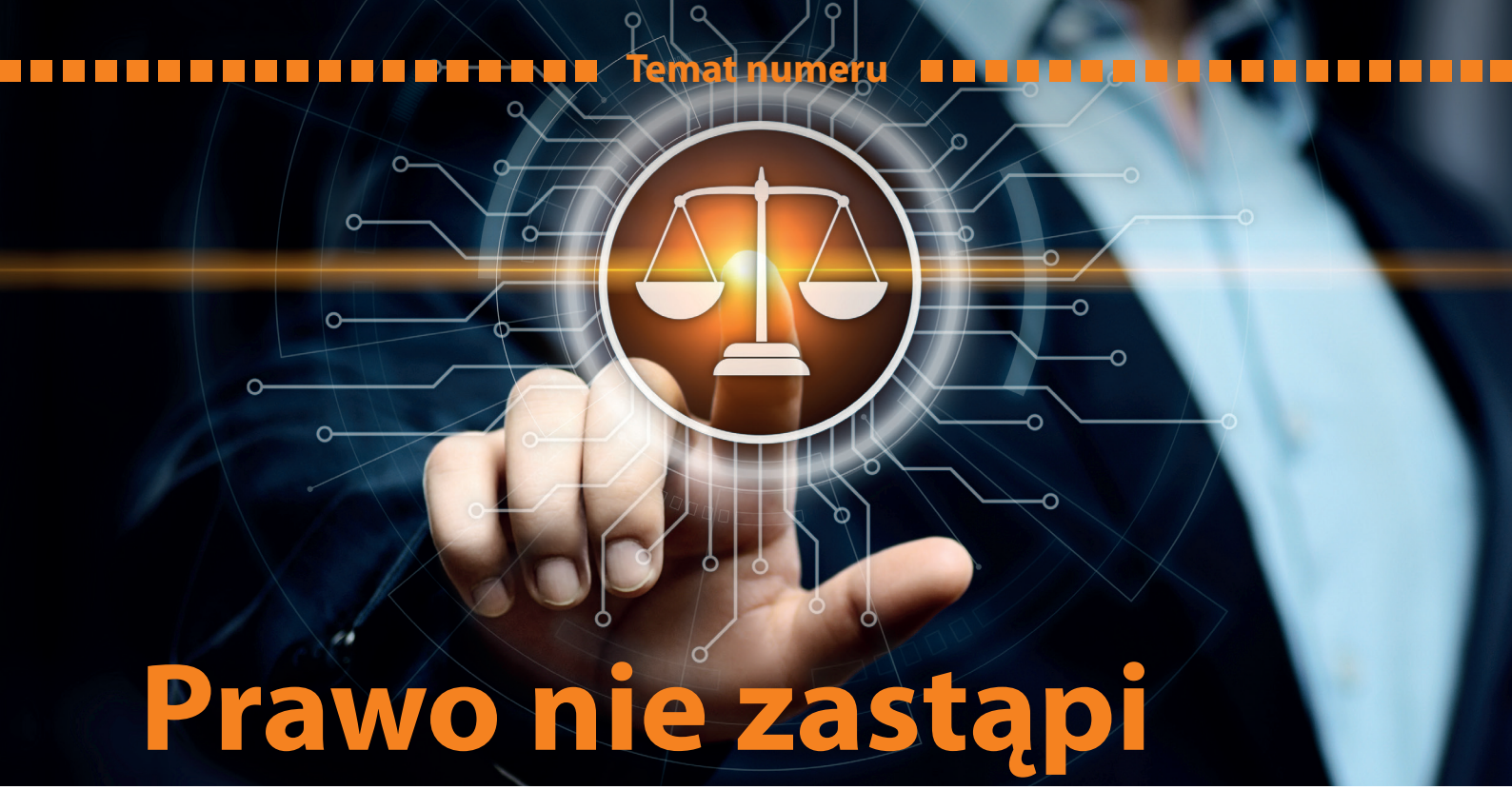


Prawo nie zastąpi zdrowego rozsądku

Prawo nigdy nie nadążało za technologią. Unia Europejska, stając na straży praw podstawowych i wolności obywateli, generuje kolejne akty prawne mające na celu uregulowanie cyfrowego świata. O ich niedoskonałościach i potencjalnych skutkach dla gospodarki rodzimej i europejskiej dyskutują uznani prawnicy i eksperci informatyki i komunikacji elektronicznej.

W dyskusji udział wzięli członkowie PTI:

dr Agnieszka Besiekierska
– adwokat od kilkunastu lat doradzająca w obszarze ICT, adiunkt w Katedrze Prawa Informatycznego na Wydziale Prawa i Administracji UKSW

dr Joanna Mazur
– Wydział Zarządzania i DELab UW

dr hab. Arwid Mednis
– Wydział Prawa i Administracji UW i Kancelaria Kobylańska Lewoszewski Mednis sp. j.

Jarosław Mojsiejuk
– ekspert Rady ds. Cyfryzacji ubiegłej i obecnej kadencji, Związek Cyfrowa Polska, pracownik HPE

Wiesław Paluszyński
– prezes PTI

Artur Piechocki
– radca prawny, założyciel kancelarii APLAW, współzałożyciel i Prezes Sądu Polubownego ds. Domen Internetowych przy PIIT, ekspert Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji

Dyskusję prowadził
dr Tomasz Kulisiewicz
– sekretarz Sektorowej Rady ds. Kompetencji – Informatyka

Tomasz Kulisiewicz: Finiszują prace nad kilkoma istotnymi regulacjami europejskimi, dotyczącymi zarówno samych danych, jak i szeroko pojętej komunikacji elektronicznej. Które z nich mogą mieć największy wpływ na gospodarkę, życie społeczne i na administrację publiczną w Polsce?

Agnieszka Besiekierska: Wydaje mi się, że najistotniejszym aktem będzie świeżo przyjęta dyrektywa NIS 2. Cyberbezpieczeństwo jest kluczowe dla różnych technologii i obejmuje wszystkie działalności w cyfrowym świecie. Dyrektywa NIS 2 dotyczy znacznie większej liczby podmiotów niż jej poprzednia wersja i wprowadza m.in. sankcje finansowe, co sprawia, że jej przepisy trzeba będzie poważnie potraktować. Widzę tu analogię do RODO.

Jarosław Mojsiejuk: Cyberbezpieczeństwo jest bardzo ważne we wszystkich dziedzinach. Nowa dyrektywa obejmuje komunikację elektroniczną i administrację publiczną, wprowadza też obowiązkową certyfikację w kluczowych rozwiązaniach. Uważam, że implementacja NIS 2 może nawet wymagać nowej ustawy o KSC, nie tylko jej nowelizacji.

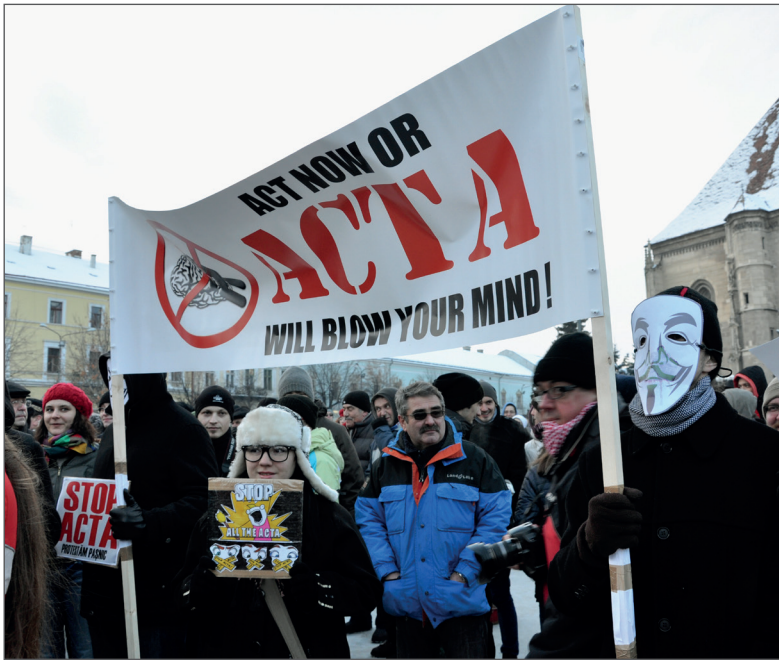
Dla mnie szczególnie ważne są prace nad tymi rozporządzeniami unijnymi, które dotyczą zarządzania danymi. Jedno z nich już mamy. To Data Governance Act, rozporządzenie w sprawie zarządzania danymi wprowadzające nowy wymiar w organizacjach – wymiar danych. Drugie to Europejski akt w sprawie danych (Data Act). Przedstawiciele biznesu na razie nie wydają się być nim szczególnie zainteresowani, choć budzi kontrowersje. Zakłada np. zakaz transferu danych nieosobowych poza granice europejskiego obszaru gospodarczego (z nielicznymi wyjątkami). Jest to regulacja bardziej restrykcyjna niż RODO. A co ze Stanami Zjednoczonymi? Jak ta regulacja wpłynie na dostawców usług chmurowych? UE promuje suwerenność cyfrową, ale ta suwerenność ma wyraźnie ostrze antyamerykańskie. Amerykańscy dostawcy chmury w państwach europejskich zajmują 70% rynku i niektóre unijne prezydencje dążyły do tego, żeby ten udział ograniczyć. Byłaby to duża szkoda dla naszego rynku.

Trudno natomiast na razie ocenić wpływ Aktu w sprawie sztucznej inteligencji (AIA), bo trwają prace i konkurują ze sobą dwa podejścia: po jednej stronie są zwolennicy bezwzględnej konkurencji rynkowej, po drugiej – osoby reprezentujące perspektywę europejską, stojącą na straży praw obywateli. Nie ulega jednak wątpliwości, że AIA przyniesie istotne zmiany, bo zmieniona zostanie sama definicja sztucznej inteligencji i zostanie poszerzony zakres terytorialny obowiązywania aktu. Obejmie on bowiem dostawców i użytkowników systemów sztucznej inteligencji także spoza UE, jeśli rezultaty ich działania dotyczą terytorium Unii lub jej obywateli.

Artur Piechocki: Dla mnie osobiście przykładem dobrej regulacji jest rozporządzenie w sprawie odporności na zagrożenia cyfrowe (DORA). Akt ten jest skierowany do określonego sektora, więc wąski, ale niezwykle precyzyjny. Pokazuje mechanizmy związane nie tylko z bezpieczeństwem ICT, lecz także z zarządzaniem kryzysowym. To kwintesencja tego, co ważne w cyberbezpieczeństwie i – co istotne – proste do zastosowania.

Rola aktów prawnych zależy od tego, do kogo są kierowane. Akt o usługach cyfrowych (DSA) ma chronić użytkowników, na straży konkurencji i demonopolizacji stoi Akt o rynkach cyfrowych (DMA), dla wszystkich będzie ważna implementacja NIS 2. Plusem NIS 2 jest obejmowanie coraz większego zakresu sektorów i łańcuchów dostaw dla podmiotów infrastruktury krytycznej. Zarówno NIS 2, jak i DORA odnoszą się do utrzymania ciągłości działania organizacji oraz planów przywracania działania po incydencie.

Joanna Mazur: Zgadzam się, że dużo zależy od tego, do kogo kierujemy regulację i co chcemy osiągnąć. Dla mnie najistotniejszy jest akt o rynkach cyfrowych. Cieszę się, że są podejmowane wysiłki na rzecz zmiany struktury rynku. Jednak z pewnością żaden ze wspomnianych aktów nie będzie tak kontestowany jak ACTA, ani nie zapisze się tak szeroko w świadomości wszystkich jak RODO.



Obrońcy swobód obywatelskich masowo protestowali przeciwko dołączeniu UE do ACTA (Anti-counterfeiting Trade Agreement) – układu między Australią, Kanadą, Japonią, Koreą Południową, Meksykiem, Marokiem, Nową Zelandią, Singapurem, Szwajcarią i USA. ACTA to umowa handlowa zobowiązująca jej sygnatariuszy do walki z łamaniem prawa własności intelektualnej oraz handlem podrabianymi towarami. Protestujący obawiali się, że pod pretekstem walki z piractwem będą cenzurowane różne treści w Internecie.

Arwid Mednis: Na pytanie o istotność wprowadzanych regulacji odpowiem jak rasowy prawnik: to zależy. W niektórych przypadkach te akty pojawiają się dlatego, że trzeba jakąś sferę uregulować. Funkcją UE i jej organów jest rozwój gospodarczy Unii, jak również ochrona praw podstawowych. My może byśmy i nie chcieli regulować sztucznej inteligencji, ale musimy, bo ta technologia niesie konkretne zagrożenia dla praw podstawowych.

Uprzedzam następne pytanie: czy w ten sposób nie hamujemy biznesu? Pewnie tak. Stworzenie aktu prawnego to dopiero początek, prawdziwe problemy zaczynają się na etapie stosowania prawa. Za tekstem prawa idzie mnóstwo zaleceń, opinii, wytycznych ze strony różnych organów. Cyberbezpieczeństwo jest bardzo ważne, trzeba mieć jednak na uwadze, że podmiotowo dyrektywa NIS 2 nie będzie dotyczyć nas wszystkich. To jest cecha prawa europejskiego, które działa na zasadzie pewnej proporcjonalności: reagujemy tam, gdzie jest to niezbędne.

W regulacji cyberbezpieczeństwa nie jest ważne cyberbezpieczeństwo jako takie, ale ochrona usług najważniejszych (kluczowych, cyfrowych i administracyjnych). Natomiast nie mamy ogólnej regulacji, jak my wszyscy powinniśmy zachowywać się w sieci, mamy tylko regulacje fragmentaryczne.

> *Nie do końca widzę sens niektórych wspomnianych aktów prawnych i uważam, że koszt ich wdrożenia w przedsiębiorstwach może się okazać niewspółmierny do korzyści.*

Wysocy urzędnicy brukselscy częściowo podzielają taką opinię. Nie wszyscy sobie wyobrażają, jak to będzie działać, a na dodatek pojawiają się pewne komplikacje. Np. w Data Act mamy zakaz stosowania niedozwolonych klauzul w umowach dotyczących udostępniania danych. Kiedy przeczytałem ostatnią wersję przedstawioną w ramach prezydencji czeskiej, to byłem jako praktyk bardzo zdziwiony: jak przedsiębiorca będzie sprawdzał w stosunku do kogo będzie mógł klauzule zastosować, a do kogo nie? To oznacza obowiązek pozyskania od kontrahenta masy informacji, w tym ujawnienia jego powiązań. Ten problem ujawni się dopiero na etapie stosowania prawa. Może się okazać, że akty budowane w zbożnych celach okażą się niedrożne i będziemy mieli problem z ich stosowaniem. Obym się mylił.

Agnieszka Besiekierska: Również odnoszę wrażenie, że podejście do tworzenia nowego prawa na poziomie UE jest bardzo pryncypialne. Ważne stają się zasady, a nie koszty. Ekonomiczna analiza prawa jest dziedziną funkcjonującą głównie w środowisku akademickim i nieszczególnie popularną, a szkoda. Moim zdaniem coraz rzadziej nowym regulacjom towarzyszą solidne analizy dotyczące ich efektywności i kosztów.

Jarosław Mojsiejuk: Z punktu widzenia przedsiębiorstwa mamy do czynienia ze zjawiskiem, które Michał Jaworski niegdyś ochrzcił mianem tsunami legislacyjnego. Tych aktów jest tak wiele, że sami jako prawnicy mamy spory problem z ich ogarnięciem.

Tsunami jest delikatnym określeniem, dosadniej mówi się o biegunce legislacyjnej…

Jarosław Mojsiejuk: Akceptuję oba określenia w zależności od stanu emocjonalnego rozmówcy. Słusznie podnosimy sprawę kosztów regulacji. Projekt Data Act chroni szczególne prawa różnego typu konsumentów oraz małych i średnich firm i wprowadza przenaszalność danych użytkowników Internetu Rzeczy. Urządzeń IoT będzie coraz więcej i nikt nie szacuje kosztów wytworzenia interfejsów. Jeśli azjatyccy konkurenci nie będą musieli zapewniać tej przenaszalności, to na pewno wpłynie to niekorzystnie na konkurencyjność zobowiązanych do tego podmiotów unijnych.

Przedsiębiorstwo, w którym pracuję, ma platformę sprzedażową dla profesjonalnych odbiorców, oferuje też usługi chmurowe. Za chwilę będzie musiało według nieistniejących jeszcze standardów stworzyć przenaszalność danych chmurowych pomiędzy różnymi dostawcami. Wymyślono to m.in. dlatego, żeby uderzyć w największe firmy, ale koszty dla małej firmy z Polski będą proporcjonalnie znacznie wyższe niż dla światowego potentata. Zaczynamy też dostrzegać sprzeczności z innymi aktami. Data Act nakłada np. obowiązek ujawnienia danych objętych tajemnicą przedsiębiorstwa. Naturalne wydaje się więc pytanie, na czym ma polegać ochrona tajemnicy handlowej w UE? Z jednej strony mamy prawa podstawowe, z drugiej – ochronę przed nieuczciwą konkurencją.

Wiesław Paluszyński: Już RODO pokazało, jak fikcja góruje nad rzeczywistością. Mamy fasadową implementację – niech mi ktoś pokaże podmiot publiczny, który ma opisane procesy, zdefiniowane obszary ryzyka związane z przetwarzaniem danych osobowych i powstałą w efekcie mapę ryzyk. 99% podmiotów administracji publicznej, która przetwarza najwięcej danych osobowych, uprawia fikcję. Firmy prawnicze przychodzą do takich podmiotów z gotową mapą ryzyk (której nikt nie będzie czytał) do umieszczenia w 4 metrach bieżących dokumentacji na półce. Tak wygląda praktyka wdrażania RODO i nikt nad tym nie panuje. Gdyby mała lub średnia firma chciała funkcjonować zgodnie z tymi wszystkimi aktami, na pewno by zbankrutowała.

Arwid Mednis: Wdrożenie RODO poszło w złym kierunku. Podejście oparte na ryzyku (*risk base approach*) ze strony prawodawcy było słuszne, ale my popadliśmy w jakąś

gorączkę procedur, polityk i klauzul, o wypaczeniach typu „szafki zgodne z RODO" nie wspominając. Najważniejsze stało się posiadanie „papierów" na okoliczność kontroli. Sens regulacji został przesłonięty przez formalizm. Natomiast co do podmiotów publicznych: od dawna jestem przeciwny ich pobłażliwemu traktowaniu.

Artur Piechocki: W odniesieniu do RODO byliśmy na początku sceptyczni, bo widzieliśmy, że użytkownik w Europie musi o wiele więcej „przeklikać", żeby dotrzeć do poszukiwanej informacji na stronie internetowej niż użytkownik w USA, co od razu nas stawiało na gorszej pozycji. Z czasem jednak RODO stało się na tyle powszechne, że poszczególne kraje, a także niektóre stany USA zaczęły wdrażać rozwiązania wzorowane na RODO. A więc RODO wytyczyło kierunek międzynarodowy, nie tylko w Europie. Na pewno prywatność jest teraz lepiej chroniona, choć zgadzam się, że zbytni formalizm wypacza ideę.

Wiesław Paluszyński: Jestem zwolennikiem określenia biegunka legislacyjna. Definicje tych samych pojęć są w różnych aktach różne, nie podjęto nawet wysiłku, żeby zunifikować obszar definicyjny. Dodatkowo polskie definicje nie zgadzają się z unijnymi. Nikt normalny, kto ma stosować prawo, nie jest w stanie się w tym poruszać. Jako prezes PTI chciałbym, żeby nasza branża mogła mieć jasne, jednolite reguły postępowania.

> *Potrzebne są proste regulacje, rozwiązujące rzeczywiste problemy, a nie nadmiarowe, monstrualne dokumenty, które załatwiają kilka istotnych problemów, generując przy okazji wiele kolejnych.*

Na początku października ukazała się 8. wersja nowelizacji ustawy o KSC. Konieczność nowelizacji była pretekstem, przez który w Polsce wciąż nie mamy rozdysponowanego pasma 3,6-3,8 GHz, bardzo ważnego dla świadczenia usług komórkowych w technologii 5G…

Artur Piechocki: Dla mnie procedowanie ustawy o KSC teraz, gdy wiemy, że trzeba będzie wdrażać NIS 2, nie ma już wiele sensu. Trzeba od razu wdrażać rozwiązania przyjęte w NIS 2. Dublowanie się prawa poza kosztami rodzi inne niewiadome. Nie wiemy, jak zachowa się regulator, jak orzekać będą sądy administracyjne. Jak przedsiębiorca ma się w tym odnaleźć?

Jarosław Mojsiejuk: Nie zgadzam się z tezą, że przyjęcie dyrektywy NIS 2 ma oznaczać konieczność zaniechania nowelizacji ustawy o KSC. W nowej dyrektywie jest część bezpieczeństwa pozostawiona krajom członkowskim. Na przykład, my mamy inne interesy niż Niemcy, którzy są żywotnie zainteresowani rozwijaniem swojego eksportu do Chin. Czasami pod szyldem praw podstawowych kryje się brutalna gra interesów krajów członkowskich. Nie sądzę, żeby najlepszym narzędziem kształtowania rynku była „młotkowa regulacja". Nie zapominajmy też przy okazji dyskusji o bezpieczeństwie i nowelizacji ustawy o KSC, że tuż za naszą granicą toczy się wojna i że w pierwszym jej dniu zdezaktywowano system internetowej transmisji satelitarnej teoretycznie amerykańskiej, a praktycznie ukraińskiej firmy Viasat. Wydawałoby się że bezpieczny, bo satelitarny, a nikt do satelitów nie strzelał. To pokazuje skalę zagrożeń!

Wiesław Paluszyński: Ustawę o KSC nowelizujemy już dwa lata! To nieporozumienie: łatwiej byłoby wdrażać NIS 2, gdybyśmy wreszcie dokończyli nowelizację, zwłaszcza że w wielu obszarach znowelizowana ustawa byłaby zgodna z NIS 2. Problem polega na tym, że rząd wstawił do nowelizacji rzeczy, które nigdy nie powinny się tam znaleźć – np. próby utworzenia hurtowego operatora 5G. Jeśli mamy teraz przed sobą 32 miesiące na implementację NIS 2, to nie stać nas na to, żeby funkcjonować bez aukcji na 5G.

Na procesy legislacyjne związane z cyberbezpieczeństwem ogromny wpływ ma gra interesów graczy globalnych, związanych z rosyjskim i chińskim sektorem wojenno-przemysłowym. Jakiś czas temu forsowano argument, że nie wolno do wymagań technicznych dołączać wymagań politycznych, bo to psuje prawo. Niestety – tam, gdzie technologia jest elementem polityki, same argumenty techniczne nie wystarczą.

> *Przy okazji: czy ktoś zrobił analizę algorytmizacji tych aktów, czy one są wdrażalne w sensie algorytmicznym, o co walczymy jako środowisko informatyczne od prawie 30 lat. Ciekawi mnie, czy ktoś by się podjął takiej analizy w przypadku Data Act.*

Arwid Mednis: Koszty Data Act będą duże, w dodatku nie jesteśmy pewni skutków tej regulacji. Pomyślmy, co czeka np. producenta samobieżnego odkurzacza, który będzie musiał dołączyć do tego sprzętu domowego wszystkie wymagane klauzule informacyjne i pomyśleć o sposobie przekazywania danych użytkownikowi, bez względu na to, kto nim jest. Na końcu musimy przekonać tego użytkownika, żeby on te dane gdzieś przekazał, bo RODO nadal obowiązuje.

Jest jeszcze jeden istotny problem: jak te wszystkie akty mają się do siebie?

Arwid Mednis: Popatrzmy na przykład na dostawców komunikatorów, którzy żyli sobie w błogim przekonaniu, że ich obszar działania był niemal nie regulowany. Europejski

Kodeks Łączności Elektronicznej już ich objął, a pod pewnymi warunkami – na podstawie Digital Markets Act – mogą być nawet tzw. gatekeeperami, którzy muszą zwracać uwagę na przekazywane treści.

Obowiązki z różnych regulacji będą się zazębiały i generowały problemy. Jeśli w systemach AI będę wykorzystywał dane osobowe, będę musiał dokonać oceny ryzyka zarówno w odniesieniu do RODO, jak i do AIA. Jeśli będę musiał wykonać oba te ćwiczenia, to oczywiście koszty wzrosną.

Jarosław Mojsiejuk: Możesz w ogóle nie wiedzieć, czy masz do czynienia z danymi osobowymi, bo dane są szyfrowane, tak jest w przypadku niektórych usług chmurowych. Nie bardzo więc nawet wiemy, w jakim reżimie będziemy działali.

Arwid Mednis: Technologie stawiają przed nami problemy nierozwiązywalne – patrz blockchain – i nie jest to wina technologii.

Artur Piechocki: Brakuje interoperacyjności i jednoznacznych wytycznych, jak te akty powinny być stosowane.

Joanna Mazur: To całkiem dobry żart, że nie ma interoperacyjności między aktami prawnymi mającymi (przynajmniej w części) mówić o interoperacyjności. Mam obawy, że proceduralne podejście, o którym była mowa, może także dotknąć aktu o sztucznej inteligencji, co dodatkowo może zmniejszyć jego skuteczność w zestawieniu z trudnością ze sprecyzowaniem znaczenia używanych w nim niektórych pojęć. W spisie systemów zakazanych znalazły się takie zastosowania, które z punktu widzenia ochrony praw podstawowych nigdy nie powinny mieć miejsca, więc nie powinien zaistnieć powód ich zakazywania.

Wiesław Paluszyński: Co do interoperacyjności, to logika prac nad aktami legislacyjnymi jest dla mnie kompletnie nieczytelna. Gdy wchodziło prawo unijne, nie definiowano obszaru regulacji, tylko jego cel. Gdy popatrzymy na te akty prawne, które dzisiaj leżą na stole, konia z rzędem temu, kto powie, jaki jest cel tych regulacji.

Do tego dochodzą tzw. wrzutki. Jest to nasza polska specjalność. Przykładem jest propozycja Ministerstwa Sprawiedliwości uchwalenia ustawy zapobiegającej mowie nienawiści. Projekt przewiduje powstanie Głównego Urzędu Kontroli Publikacji, Prasy i Widowisk pod nową nazwą. Starsi doświadczają pewnego Déjà vu.

Drugi przykład: próba walki ze spoofingiem. Problem powinien być rozwiązany metodą regulacji miękkich między operatorami a regulatorem. U nas usiłuje się to rozwiązać ustawą, która poddałaby cały ruch i cały rynek inwigilacji służb, otwierając zarazem pole do nadużyć. W krajach unijnych dobre praktyki są częścią systemu prawnego.

Jarosław Mojsiejuk: Nadmiar regulacji spowoduje, że gospodarka europejska będzie się rozwijała w wolniejszym tempie niż konkurencja, bo nie da się wyhamować gigantów amerykańskich. Moim zdaniem trzeba bardzo uważać z forsowaniem rozwiązań prawnych. Być może cele są szczytne, ale efekty nadmiaru regulacji dotkną nie tylko polskich przedsiębiorców z wielu sektorów, lecz także całą Europę, powodując opóźnienia gospodarcze Unii i zaburzenie stosunków transatlantyckich. Nie zapominajmy też o tym, że świat się staje coraz bardziej dwubiegunowy.

Arwid Mednis: Wątek nadregulacji, która krępuje inwestycje, jest tematem trudnym. We wszelkich dostępnych raportach Europa pod względem rozwoju technologii AI zajmuje trzecie miejsce, po Stanach Zjednoczonych i Chinach. AIA plus dyrektywa o odpowiedzialności za sztuczną inteligencję, którą się szykuje, mogą spowodować, że wyprzedzą nas także Indie. Z drugiej strony wszyscy jesteśmy świadomi zagrożeń dla praw i wolności obywatelskich. Artur Piechocki wspomniał o RODO. Mark Zuckerberg powiedział swojego czasu, że o prywatności należy zapomnieć, bo to przeżytek. Prawo dotyczące AI może przynieść podobne rezultaty jak RODO, jakiś efekt promieniujący i promujący prawa podstawowe.

Zresztą Amerykanie także zaczęli dostrzegać problem: po przekroczeniu pewnego progu zaczęli zwracać większą uwagę na kwestię prywatności i mamy tam już regulacje naśladujące RODO. AIA zakazuje zautomatyzowanego scoringu społecznego – zrobotyzowanej oceny zachowań ludzi. Być może kosztem inwestycji zachowamy balans z prawami podstawowymi, to by się wszystkim przydało. Może z czasem inni dostosują się do tych wyższych europejskich standardów.

Jarosław Mojsiejuk: Prawom podstawowym najbardziej zagrażają systemy typu *predictive active* – wszyscy pamiętamy „Raport mniejszości", dystopijny film Spielberga sprzed 20 lat, traktujący o tym, że XXI w. można będzie przewidzieć przyszłość, a winnych ukarać, zanim popełnią zbrodnię. Obecnie to nie science fiction – systemy *predictive active* Amerykanie stosowali w świecie realnym i na podstawie uzyskanych z nich danych wysyłali patrole policyjne we wskazane miejsca. Organizacje praw człowieka podnoszą, że systemy AI nie powinny być wykorzystywane do oceny ryzyk migracyjnych, chociaż np. unijny system Schengen stosuje pewne szacowanie takiego ryzyka.

W próbach regulacji sztucznej inteligencji podnosi się kwestie wyjaśnialności. Tymczasem bywa, że twórcy programu tracą nad nim kontrolę, bo program nie tylko się uczy, lecz też sam się modyfikuje.

Jarosław Mojsiejuk: Pojawia się zasadnicze pytanie, czy człowiek jest w stanie nadzorować taki system. Swojego czasu mocno dyskutowaliśmy, jak powinny być wydawane decyzje o dotacjach unijnych dla rolników: czy ma to robić

urzędnik, czy bezstronne algorytmy. Zdecydował właśnie obowiązek zapewnienia możliwości odwołania się od takiej decyzji. W prawie bankowym mamy już takie rozwiązania.

Artur Piechocki: Wolumen, jakość i szybkość przetwarzanych danych wpłyną na rozwój AI. Pytanie, czy AI Act jest wystarczająco uniwersalny. Teraz wydaje się abstrahować od technologii, ale nie wiemy, w którą stronę technologia będzie zmierzać. Im regulacja jest ogólniejsza, tym lepiej, mając na uwadze rozwój np. komputerów kwantowych.

Wiesław Paluszyński: Komputer kwantowy jest jak Yeti: wszyscy o nim mówią i nikt go nie widział. Problem sztucznej inteligencji nie polega na szybkości działania komputera. AI to połączenie uczenia maszynowego z sieciami neuronowymi, ale u jej podstaw jest algorytm wymyślony przez człowieka. Sztuczna inteligencja nie ma inteligencji wrodzonej, tylko wyuczoną, dlatego tak istotna jest jakość danych opracowanych przez człowieka i stosowanych w uczeniu systemu AI. Dane można zmanipulować nie tylko celowo, lecz także przypadkowo. Chińczycy po to kradną dane, żeby uczyć swoje algorytmy w określonym kontekście.

IBM na razie symuluje działanie komputera kwantowego na wielkich komputerach. Na uczelniach na świecie już od 10 lat uczy się programowania kwantowego (w tym numerze „Domeny" kończymy publikację „Przewodnika po nauczaniu informatyki kwantowej" autorstwa prof. Marka Perkowskiego z Portland State University), bo na razie algorytmy AI nie dają się stosować na komputerze kwantowym. Komputer kwantowy potrafi rozwiązywać problemy analogowe bez przechodzenia przez cyfryzację, więc znajdzie zastosowanie np. w medycynie i chemii – wszędzie tam, gdzie mamy do czynienia z bardzo złożonymi związkami chemicznymi. Cyfryzacja jest stratna i ta stratność powoduje, że osiągane wyniki są obarczone błędem. Nie do końca wiadomo, w którym rzędzie wielkości danych następuje istotne zniekształcenie problemu. Komputera kwantowego nikt jeszcze nie zbudował, bo nie udało się uzyskać stabilności kubita. Nie wiadomo też, czy komputer kwantowy będzie działał tak, jak to dzisiaj wymyśliliśmy. Sztuczna inteligencja rozwija się równolegle. Przy okazji zapraszam na konferencję PTI poświęconą AI z okazji Światowego Dnia Społeczeństwa Informacyjnego w maju przyszłego roku.

Arwid Mednis: Prawo nie jest panaceum na wszystko, nie może zastąpić zdrowego rozsądku – niech to będzie podsumowaniem tej dyskusji.

Tomasz Kulisiewicz

Omawiane akty prawne

- AIA (Artificial Intelligence Act) – Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii (https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52021PC0206)
- DGA (Data Governance Act) – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 w sprawie europejskiego zarządzania danymi i zmieniające rozporządzenie (UE) 2018/1724 (Akt w sprawie zarządzania danymi) (http://data.europa.eu/eli/reg/2022/868/oj)
- DMA (Digital Markets Act) – Rozporządzenie Parlamentu Europejskiego i Rady w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym (Akt o rynkach cyfrowych) (https://eur-lex.europa.eu/eli/reg/2022/1925/oj)
- DSA (Digital Services Act) – Rozporządzenie Parlamentu Europejskiego i Rady w sprawie jednolitego rynku usług cyfrowych (Akt o usługach cyfrowych) i zmieniające dyrektywę 2000/31/WE (https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52020PC0825)
- DORA (Digital Operational Resilience Act) – Rozporządzenie Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 oraz (UE) nr 909/2014 (https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52020PC0595)
- NIS 2 – Dyrektywa Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylająca dyrektywę (UE) 2016/1148 (Dyrektywę NIS w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii) (https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=COM:2020:823:FIN)