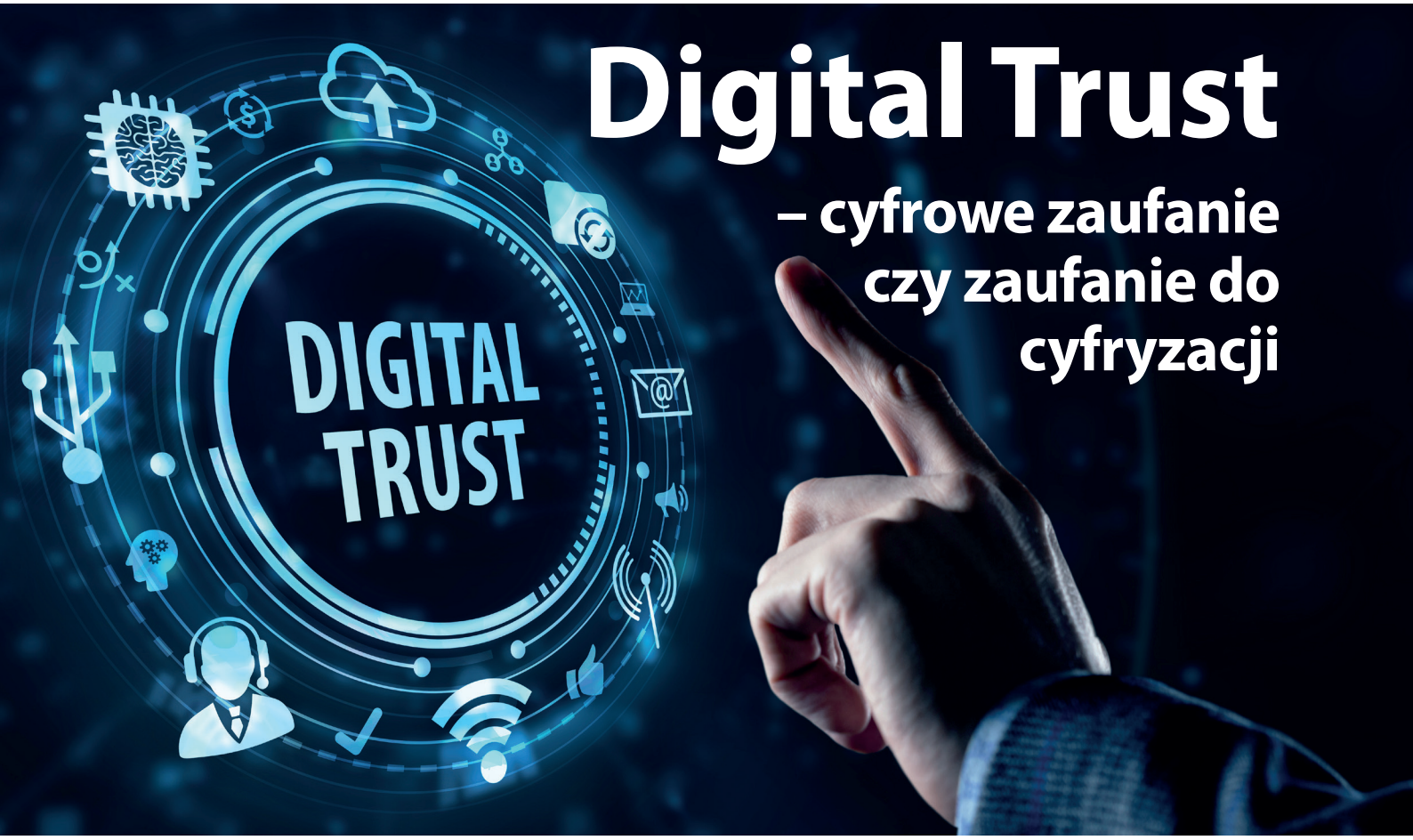


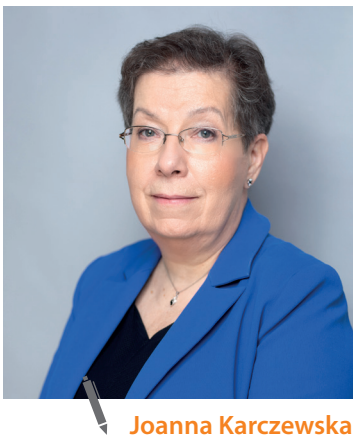
Digital Trust – cyfrowe zaufanie czy zaufanie do cyfryzacji

Trust to zaufanie, ufność, wiara (www.ling.pl). Zaś zaufanie to przekonanie, że jakiejś osobie lub instytucji można ufać i że czyjeś słowa, informacje itp. są prawdziwe (https://sjp.pwn.pl). Skoro cyfryzacja jest coraz powszechniejsza, to zaufanie odnosi się także do systemów informatycznych. Chcemy wierzyć, że systemy nas nie oszukają i nie zrobią nam niczego złego.

Niestety, możemy się rozczarować i to boleśnie.

(Nie)Wiara w banki

Dotkliwe dla mnie i mojej rodziny okazało się zastosowanie przez dwa banki – niezależnie od siebie – algorytmów cyfrowych dla zapewnienia zgodności z jednym z przepisów nałożonych na instytucje finansowe. Banki uznały, że sprawa jest prosta, wręcz banalna i zrzuciły ją na swoje sztuczne inteligencje oczekując, że będziemy pokornie czapkować maszynie. Przyjęty przez oba banki sposób postępowania zdecydowanie doprowadził do utraty naszego zaufania i naruszenia naszej prywatności (nie podam nazw instytucji, bo sprawy się toczą).



Joanna Karczewska
One of Europe's Top Cyber Women

Zastosowałam metodykę PIA francuskiego organu ochrony danych osobowych CNIL do oceny sytuacji, w jakiej się znaleźliśmy. W skali (od 1 – bez znaczenia do 4 – maksymalne znaczenie) istotności skutków bezpośrednich i pośrednich działania algorytmów bankowych znaleźliśmy się na poziomie 3 – poważnym, gdyż doznajemy znaczących niedogodności, z którymi sobie jednakże radzimy sobie z poważnymi trudnościami.

(Nie)Wiara w rejestry publiczne

Z banku można zrezygnować. Niestety, z rejestru publicznego obywatel nie może się wypisać. Zatem ich wiarygodność jest kluczowa. Teoretycznie w e-rejestrach prowadzonych przez państwo są same prawdziwe dane. Zdziwienie, zdumienie i zaskoczenie pojawiają się, gdy dane w systemie nie odpowiadają danym rzeczywistym, a urzędnik bardziej wierzy systemowi niż faktom i na zainteresowanego zrzuca udowodnienie błędu. Każdy taki incydent powoduje zmniejszenie zaufania do administracji publicznej. Oto przykłady:

- **Centralna Ewidencja i Informacja o Działalności Gospodarczej**

Została wdrożona pod koniec 2011 r. Ze względu na opóźnienia w migracji danych z systemów gminnych wyłączono weryfikację nazw ulic z referencyjną bazą adresów TERYT. Skutek? Do dziś dnia w bazie są adresy niezgodne z krajowym rejestrem urzędowym podziału terytorialnego kraju prowadzonym przez GUS, a dokładnie z Centralnym Katalogiem Ulic. Skąd to wiem? Bo tak jest w przypadku mojej kamienicy. Owszem, przeglądarka wpisów CEIDG podpowiada pełną nazwę ulicy zgodną z bazą TERYT. Jednak po jej wybraniu możemy nie zobaczyć niektórych przedsiębiorców, jeżeli podamy plac lub aleję jako kryterium wyszukiwania. Dla Warszawy system wyświetli następujące liczby wpisów:

nazwa pełna	wpisów	nazwa niepełna	wpisów
Plac Konstytucji	59	Konstytucji	112
Aleja Jana Chrystiana Szucha	38	Szucha	111

Organy administracji publicznej nie mogą domagać się okazywania, przekazywania lub załączania do wniosków i innych przedkładanych przed nimi pism zaświadczeń o wpisie do CEIDG, bowiem same pobierają z systemu plik pdf z danymi publicznymi przedsiębiorcy. Błędy w jego danych mogą uniemożliwić jego udział w przetargu publicznym czy wynajem lokalu komunalnego. Znam przypadek sprzed kilku tygodni, gdy na podstawie błędnego wpisu miejsca wykonywania działalności gospodarczej najemcę jednego z kilku lokali użytkowych w budynku uznano za właściciela całej nieruchomości.

- **Elektroniczne Księgi Wieczyste**

Były wdrażane w latach 2003–2010. Tyle trwała migracja, która także spowodowała wiele błędów w danych. Sama się o tym przekonałam dopiero po czterech latach od migracji, gdy poszłam do sądu po nowy numer księgi wieczystej mojego mieszkania. Okazało się, że nazwa ulicy w EKW jest niezgodna z bazą TERYT. W 2011 r. jej aktualizacja zajęła kilka tygodni. W zeszłym tygodniu usłyszałam od znajomego, że 14 miesięcy (słownie: czternaście) potrwa sprostowanie stwierdzonego w marcu br. błędu w jego imieniu popełnionego w trakcie migracji, czyli ręcznym przepisywaniu danych z akt do systemu. Nie ma mowy o sprzedaży nieruchomości czy innym jej dysponowaniu dopóki błąd nie zostanie usunięty.

- **Platforma Usług Elektronicznych ZUS**

Każdy z nas jest klientem Zakładu Ubezpieczeń Społecznych. Jesteśmy płatnikami i/lub świadczeniobiorcami. Na informatyzację ZUS-u wydano miliardy złotych. W Strategii ZUS na lata 2021–2025 słowo „automatyzacja" występuje 36 razy w kontekście świadczeń emerytalno-rentowych, rozliczeń płatników składek, wypłat zasiłków, procesów oraz wymiany danych z podmiotami i instytucjami zewnętrznymi. Automatyzacja ma m.in. ograniczyć błędy w decyzjach dla świadczeniobiorców w wyniku mniejszego udziału pracownika w procesie (powtarzalne czynności będą realizowane automatycznie przez system). Krótko mówiąc, ZUS ma być innowacyjną instytucją zaufania i zabezpieczenia społecznego.

Platforma Usług Elektronicznych ZUS

W 2017 r. próbowałam uzyskać z ZUS-u szczegółowe informacje, jak Zakład wyliczył moją emeryturę. Nie udało się pomimo długich starań. Miałam wątpliwości co do obliczenia wysokości świadczenia przedstawionego w decyzji i nadal nie wiem, skąd się biorą wartości kolejnych miesięcznych przelewów. W ramach innowacyjności ZUS powinien udostępniać w systemie PUE indywidualne szczegółowe algorytmy wyliczenia świadczenia. Wtedy wystarczy zalogować się i pobrać stosowny e-dokument – bez korespondencji w formie papierowej. To dopiero byłby dowód zaufania, uczciwości i szacunku Zakładu wobec swoich interesariuszy.

(Nie)Wiara w cyfryzację

Brak zaufania i wiary w dobre intencje pomysłodawców pojawia się także w kontekście nowych propozycji administracji publicznej utworzenia kolejnej centralnej bazy przetwarzającej nasze dane lub rozszerzenia już istniejącej. Ostatnio krytyczne komentarze wywołały m.in. następujące pomysły:

Zintegrowana Platforma Analityczna

Na portalu Dziennik Gazeta Prawna 4 lutego br. ukazał się artykuł o alarmistycznym tytule „Orwell po polsku. Rząd pracuje nad megabazą. Potencjał do nadużyć". Redaktor odniósł się do kolejnego etapu budowy Zintegrowanej Platformy Analitycznej. Kolejnego, bo projekt trwa od 1.11.2017 r. (jak wynika z dokumentów Komitetu Rady Ministrów do spraw Cyfryzacji i Programu Operacyjnego Polska Cyfrowa), zaś projekty zapisów ustawy i rozporządzenia dotyczących ZPA były dostępne na stronach RCL-u od marca 2021 r.

ZPA ma umożliwić:

- korelację danych pochodzących z różnych rejestrów prowadzonych obecnie w ramach administracji publicznej w celu analizy posiadanych zbiorów, budowania modeli statystycznych umożliwiających predykcję i przewidywania kierunków wprowadzania polityk publicznych;

- uzyskanie analiz wielowymiarowych, które będą podstawą do zwiększenia skuteczności i szybkości działań administracji w wybranych obszarach problemów społecznych i gospodarczych, poprzez wsparcie i przyspieszenie procesów decyzyjnych za pomocą wysokiej jakości informacji analitycznej.

Przez dwa dni wszystkie media bezrefleksyjnie powtarzały tezy artykułu. Minister J. Cieszyński uspokoił nastroje, ogłaszając chęć spotkania i dyskusji. Całe zamieszanie wywołało u mnie zdziwienie, zdumienie, zaskoczenie i ... zażenowanie. Bowiem żadna z osób wymienionych w artykule nie podzieliła się swoimi obawami, gdy była na to właściwa pora, czyli w czasie pierwszego i drugiego czytania proponowanych zmian w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne na posiedzeniach Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii Sejmu RP w lipcu 2021 r. Na spotkaniu nie byłam, chociaż wysłałam zgłoszenie. Z twitterowego komunikatu po spotkaniu (https://twitter.com/CyfryzacjaKPRM/status/1519252003502931969) możemy się dowiedzieć, że zadanie ma być realizowane przy zachowaniu kontroli społecznej. Na razie nie wiemy, na czym kontrola ma polegać. Zatem wątpliwości pozostają.

Centralna Informacja Emerytalna

– Powołanie do życia CIE będzie odpowiadać na zapotrzebowanie społeczne, mitygować lęki oraz pozwoli Polakom lepiej planować przyszłość, o którą – jak wynika z badań – się martwią. Nawet 39% rodaków twierdzi, że co najmniej raz w miesiącu dopadają ich obawy związane z długoterminowym planowaniem finansów. Polacy są też zdecydowanie mniej przekonani o możliwości zapewnienia sobie komfortowej emerytury niż mieszkańcy innych krajów. Tak pomysłodawca uzasadnia projekt ustawy, która ma doprowadzić do zgromadzenia w jednym miejscu danych ze wszystkich filarów zabezpieczenia emerytalnego: publicznego (ZUS i KRUS), firmowego (PPK i PPE) i indywidualnego (IKE, IKZE i OFE). Docelowo *powstanie system dostarczający możliwie pełnej i kompleksowej informacji o stanie i możliwościach dalszego oszczędzania oraz oferujący zestaw narzędzi do administrowania tymi oszczędnościami*.

Z zapisów projektu ustawy wynika, że CIE będzie dublować PUE ZUS-u. Nie mogę się natomiast doczytać kolejności zasilania systemu naszymi danymi. Założenie profilu CIE i korzystanie z usług elektronicznych świadczonych za pomocą systemu CIE ma być dobrowolne. Czy CIE będzie odpytywać inne systemy o nasze dane dopiero gdy założymy profil, czy też już wcześniej je otrzyma i nam je po prostu udostępni po założeniu profilu? Tytuły prasy internetowej stanowią najlepszy komentarz: „Centralna Informacja Emerytalna, czyli Wielki Brat zagląda nam do portfela", „Po co rządowi Centralna Informacja Emerytalna? Bo obywatelom się nie przyda", „Rząd sprawdzi, ile masz na koncie. Czy jak masz nadwyżkę nie będzie dopłacał do emerytur?".

(Nie)Wiara w AI

Ja już wiem, jak bardzo sztuczna inteligencja może zaszkodzić. Dlatego doceniam powołanie w 2020 roku Podkomisji stałej do spraw regulacji prawnych dotyczących

algorytmów cyfrowych w ramach Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii Sejmu RP. Inicjatorem i wnioskodawcą powołania Podkomisji był poseł Grzegorz Napieralski, który został wybrany na jej przewodniczącego. Do dyskusji i współpracy ponad podziałami politycznymi i ponad wszelkimi sporami zaproszono wszystkie siły polityczne, rząd, instytucje rządowe, izby gospodarcze, branże, związki zawodowe, uczelnie, rzecznika praw konsumenta. Jak zaznacza Przewodniczący, debata na Podkomisji ma na celu budowanie norm, prawa, współpracę, aby rozwój technologiczny był dla człowieka, a nie obok człowieka.

Na posiedzeniach Podkomisji już dwukrotnie omawiano wyzwania i zagrożenia stosowania algorytmów cyfrowych dla pracowników i pracodawców oraz propozycje rozwiązań prawnych. Jak zaznaczył poseł Adrian Zandberg: *mamy w Polsce problem z zastąpieniem ludzkich decyzji przez algorytm i nadaniem tym decyzjom algorytmu rangi obiektywności, z którą nie można negocjować, z którą nie można polemizować, z którą nie można dyskutować. To jest zaprzeczeniem tego, w jaki sposób, przynajmniej co do zasady, ma być zorganizowane w Polsce środowisko pracy, opierające się na dialogu społecznym. Tej przestrzeni na dialog, negocjacje, dyskusje nie ma w chwili, kiedy odpowiedzią na każde pytanie jest „algorytm podjął decyzję", a odpowiedzią na pytania, w oparciu o jakie przesłanki – „nie interesuj się".*

Bardzo ciekawe były wypowiedzi pracowników dwóch dużych firm międzynarodowych, którzy opowiadali o praktykach swoich pracodawców. W jednej z firm stosuje się algorytmy cyfrowe do wyliczenia m.in. tzw. wskaźników wydajności pracowników w systemie komputerowym o nazwie ADAPT. W drugiej firmie algorytmy cyfrowe wyliczają m.in. trasy dostawy nieuwzględniające robót drogowych i wypadków czy bonusy za wagę przesyłek i za złe warunki atmosferyczne oraz dokonują oceny pracowników. W obu firmach, jak i w wielu innych, algorytmy są zwłaszcza z perspektywy pracowników bardzo mocno nieprzejrzyste, co oznacza, że na poziomie bardzo praktycznym pracujący nie mają jasności co do tego, jakie dane są zbierane na temat ich pracy i na podstawie jakich przesłanek są podejmowane decyzje dotyczące ich obciążenia pracą, dotyczące oceny pracy, dotyczące wynagrodzenia, dotyczące awansu. Oba przypadki opisane w trakcie posiedzenia Podkomisji pokazują, jak nieprzejrzyste algorytmy cyfrowe pracy mogą doprowadzić do braku zaufania interesariuszy do technologii i do ludzi, którzy stoją za tymi technologiami.

(Nie)Wiara w gotowość

W marcu br. Kancelaria Prezesa Rady Ministrów ogłosiła przetarg na przeprowadzenie badania „W drodze ku

Komisja Europejska także pracuje nad nowymi przepisami dotyczącymi sztucznej inteligencji, zmieniającymi zasady bezpieczeństwa w taki sposób, aby zwiększyć zaufanie użytkowników do produktów nowej generacji o wszechstronnych zastosowaniach. Przyjęto w nich podejście oparte na analizie ryzyka. Systemy AI wysokiego ryzyka będą musiały spełnić rygorystyczne wymogi przed wprowadzeniem do obrotu:

- **odpowiednie systemy oceny i ograniczania ryzyka;**
- **wysoka jakość zbiorów danych zasilających system w celu zminimalizowania ryzyka i dyskryminujących skutków;**
- **ewidencjonowanie działania w celu zapewnienia identyfikowalności wyników;**
- **szczegółowa dokumentacja zawierająca wszystkie informacje na temat systemu i jego celu, aby organy mogły ocenić jego zgodność z wymogami;**
- **jasne i odpowiednie informacje dla użytkownika;**
- **odpowiednie środki nadzoru przez człowieka w celu zminimalizowania ryzyka;**
- **wysoki poziom solidności, bezpieczeństwa i dokładności.**

W swoim sprawozdaniu z dnia 19.02.2020 r. na temat wpływu sztucznej inteligencji, internetu rzeczy i robotyki na bezpieczeństwo i odpowiedzialność [ang. Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics] Komisja Europejska zaznaczyła, że: *pojawienie się nowych technologii cyfrowych, takich jak AI, IoT i robotyka stwarza nowe wyzwania w zakresie bezpieczeństwa produktów i odpowiedzialności za produkt, takie jak łączność z internetem, autonomia, zależność od danych, nieprzejrzystość, złożoność produktów i systemów, aktualizacje oprogramowania oraz bardziej złożone systemy zarządzania bezpieczeństwem i łańcuchy wartości.* Poddaje więc pod rozwagę wprowadzenie zmian w dyrektywie w sprawie odpowiedzialności za produkty i w krajowych systemach odpowiedzialności, by ułatwić poszkodowanym uzyskanie odszkodowania we wszystkich przypadkach, w których byłoby to zasadne.

doskonałości cyfrowej", czyli gotowości wdrożenia, poziomu wiedzy i wykorzystania nowych technologii w sektorze publicznym i prywatnym. Kancelaria jest gotowa wydać na nie 550 tys. zł. Zamówienie jest podzielone na cztery części: A – jednostki samorządu terytorialnego, B – administracja centralna, C – spółki skarbu państwa oraz D – małe i średnie przedsiębiorstwa. Zdziwienie, zdumienie i zaskoczenie wywołało u mnie użycie pojęcia „doskonałości cyfrowej". Ewidentnie pomysłodawca naiwnie wierzy, że nowe technologie doprowadzą do idealnego działania e-administracji państwowej.

> *Do kogo mamy się wtedy zgłosić?*
> *Z kim mamy rozmawiać?*
> *Gdzie złożyć skargę?*
> *Kto się poczuje do odpowiedzialności?*
> *Kto nam pomoże?*

Dalekie od doskonałości są warunki przetargu. Zgodnie z SIWZ-em Wykonawca zapewni Zamawiającemu bieżący dostęp do bazy danych kontaktów z badanymi, zawierającej m.in. dane osobowe, tj. imię, nazwisko, telefon oraz stanowisko i zamiast oraz nazwę jednostki. Jeden z potencjalnych oferentów zwrócił uwagę w pytaniu 21, że taki zapis jest niezgodny z Międzynarodowym kodeksem praktyki badań rynkowych i społecznych wydanym przez ICC/ESOMAR, regulującym działalność zawodową obejmującą dziedzinę naukowych badań rynku. Zaznaczył, że przestrzegając zasad etyki badawczej, należy chronić respondentów i budować zaufanie do prowadzonych badań. Zaś wskazany zapis pozwala Zamawiającemu na powiązanie badanej osoby z udzielanymi przez nią odpowiedziami. Odpowiedź Zamawiającego przytaczam w całości: *W przypadku badania MŚP – pełna zgoda. Zamawiający nie będzie chciał mieć dostępu do danych ankietowanych. Jednak w przypadku administracji publicznej wykonawca musi mieć na uwadze, że będzie badać jednostki administracji, a odpowiedzi będą udzielać urzędnicy pełniący funkcje publiczne. Jak wynika z informacji z otwarcia ofert, są firmy, które nie przejmują się etyką badawczą i zaufaniem respondentów.*

Trwa informatyzacja, cyfryzacja, digitalizacja wszystkiego, co popadnie i gdzie popadnie. Wszyscy się ekscytują, zachwycają i chwalą swoimi wdrożeniami. A co się dzieje, gdy owe wspaniałe rozwiązania informatyczne zaczynają źle działać? Przecież wcześniej czy później coś pójdzie nie tak. Do kogo mamy się wtedy zgłosić? Z kim mamy rozmawiać? Gdzie złożyć skargę? Kto się poczuje do odpowiedzialności? Kto nam pomoże? Te i podobne pytania będziemy zadawać coraz częściej. Nie będzie cyfrowego zaufania bez jasnej, jednoznacznej i rzetelnej odpowiedzi na nie. Pozostanie strach, niepewność, przygnębienie, bezsilność, bezradność, niesmak. Czy tego chcemy?

ISACA na ratunek

Stowarzyszenie ISACA postanowiło wesprzeć organizacje w budowaniu bezpieczniejszego cyfrowego świata dla nas wszystkich (https://www.isaca.org/digital-trust).

W swoim opracowaniu zatytułowanym „Digital Trust: A Modern-Day Imperative" wskazuje sześć czynników określających cyfrowe zaufanie:

- jakość [ang. *quality*],
- dostępność [ang. *availability*],
- bezpieczeństwo i prywatność [ang. *security and privacy*],
- etyka i integralność [ang. *ethics and integrity*],
- transparentność i uczciwość [ang. *transparency and honesty*],
- stabilność i odporność [ang. *stability and resilience*].

Wymienione czynniki stanowią podstawę nowej metodyki „Digital Trust Ecosystem Framework", która będzie dostępna jeszcze w tym roku. Brałam udział w jej opracowaniu i gorąco polecam ją zarówno bankom i podmiotom z sektora prywatnego, jak i jednostkom sektora finansów publicznych.

Wszystkie informacje zawarte w artykule są podane według stanu na dzień 24 maja 2022 r.