Zastosowanie SI będzie bardzo szerokie, a to co nas ogranicza, to środki finansowe i wyobraźnia

Posted on 2024-10-31

Z Tomaszem Izydorczykiem, członkiem Społecznego Zespołu Ekspertów przy PUODO rozmawiał Karol Witowski, p.o. Rzecznika Prasowego UODO.

9 października br. w Chorzowie odbyło się seminarium ZUS i UODO „Czas wyzwań – projektowanie systemów AI oraz wdrożenie NIS2 w organizacji". Poprowadził Pan wykład „Analiza ryzyka przy projektowaniu systemów AI". Powiedział Pan na wstępie, że „technologia nie jest niebezpieczna, tylko ludzie, którzy jej używają". Boimy się błędów ludzkich przy wdrażaniu AI, a nie sztucznej inteligencji samej w sobie?

Do takiego wniosku doszedłem podczas jednego z wspólnie organizowanych przez UODO i Społeczny Zespół Ekspertów seminariów. Rozmawiając o ocenie ryzyka, zawsze musimy osadzić te ryzyka w jakimś kontekście, w stanie faktycznym. Wtedy zastanawiamy się jak używana w danym procesie technologia może wpływać na nas, na ludzi, czyli podmiot

danych. Aby na to pytanie udzielić odpowiedzi, trzeba najpierw zrozumieć, w jaki sposób dochodzi do przetwarzania danych osobowych z pomocą tej technologii.

Gdy już wiemy, jak wygląda proces przetwarzania, to dochodzimy do naturalnego wniosku, że to nie technologia decyduje o tym, co zrobi z naszymi danymi czy naszą prywatnością. To właśnie człowiek, który korzysta z tej technologii może wpływać na poziom ochrony naszych praw. Spójrzmy na to od strony praktycznej: otrzymujemy spam za pomocą systemu pocztowego nie dlatego, że to ten system podjął taką decyzję. To człowiek ustawił system pocztowy, aby rozsyłał duże ilości wiadomości, które zaśmiecają nasze skrzynki.

Podobnie będzie w przypadku zastosowania sztucznej inteligencji. Ten sam system oparty o sztuczną inteligencję, bazujący na tysiącach doświadczeń nauczycieli i procesach edukacyjnych różnych poziomów edukacyjnych może z jednej strony wspierać system edukacji dostosowany do indywidualnych warunków i potrzeb młodego człowieka, a z drugiej strony może zostać wykorzystany do stygmatyzowania, oceniania lub dyskryminowania określonych grup uczniów, z uwagi na pewne cechy indywidualne. Ten sam system zarządzający bezpieczeństwem migracji czy kontroli granic może posłużyć do zapewnienia bezpieczeństwa granic Unii Europejskiej, ale równocześnie może być wykorzystany do dyskryminacji na tle rasowym lub etnicznym. Rolą naszą – osób biorących udział w ocenie ryzyka takich systemów jest dogłębne poznanie możliwości danego systemu sztucznej inteligencji i przewidywanie, jak może on być wykorzystany (przypadkowo lub intencjonalnie) z negatywnym skutkiem dla praw lub wolności ludzi.

Mówi się, że Europa wpadła w pułapkę przeregulowania sztucznej inteligencji przez co jest w tyle za Ameryką, jeśli chodzi o rozwój AI. Wymagania, jakie sobie stawia UE stale rosną, w związku z tym wciąż pracuje nad nowymi rozwiązaniami prawnymi – to sugeruje, że zawsze będziemy w tyle za Stanami. Tymczasem wspomniał Pan, że USA również intensywnie zajmują się projektami aktów prawnych, które mają dotyczyć sztucznej inteligencji.

30 października 2023 r. Prezydent Stanów Zjednoczonych Ameryki wydał Rozporządzenie

Zastosowanie SI będzie bardzo szerokie, a to co nas ogranicza, to środki finansowe i wyobraźnia

wykonawcze w sprawie bezpiecznego, pewnego i godnego zaufania rozwoju i użytkowania sztucznej inteligencji[1]. W rozporządzeniu Prezydent Biden podkreśla to, co wcześniej już zostało wspomniane: „Ostatecznie AI odzwierciedla zasady ludzi, którzy ją budują, ludzi, którzy jej używają, i danych, na których jest zbudowana." Na dedykowanej stronie rządu USA ai.gov możemy monitorować postępy w realizacji rozporządzenia prezydenta.

Z kolei organizacja IAPP[2] także monitoruje globalne polityki prawa w zakresie AI na całym świecie. To są już setki aktów lub projektów aktów prawnych, działań o charakterze legislacyjnym lub tzw. „miękkich wytycznych". Uniwersytet Stanforda odnotował ogromny wzrost liczby krajów, których prawa zawierają termin „AI" – z 25 krajów w 2022 r. do 127 w 2023 r.[3] Europejczycy uchwalili AI Act (najprawdopodobniej pierwsi), ale czeka nas jeszcze długa droga uzupełnienia regulacji o krajowe przepisy i uruchomienie operacyjne urzędów ds. sztucznej inteligencji w każdym kraju członkowskim.

Z kolei MIT Technology Review[4] podaje, że „Ponad 120 projektów ustaw związanych z regulacją sztucznej inteligencji krąży obecnie w Kongresie USA". Jak widać cały świat już to robi lub zamierza „regulować" sztuczną inteligencję, a właściwie jej tworzenie i użytkowanie. I właśnie, żeby nie pozostawać za Stanami Zjednoczonymi, nasza rola jest taka, aby dokładnie poznać, jak działa sztuczna inteligencja, bardzo dobrze znać przepisy i umieć je interpretować. Można by zapytać: dlaczego? Jeśli okaże się, że SI wymyka się nam spod kontroli albo nadmierna regulacja SI blokuje konkurencyjność czy efektywność europejskiego wykorzystania sztucznej inteligencji, to będzie nam – praktykom, ekspertom bardzo łatwo pokazać prawodawcom czy decydentom politycznym, jakie zmiany w prawie trzeba zrobić, aby nie pozostawać w tyle. Jedną z dróg do osiągnięcia tego celu jest właśnie edukacja poprzez debaty, konferencje, seminaria, artykuły i każda inna forma uświadamiana – w tym właśnie także Biuletyn UODO.

Zwrócił Pan uwagę na badania prof. Kosińskiego, który publikował swoje prace nt. wyciągania wniosków statystycznych na podstawie dużych baz danych. Wnioski z tych badań

Zastosowanie SI będzie bardzo szerokie, a to co nas ogranicza, to środki finansowe i wyobraźnia

dają dużo do myślenia. Na pewno, żeby przesadnie nie dzielić się informacjami o sobie w mediach społecznościowych.

Z jednej strony jesteśmy „ekshibicjonistami" i lubimy publikować w sieci nasze zdjęcia, komentarze czy inne treści pochodzące od nas, z drugiej strony chcemy, aby „pewne" informacje nie ujrzały światła dziennego lub pozostały w wąskim gronie najbliższych osób. Niestety mam przykrą wiadomość dla nas wszystkich. To, co wydaje nam się, że jest głęboko ukryte, można wywnioskować z innych informacji, z pozoru nieistotnych, oczywistych czy nie naruszających naszą prywatność nadmiernie. Badania prof. Kosińskiego, ale i wiele innych badań naukowców dowodzą, że przy dużych zbiorach danych/ informacji oraz zestawieniu różnych zbiorów danych nieosobowych z danymi osobowymi, można wywnioskować inne dane, w tym dane szczególnej kategorii. Zrozumienie, że na podstawie danych zwykłych można wyciągnąć wnioski dotyczące tzw. danych wrażliwych przebija się także do świadomości sądów (np. orzeczenia TSUE sygn. C-184/20[5] czy C-252/21[6]). Jeśli tylko do świadomości organów ochrony danych i sądów, a tym samym społeczeństwa dotrze, jaki potencjał drzemie w danych i co na ich podstawie korporacje są w stanie wywnioskować, (co widać na bazie badań naukowych opartych o statystyczne metody ilościowe), może zaczniemy bardziej dbać o to, co udostępniamy w internecie i jakie ślady cyfrowe po sobie zostawiamy.

RODO jest podstawową regulacją, na której opierają się pozostałe przepisy: AI Act, DSA, Dora, NIS2, KSC. Jaka jest między nimi relacja i kogo dotyczy AI Act?

Kiedyś w rozmowie z przedstawicielką UODO usłyszałem bardzo ciekawą metaforę. Otóż RODO miało być w tej metaforze dywanem – czyli taką podstawą dla wszystkiego, co na nim stoi. Inne regulacje prawne miały być meblami, które znajdują na tym dywanie. Te meble to właśnie AI Act, DSA, DGA, DA, Dora czy NIS2 i wiele innych regulacji. Wszystko, co łączy te akty prawne to dane. Zarówno dane osobowe, jak i nieosobowe. W dzisiejszym świecie, mocno technologicznym, trudno jest mówić o danych bez danych osobowych. Nawet smart

Zastosowanie SI będzie bardzo szerokie, a to co nas ogranicza, to środki finansowe i wyobraźnia

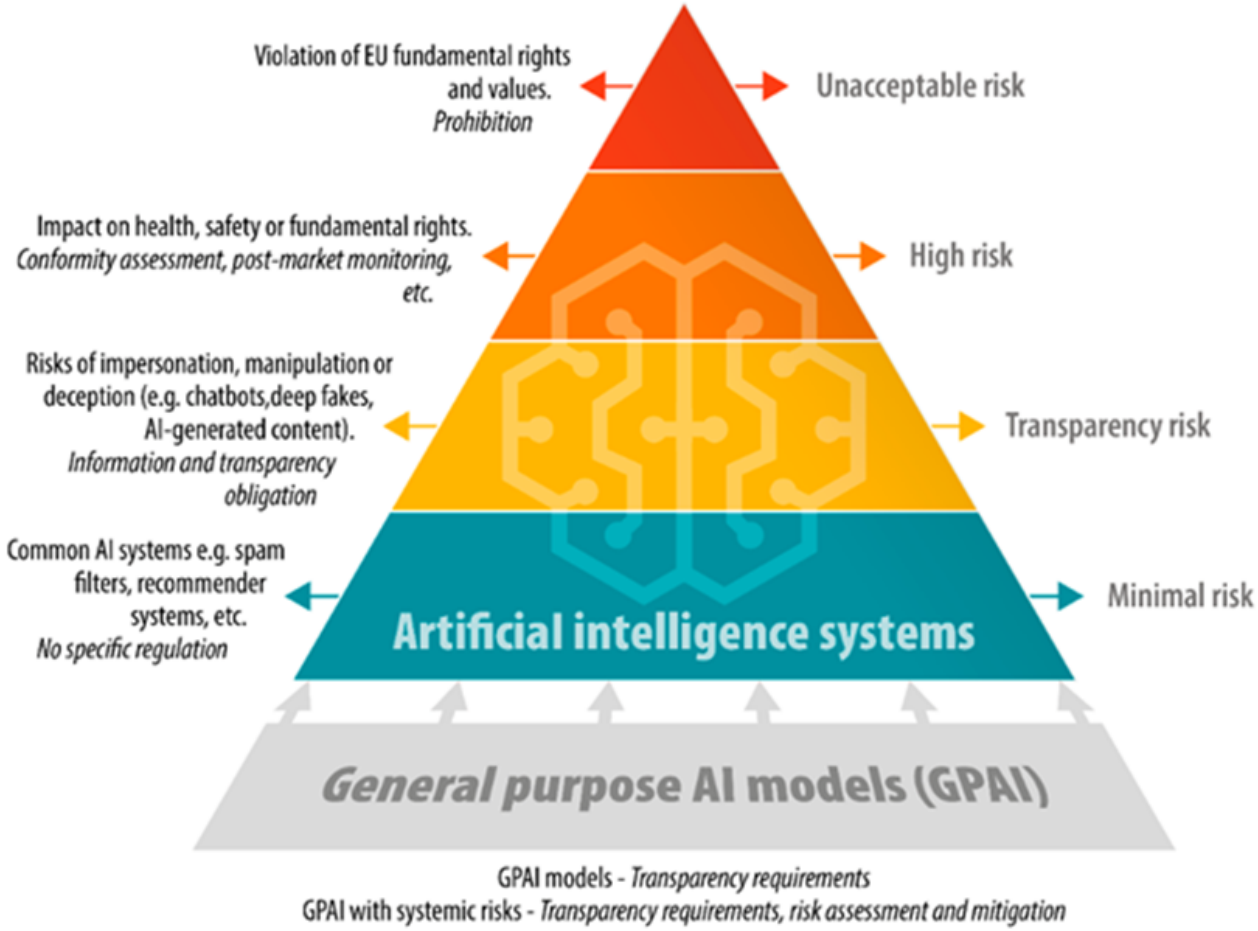
TV, lodówka podłączona do internetu, czy samochód użytkowane są przez ludzi. Dane, które są generowane przez te urządzenia pochodzą przecież od ludzi i wynikają ze sposobu użytkowania tych urządzeń.

Jeśli chodzi o relacje pomiędzy AI Act a innymi regulacjami, to możemy zobrazować sobie, że za pomocą sztucznej inteligencji możemy realizować obowiązki wynikające ze wszystkich innych aktów prawnych. Możemy wyobrazić sobie, że sztuczna inteligencja będzie realizowała wnioski podmiotów danych o dostęp do danych czy uzyskania kopii danych na podstawie RODO. Podobnie można zaimplementować rozwiązania oparte o sztuczną inteligencję, które będą rozpatrywały wnioski o usunięcie treści nielegalnych na platformach internetowych w oparciu o przepisy DSA. Automatyczne decyzje dotyczące cyberzagrożeń mogą być rozpoznawane, analizowane przez sztuczną inteligencję, a to będzie realizacja wymogów DORA, NIS2. Jak widać wszystkie te regulacje, które są realizacją strategii Unii Europejskiej polegającej na gospodarce opartej o dane, gospodarce opartej o usługi cyfrowe, przeplatają się między sobą i zazębiają.

Jak unijne rozporządzenie AI Act klasyfikuje systemy sztucznej inteligencji? Jakie są poziomy ryzyka? Jak zarządzać ryzykiem zgodnie z AI Act? Inna jest perspektywa ryzyka z punktu widzenia RODO, a inna z AI Act.

Na bazie lektury Rozporządzenia UE nr 2024/1689 w sprawie sztucznej inteligencji można system SI z uwagi na ryzyko podzielić na cztery klasy systemu o: nieakceptowalnym ryzyku, wysokim ryzyku, transparentnym ryzyku i minimalnym ryzyku.

Zastosowanie SI będzie bardzo szerokie, a to co nas ogranicza, to środki finansowe i wyobraźnia



Źródło: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf

Zarządzanie ryzykiem w systemach sztucznej inteligencji jest o wiele bardziej sformalizowane i poukładane niż wynikałoby to z przepisów RODO. Organizacje, które będą podlegały pod AI Act będą zmuszone do wprowadzenia systemowego zarządzania ryzykiem, o czym mowa w art. 8 tego rozporządzenia. Systemowość oznacza ciągły, iteracyjny proces, planowany i realizowany przez cały cykl życia systemu AI wymagający regularnego systematycznego przeglądu i aktualizacji. Proces ten obejmuje następujące cztery główne etapy:

Zastosowanie SI będzie bardzo szerokie, a to co nas ogranicza, to środki finansowe i wyobraźnia

1. identyfikację i analizę znanego i dającego się racjonalnie przewidzieć ryzyka,
2. oszacowanie i ocenę ryzyka, jakie może wystąpić podczas wykorzystywania systemu AI,
3. ocenę innego mogącego wystąpić ryzyka na podstawie analizy danych zebranych z systemu monitorowania,
4. przyjęcie odpowiednich i ukierunkowanych środków zarządzania ryzykiem.
   Dla nas, praktyków ochrony danych, nie jest to nic zaskakującego czy nowatorskiego. Jeśli mówimy o prawdziwym systemie ochrony dany osobowych zgodnym z RODO, wydaje się że systemowe podejście do zarządzania ryzykiem jest kluczem do zapewnienia zgodności, nawet jeśli ta „systemowość" nie jest wymuszana regulacją. W przypadku systemów sztucznej inteligencji, w szczególności wysokiego ryzyka, ta systemowość będzie wymuszona przez przepisy.

   Perspektywa ryzyka zarówno z RODO, jak i AI Act jest bardzo zbliżona do siebie. Zarówno w przepisach o ochronie danych, jak i w przepisach o sztucznie inteligencji w centrum zainteresowania jest człowiek i jego prawa. W przypadku RODO mówimy o ochronie praw każdej pojedynczej jednostki, natomiast w przypadku systemów sztucznej inteligencji będziemy minimalizować skutki, jakie mogą mieć wpływ nie tylko na ludzi, ale i poziom ochrony zdrowia, bezpieczeństwa, praworządności i ochrony środowiska, co wynika z art. 1 ust. 1 AIA.

   To, że rozporządzenie ws. sztucznej inteligencji wprowadza regulacje dotyczące oceny ryzyka, nie oznacza że jej przeprowadzenie zwalniać będzie administratora z ogólnej oceny ryzyka naruszenia praw i wolności wynikających z RODO. Dlatego nie zapominajmy, że ten sam proces / system, jeśli będzie oparty o sztuczną inteligencję i jednocześnie przetwarzał dane osobowe, będziemy musieli dokonać oceny z dwóch punktów widzenia (dwóch regulacji).

   Wykorzystanie sztucznej inteligencji do analizy wniosków o wypłatę świadczeń w ZUS-ie to możliwa niedługa przyszłość? Jakie jeszcze zadania będziemy mogli powierzyć sztucznej

Zastosowanie SI będzie bardzo szerokie, a to co nas ogranicza, to środki finansowe i wyobraźnia

inteligencji?

Wierzę, że jest to możliwe. Już teraz wiele typów wniosków o wypłatę świadczeń zostało w wysokim stopniu zautomatyzowanych. Do takiego modelu dąży nie tylko ZUS, ale i cały sektor ubezpieczeń, mając na celu obniżanie kosztów procesu, przyspieszanie jego realizacji i wykrywania nadużyć.

Wydaje się, że zadania, jakie będziemy mogli powierzyć sztucznej inteligencji nie mają końca. Zaczęliśmy od prostych rzeczy jak gry w szachy, analizowanie obrazów, wykrywanie chorób na zdjęciach rentgenowskich. Aktualnie za pomocą AI generujemy treści (teksty), obrazy, nawet muzykę. Już dziś możemy korzystać z prostych rozwiązań jak podpowiedzi w treści e-maili, które na co dzień piszemy w systemach pocztowych, korektę tekstu, który wpisujemy za pomocą klawiatury, zamianę treści rozmów nagranych za pomocą plików audio na tekst pisany (tzw. transkrypcji), a nawet tłumaczenia symultaniczne. Napominajmy o tym, że SI może być wykorzystywana do generowania fajowych zdjęć, treści czy postów w mediach społecznościowych. Z pewnością zastosowanie sztucznej inteligencji będzie bardzo szerokie, a to co nas ogranicza, to środki finansowe i wyobraźnia. Łatwo nam wyobrazić sobie zastosowanie AI w komercji. Z jakich zastosowań sztucznej inteligencji mógłby teoretycznie skorzystać ZUS czy inne instytucje użyteczności publicznej? Jakie korzyści mogą płynąć z tej technologii dla obywatela?

Myślę, że duże podmioty publiczne takie jak właśnie ZUS mogą skorzystać z zastosowania sztucznej inteligencji wszędzie tam, gdzie posiadają duże ilości danych, a obsługiwane procesy są w miarę powtarzalne, jednakże wymagają analizy informacji wpływających do urzędu. Jeżeli do danego podmiotu wpływają masowo podobne wnioski i podmiot ten posiada wiedzę na temat tego, jakie one były do tej pory, to sztuczna inteligencja mogłaby takie wnioski analizować i rozpatrywać. W ten sposób najbardziej żmudną pracę, którą muszą wykonywać ludzie można zastąpić algorytmami SI. Oczywiście wymagałoby to wprowadzenia systemu kontroli jakości

Zastosowanie SI będzie bardzo szerokie, a to co nas ogranicza, to środki finansowe i wyobraźnia

i prawidłowości rozpatrywanych spraw.

Wyobrażam sobie, że równolegle do systemu opartego o sztuczną inteligencję pracowałby merytoryczny zespół pracowników kontrolujący efekty pracy SI oraz rozpatrujący odwołania lub sprzeciwy co do wyłącznie zautomatyzowanego podejmowania decyzji. Na końcu takiej usługi publicznej obywatel o wiele szybciej załatwia tę sprawę, z uwagi na to, że systemy AI mogą pracować 24 h na dobę. Zaoszczędzony w ten sposób czas można poświęcić na bardziej dokładne analizowanie tych spraw, które będą kierowane do rozpatrywania przez zespoły ludzi. Pracownicy nie będą przeładowani ilością spraw i będą mieli więcej czasu na merytoryczne rozpoznanie danej sprawy. I może dzięki tym sposobom uda nam się w przyszłości pracować cztery, a nie pięć dni w tygodniu.

Na jakie kwestie szczególnie muszą uważać instytucje przy wdrażaniu rozwiązań opartych na AI?

Moim zdaniem najważniejszą kwestią, na którą muszą zwrócić uwagę instytucje przy wdrażaniu rozwiązań opartych o sztuczną inteligencję jest zagadnienie danych treningowych. Mamy takie polskie powiedzenie „Czego Jaś się nie nauczy, tego Jan nie będzie umiał”. To powiedzenie idealnie pasuje do ryzyka, jakie mamy w związku z rozwojem sztucznej inteligencji. W zależności od tego, jakie dane wejściowe zostaną wykorzystane do nauki sztucznej inteligencji, możemy otrzymać w rezultacie lepsze lub gorsze wyniki działania takiego systemu. Oczywiście jest to istotne pod warunkiem, że osoby, które będą trenowały sztuczną inteligencję, a następnie ją wykorzystywały mają dobre intencje i będą to robiły w celu poprawy jakości życia ludzi, a nie przeciwko nam.

W czasie konferencji „Ochrona danych w robotyce medycznej w dobie AI ACT i EHDS” prowadził Pan debatę o robotach medycznych w kontekście cyberzagrożeń. Jakie są najważniejsze wnioski z tej dyskusji?

Z mojego punktu widzenia najważniejsze wnioski, jakie płyną z tej konferencji są dwa.

Zastosowanie SI będzie bardzo szerokie, a to co nas ogranicza, to środki finansowe i wyobraźnia

Pierwszy to taki, że niezależnie od tego, ile milionów złotych wydamy na najnowocześniejsze i najlepsze roboty ratujące zdrowie i życie ludzi, mogą one nie być zdolne do leczenia, jeśli nie zadbamy o cały ekosystem cyberbezpieczeństwa i cyberhigieny w zakresie całego podmiotu medycznego.

Drugi wniosek nasuwa się taki, że w kontekście ostatnich wydarzeń na Bliskim Wschodzie (wybuchające pagery, telefony i inne urządzenia ICT), musimy na serio potraktować wdrożenie przepisów NIS2 / KSC i zapewnić cyberbezpieczeństwo w całym łańcuchu dostaw. Jeśli tak małe i tanie urządzenia mogą wyrządzać ludziom taką krzywdę, to wyobraźmy sobie co może się zdarzyć, jeśli terroryści czy cyberprzestępcy dostaną się do systemu zarządzającego robotem medycznym czy innymi urządzeniami medycznymi?

To już nie chodzi tylko o życie czy zdrowie jednego człowieka, który będzie operowany takim robotem medycznym. Ale chodzi o tysiące urządzeń diagnostycznych, monitorujących czy dawkujących leki. Dla terrorystów czy przestępców nie ma żadnej granicy, której by nie przekroczyli, a rozwój nowoczesnej medycyny jest silnie skorelowany i zależy od urządzeń przetwarzających dane
i podłączanych do internetu.

Branża medyczna należy do jednej z ulubionych ofiar hakerów. Czy da się w ogóle w pełni zapewnić bezpieczeństwo danych medycznych? Z optymistycznych konkluzji w trakcie spotkania paneliści poruszyli temat certyfikacji robotów medycznych, które dają pewne gwarancje ochrony danych.

Zapewnienie bezpieczeństwa danych to nie jest stan zero-jedynkowy. To proces nieustannej analizy zagrożeń, oceny ryzyka, wprowadzania środków bezpieczeństwa, monitorowania i wdrażania działań korygujących i zapobiegawczych. Podobnie jak w medycynie coraz częściej podchodzi się do pacjenta holistycznie, tak samo my w ochronie i bezpieczeństwie danych musimy podchodzić całościowo i kompleksowo. To może oznaczać, że przy obsłudze takiego skomplikowanego i bardzo nowoczesnego robota medycznego musimy zapewnić nie

Zastosowanie SI będzie bardzo szerokie, a to co nas ogranicza, to środki finansowe i wyobraźnia

tylko kompetentnych i wyszkolonych lekarzy, inżynierów utrzymujących i rozwijających takiego robota, ale także naszych „zakładowych informatyków", którzy zagwarantują, że ten robot będzie miał możliwość egzystencji w ekosystemie podmiotu medycznego.

Nie zapominajmy w tym holistycznym podejściu o inspektorach ochrony danych, którzy muszą wykazać się wyjątkowo interdyscyplinarną wiedzą na temat ochrony danych w związku z całym ekosystemem szpitala, nie tylko ich pracownikami, systemami informatycznymi, ale także urządzeniami, które przetwarzają dane pacjentów. Wyroby czy roboty medyczne, systemy zarządzania bezpieczeństwem informacji należy certyfikować i regularnie poddawać audytom zewnętrznym.

Jestem ciekawy, jak Pan odpowie na pytanie, które sam Pan zadał uczestnikom swojego panelu: Poufność, dostępność, integralność danych. Który z tych trzech elementów jest najbardziej istotny dla człowieka, który korzysta z usług sektora medycznego?

Biorąc pod uwagę nasz kontekst kulturowy, my Polacy często rozmawiamy z wieloma osobami na temat naszego stanu zdrowia. Dlatego nie uważam, aby poufność była najistotniejsza, w sytuacji kiedy integralność danych może oddziaływać bezpośrednio na zdrowie lub życie pacjenta w podmiocie medycznym. Oczywiście nie mówię o sytuacji, kiedy wyciekają dane dotyczące zdrowia osób eksponowanych np. politycznie lub biznesowo. Myślę, że przeciętny Kowalski nie będzie tak bardzo zirytowany czy zestresowany w momencie, kiedy dowie się, że wyciekły jego wyniki badań diagnostycznych. Natomiast jeśli ten sam Kowalski zobaczy nie swoje wyniki badań, które zostały przypisane jemu (naruszenie integralności) poziom stresu takiego Kowalskiego może doprowadzić do opłakanych skutków.

Podobnie będzie w przypadku leczenia wady wzroku. To, że noszę okulary widać i raczej nie mam z tym problemu, aby ktoś dowiedział się o tym, że leczę się u okulisty. Jednakże bardzo chciałbym wierzyć w to, że program, który został przygotowany do laserowej korekty wzroku nie miał żadnej ingerencji z zewnątrz i podane parametry działania tego urządzenia nie

zostały zmienione i są dostosowane do mojej wady wzroku. Biorąc pod uwagę ten właśnie kontekst uważam, że w przypadku podmiotów medycznych integralność danych, a także ciągłość dostępu do danych oraz ciągłość realizacji usług przez systemy informatyczne szpitala są kluczowe z punktu widzenia zdrowia i życia podmiotów danych, czyli pacjentów podmiotów leczniczych.

W Społecznym Zespole Ekspertów przy PUODO podnosi Pan świadomość społeczną na temat ochrony danych osobowych. To ważna rola. Dodam, że jest Pan bardzo aktywnym członkiem zespołu. Przypomnijmy, że wziął Pan również udział w innym seminarium UODO i ZUS „Ochrona danych jako element odporności społeczeństwa i państwa", w bardzo dla nas ważnym spotkaniu ekspertów dotyczącym praktycznych problemów w stosowaniu przepisów ustawy o ochronie sygnalistów z perspektywy RODO, a także w konferencji „Świat robotyki medycznej a ochrona danych osobowych". Jak ocenia Pan działanie zespołu i efekty jego pracy?

Trudno jest mi oceniać efekty pracy zespołu, gdy jestem jego częścią. Jeszcze trudniej oceniać mi efekty, ponieważ będą one o wiele bardziej widoczne najprawdopodobniej w kolejnych latach naszej działalności. To, co mogę powiedzieć to, że jestem dumy z zaangażowania członków naszego zespołu, bo poświęcają sporo czasu na to, abyśmy mogli zrealizować choć część naszych pomysłów. Jestem pod wrażeniem ilości inicjatyw, które uruchomiliśmy lub które jeszcze czekają na otwarcie we współpracy z Urzędem Ochrony Danych Osobowych. Bardzo pozytywnie oceniam otwartość naszych ekspertów na wszelkie prośby, wnioski czy sugestie zarówno ze strony kierownictwa UODO, jak i pracowników urzędu.

Nie jest żadną tajemnicą, że wielu z nas często krytykowało działania UODO, a między nami nie zawsze istnieje zgodność i jednolitość poglądów. To, co jest jednak budujące, to że potrafimy wspólnie rozmawiać, spierać się na argumenty w przyjaznej atmosferze, a przede wszystkim przyjmować i analizować poglądy organu ochrony danych. Dla mnie osobiście

Zastosowanie SI będzie bardzo szerokie, a to co nas ogranicza, to środki finansowe i wyobraźnia

pozytywnym efektem, który już ma miejsce, a który może nie łatwo dostrzec, jest wzajemna wymiana poglądów pomiędzy urzędnikami a nami, reprezentującymi świat nauki, doktryny i rynku.

Osobiście otrzymuję też dużo pozytywnych sygnałów od środowisk inspektorów ochrony danych na temat wspólnie organizowanych konferencji i seminariów, które mają przede wszystkim cele edukacyjne, co uważam za najważniejsze z punktu widzenia systemów ochrony danych osobowych.

Jako członek Społecznego Zespołu Ekspertów przy PUODO aktywnie uczestniczy Pan w pracach nad poradnikiem ds. zgłaszania naruszeń. Jak się pracuje w tak dużym i zróżnicowanym zespole?

Praca w dużym zespole zawsze jest wyzwaniem. Przede wszystkim w wymiarze logistyczno-czasowym. Ilość materiału, która jest do przeczytania lub do skomentowania nie ma końca. Mam ogromną potrzebę rozmowy z każdym i konfrontowania poglądów, szczególnie z tymi osobami, z których podglądami na dany temat się nie zgadzam. Tylko w ten sposób mogę przekonać się, czy moje myślenie jest prawidłowe czy może jest obarczone jakimś błędem.

Ale najważniejsze jest to, że taka pozytywna konformacja poglądów i spór na argumenty jest najlepszą formą tworzenia wartościowych treści, które powinny się znaleźć w poradnikach, które przecież będą czytane przez setki, jak nie tysiące osób. Natomiast zróżnicowanie zespołu nie odbieram jako coś negatywnego czy utrudniającego, wręcz przeciwnie, jako coś co może poprawić jakość naszej pracy. Nie od dziś wiadomo, że różnorodność środowiska /otoczenia ma wiele zalet i pozytywny wpływ na rozwój ludzi. Dlatego jestem przekonany, że uda nam się wspólnymi siłami oddać w ręce nie tylko inspektorów, wartościowy materiał do pracy.

Poza pełnieniem funkcji członka SZE, prowadzi Pan bloga, kanał na YouTube, szkolenia, konsultacje, jest Pan inspektorem ochrony danych, wykładowcą, audytorem, autorem

licznych publikacji, członkiem zarządu w NewTechLaw.eu sp. z o.o. Pomimo tylu obowiązków, podchodzi Pan do kolejnych wyzwań pełen niesłabnącej energii. Czy kluczem do tego jest pasja, której z pewnością Panu nie brakuje?

Pamiętam pierwszy dzień – 4 czerwca, gdy otrzymaliśmy powołanie do Społecznego Zespołu Ekspertów od pana prezesa Mirosława Wróblewskiego. Po zakończeniu całego dnia, jechaliśmy windą wspólnie z prawnikami UODO i padło stwierdzenie, że spotkanie naszego zespołu odbyło się w bardzo miłej i sympatycznej atmosferze. Odpowiedziałem wtedy, że my wszyscy mniej lub bardziej znamy się, często spieramy się merytorycznie i nie zawsze się ze sobą zgadzamy, ale za to się lubimy. A to, co nas wszystkich łączy, to właśnie pasja do ochrony danych osobowych i my naprawdę lubimy to, co robimy. Dla mnie ochrona danych osobowych to wielowymiarowa i interdyscyplinarna dziedzina (prawa, informatyki, nowych technologii i zarządzania), w której nie da się nudzić, zawsze jest coś do zrobienia, ale można też poznać bardzo ciekawych i wyjątkowo sympatycznych ludzi. Peter F. Drucker twierdził, że najmniej wydajna jest praca niewolnika, a najbardziej wydajna jest praca ochotnika. W takiej dziedzinie jak ochrona danych osobowych, z takimi ludźmi, praca i cała moja aktywność jest dla mnie przyjemnością, a nie obowiązkiem.

Dziękuję za rozmowę.

1. Źródło: https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/ oraz https://www.govinfo.gov/content/pkg/FR-2023-11-01/pdf/2023-24283.pdf ↩
2. Global AI Law and Policy Tracker https://iapp.org/media/pdf/resource_center/global_ai_legislation_tracker.pdf ↩
3. Źródło: https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/757605/EPRS_ATA(2024)757605_EN.pdf ↩

Zastosowanie SI będzie bardzo szerokie, a to co nas ogranicza, to środki finansowe i wyobraźnia

4. Źródło: https://www.technologyreview.com/2024/09/18/1104135/the-download-congresss-ai-bills-and-snaps-new-ar-spectacles/ ↩
5. Źródło: C-184/20 OT przeciwko Vyriausioji tarnybinės etikos komisja ↩
6. C-252/21 Meta Platforms Inc., dawniej Facebook Inc., Meta Platforms Ireland Limited, dawniej Facebook Ireland Ltd., Facebook Deutschland GmbH przeciwko przeciwko VerbraucherzentraleBundesverbandeV ↩