Gryziklawiaturki w akcji

Do historii przeszedł już gryzipiórek, czyli pracownik biurowy posługujący się gęsim piórem w swojej pracy. Dzisiaj rządzi gryziklawiaturek, czyli urzędnik korzystający z komputera i różnorakich systemów przetwarzających nasze dane osobowe do obsługi naszych wniosków, zgłoszeń i różnych innych spraw. Gdzie spotkamy gryziklawiaturków? Niestety, wszędzie.

Joanna Karczewska

absolwentka Wydziału Elektroniki PW z ponad 40-letnim doświadczeniem w informatyce. Jako certyfikowany audytor systemów informatycznych – CISA – specjalizuje się w audytach informatycznych w jednostkach sektora finansów publicznych. Pełni także funkcję inspektora ochrony danych w placówkach oświatowych. Jako Expert Reviewer uczestniczyła w opracowaniu metodyk COBIT5 i COBIT 2019, ITAF 4th Edition oraz publikacji ISACA dotyczących Digital Trust Ecosystem Framework. Bierze udział w konsultacjach aktów prawnych dotyczących bezpieczeństwa informacji, cyberbezpieczeństwa i ochrony danych osobowych, również na forum Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii Sejmu RP. Uznana w 2022 roku za jedną z Europe's Top Cyber Women. Ekspert Najwyższej Izby Kontroli.

O mojej konfrontacji ze sztuczną inteligencją banku ING i Ministerstwa Finansów/Krajowej Administracji Skarbowej (MF/KAS) informuję Państwa od dwóch lat. Po 20 latach korzystania z konta bank zidentyfikował mnie jako rezydenta podatkowego USA, bo urodziłam się w USA. W związku z FATCA bank zamierzał przekazać moje dane do Internal Revenue Service USA za pośrednictwem Krajowej Administracji Skarbowej, co było całkowicie bezprawne. Zainteresowanych szczegółami moich zmagań odsyłam do artykułu „Cyber-odklejka" w nrze 1/2023 „Domeny".

Od tego czasu:

- Rozstałam się z bankiem po tym, jak wypowiedział mi umowę. O dziwo, bank o mnie „nie zapomniał", bo już po okresie wypowiedzenia wysłał mi SMS informujący o zmianach w regulaminie bankowości elektronicznej i drugi – o zmianach w limitach przelewów BLIK, zachęcając do sprawdzenia szczegółów w moim ING.

- Napisałam do Rzecznika Praw Obywatelskich (RPO), prosząc o sprawdzenie ochrony praw obywateli polskich w związku z FATCA. Urzędnik Biura RPO odezwał się do mnie po ponad roku. Poinformował, że „kontrole w zakresie FATCA i CRS raportujących instytucji znajdują się w obszarze zainteresowania Rzecznika Praw Obywatelskich i są obecnie przedmiotem analizy". Dodał, że ewentualne wystąpienia Rzecznika w tej sprawie udostępniane będą na stronie internetowej, do której śledzenia gorąco mnie zachęca. Odpisałam, że w mojej sprawie złożyłam skargę do Prezesa UODO. Zwrotnie dowiedziałam się, że „Rzecznik działa na zasadzie subsydiarności, co oznacza, że Rzecznik nie zastępuje i nie wyręcza obywateli w prowadzeniu ich spraw, a więc nie świadczy usług typowo adwokackich". Dokładnie tego samego dnia pracownik Biura RPO oświadczył w „Faktach" TVN, że Biuro prowadzi kilkaset postępowań w sprawie poszkodowanych studentów Collegium Humanum.

- Skontaktowałam się z przedstawicielstwem drugiej strony. *I am lost for words that could describe their attitude to my case.*

- 8 stycznia 2024 r. złożyłam skargę do Prezesa Urzędu Ochrony Danych Osobowych na bezprawne i nielegalne przekazanie moich danych osobowych do państwa trzeciego. Prezes UODO postanowił podzielić postępowanie na dwa: jedno w stosunku do banku i drugie w stosunku do Ministerstwa Finansów i Krajowej Administracji Skarbowej. 30 września 2024 r. Urząd poinformował w piśmie, że zgromadził materiał dowodowy wystarczający do wydania decyzji administracyjnej. Drugie pismo odebrałam 12 listopada 2024 r. Od tego czasu zapadła cisza – mam cierpliwie czekać.

Dlaczego kolejny raz wracam do mojej sprawy? By pokazać, jakich przykrości i upokorzeń będą doznawać osoby skrzywdzone przez AI. Wprawdzie zgodnie z art. 51 ust. 3 projektu ustawy o systemach sztucznej inteligencji postępowanie nie będzie mogło„trwać dłużej niż 6 miesięcy od dnia doręczenia stronom postanowienia o wszczęciu postępowania skargowego". Jednakże w art. 52 mowa jest o postępowaniu dowodowym, a okresu jego prowadzenia nie wlicza się do terminu, o których mowa w art. 51 ust. 3. Przy wielomiesięcznym wyjaśnianiu skargi osoby poszkodowane będą krzywdzone podwójnie: najpierw przez sztuczną inteligencję, następnie przez urzędników. Nieciekawa perspektywa.

Gra pozorów

W przypadku materiału dla placówek oświatowych dot. ochrony wizerunku dzieci w internecie opublikowanego na stronach UODO (https://uodo.gov.pl/pl/138/3312), moje zastrzeżenia dotyczyły następujących zapisów na 14 str.:

- **nauczyciele/ki i rodzice korzystają z komunikacji poprzez zamknięte grupy na komunikatorach. Jeżeli razem z rodzicami komunikuje się tam nauczyciel/ka – jest osobą reprezentującą placówkę i zobowiązany jest do ochrony danych osobowych, tajemnicy służbowej. Jeżeli wysyła na takiej grupie zdjęcia, filmiki – udostępnia dane osobowe szczególne. Może lepszym rozwiązaniem będzie gromadzenie zdjęć na zabezpieczonych dyskach i dzielenie się nimi wyłącznie z rodzicami/prawnymi opiekunami;**

- **zdjęcia bardzo często wykonywane są prywatnymi telefonami, bez odpowiednich zabezpieczeń, których wymagają dane osobowe, w tym wizerunek – to rodzi szereg nieprawidłowości;**

- **przedszkola, szkoły i placówki nie zatrudniają social media menedżerów, zadania te wykonują więc nauczyciele/ki poza zakresem swoich obowiązków;**

- **jeśli rodzice, opiekunowie chcą wiedzieć, jak mają się dzieci – warto z nimi rozmawiać. Jeśli wymaga to dzielenia się zdjęciami – warto stworzyć zamkniętą grupę na komunikatorze i używać do rozpowszechniania zdjęć i filmów odpowiednio zabezpieczonych sprzętów.**

W numerze 3-4/2024 „Domeny" wspomniałam o dwóch poradnikach z dobrymi praktykami ochrony dzieci w sieci, opracowanych przez znane fundacje i bezrefleksyjnie polecanych przez instytucje państwowe. W obu przypadkach

wysłałam pisma z moimi uwagami do zainteresowanych urzędów. Od obu dostałam od urzędników uprzejme listy z podziękowaniami i zapewnieniem, że „wszystkie zgłoszone sugestie zostaną dokładnie przeanalizowane i w miarę możliwości, uwzględnione w przyszłych aktualizacjach" (UODO) lub „przekazany przez Panią dokument będzie na pewno poddany analizie podczas aktualizowania wytycznych" (Ministerstwo Sprawiedliwości).

Jak zaznaczyłam w swoim piśmie, autorzy cytowanych treści wręcz namawiają nauczycieli i nauczycielki do naruszenia przepisów dotyczących ochrony danych osobowych. Absolutnie niedopuszczalne i bezprawne jest wykonywanie poza zakresem obowiązków jakichkolwiek czynności związanych z przetwarzaniem danych osobowych dzieci będących pod ich opieką. Niedopuszczalne jest też publikowanie dywagacji dotyczących tajemnicy służbowej, danych osobowych szczególnych, grup zamkniętych, zabezpieczonych dysków czy social mediów menedżerów (korporacyjny wynalazek). I przypomniałam, że – jak ponownie wskazał Europejski Inspektor Ochrony Danych (*European Data Protection Supervisor – EDPS*) w swoim biuletynie nr 111 – planując jakiekolwiek przetwarzanie danych osobowych przede wszystkim należy:

1. sprawdzić, czy organizacja ma odpowiednią podstawę prawną do przetwarzania danych osobowych;
2. sprawdzić, czy przetwarzanie jest zgodne ze wszystkimi zasadami ochrony danych;
3. skonsultować się z inspektorem ochrony danych.

W cytowanym materiale nie znajdziemy śladu wskazówek EDPS. Na dodatek kontradyktoryjne zalecenia przedstawił Inspektor Ochrony Danych UODO w trakcie webinarium „Więcej szacunku dla młodego wizerunku" (18 grudnia 2024 r.), zorganizowanym przez Biuro Rzecznika Praw Dziecka (https://www.facebook.com/RzecznikPrawDzieckaMonikaHornaCieslak/videos/1273778826999242). Ewidentnie nie czytał materiału.

Zgodnie z planem kontroli sektorowych na 2025 r. UODO zamierza sprawdzić podmioty, które przetwarzają wizerunki dzieci, gdy wymagana jest zgoda wyrażona przez rodziców lub opiekunów prawnych. Zobaczymy, jakie kryteria oceny badanego obszaru zastosują urzędnicy.

Odkrywanie Ameryki

Również Ministerstwo Cyfryzacji od czasu do czasu poleca opracowania różnych organizacji pozarządowych jako własne. Ostatnio były to wytyczne „Umiejętności i cyberhigiena – wsparcie i rozwój kompetencji cyfrowych", przygotowane przez Stowarzyszenie Instytut Kościuszki (https://www.gov.pl/web/cyfryzacja/rekomendacje-dotyczace-umiejetnosci-cyfrowych-i-cyberhigieny). Jak zaznaczyli autorzy, dokument został przygotowany dla Ministerstwa Cyfryzacji i zawiera rekomendacje dotyczące działań mających na celu wskazanie luk, podniesienie poziomu wiedzy i umiejętności w zakresie bezpiecznego użytkowania technologii cyfrowych w Polsce.

> *Niestety, opracowanie nie zawiera nic odkrywczego. Przedstawia długą listę stwierdzeń i podpowiedzi, które my od lat formułujemy pod adresem ministra właściwego do spraw informatyzacji i jego urzędników.*

Autorzy rekomendują m.in. stworzenie katalogu kompetencji cyfrowych, obejmującego umiejętności miękkie i twarde, oraz regularną identyfikację luk kompetencyjnych z udziałem sektora prywatnego.

Pytania narzucają się same. Czyżby dotąd resort cyfryzacji nigdy się tym nie zajmował? Czyżby Sektorowe Rady ds. Kompetencji w sektorze Informatyka oraz sektorze Telekomunikacja i Cyberbezpieczeństwo nie wywiązywały się ze swoich zadań? Co z ustawowym Zintegrowanym Systemem Kwalifikacji? Wyrzucamy wieloletnią pracę nad nim do kosza? Ignorujemy istnienie Szerokiego Porozumienia na rzecz Rozwoju Umiejętności Cyfrowych?

Co dostajemy w zamian?

- Włączenie standardów cyberhigieny do regulacji prawnych i obowiązkowych szkoleń pracowników.

Zwracam autorom uwagę, że wymóg zapewnienia szkoleń w zakresie bezpieczeństwa informacji dawno już został uwzględniony w polskich przepisach. Najbardziej znane to rozporządzenie o KRI, obecnie RODO i KSC.

- Wprowadzenie mechanizmów oceny skuteczności działań edukacyjnych w obszarze cyberhigieny.

Użycie określenia „wprowadzenie" oznacza przyznanie się resortu cyfryzacji, że dotychczas tego nie robił. Czuję duży niepokój i zażenowanie, że urzędnicy nie poczuwali się do sprawdzania efektów dotychczasowych programów edukacyjnych i szkoleniowych prowadzonych przez fundacje, organizacje pozarządowe i instytucje państwowe za wiele milionów złotych z programów unijnych.

- Stworzenie platformy edukacyjnej, na przykład w ramach aplikacji M-Obywatel [pisownia oryginalna – przyp. JK], która mogłaby zwiększać świadomość na temat metod oszustw skierowanych do seniorów.

Autorzy ewidentnie nie słyszeli o nadal oczekującej na realizację rekomendacji NIK z 2022 r. stworzenia jednego,

rozpoznawalnego, oficjalnego, państwowego serwisu, zawierającego łatwo dostępne informacje na temat zagrożeń cyberbezpieczeństwa, trwających kampanii, a także zaleceń i dobrych praktyk z zakresu „cyberhigieny". Ponadto serwis czy platforma muszą być dostępne dla każdego zainteresowanego, a nie tylko dla użytkowników mObywatela.

- skorzystanie z inicjatywy Cyberpeace Builders Instytutu Cyberpeace, która oferuje wsparcie technologiczne dla organizacji wrażliwych, takich jak szpitale.

Ta rekomendacja wręcz mnie przeraziła. Wreszcie szpitale mozolnie, krok po kroju, budują swoje cyberbezpieczeństwo z pomocą i wsparciem Ministerstwa Zdrowia, Centrum e-Zdrowia i jego CSIRT-u, Polskiej Federacji Szpitali i wielu innych polskich interesariuszy. A tu raptem Ministerstwo Cyfryzacji rekomenduje im jakąś nieznaną organizację pozarządową z siedzibą w Szwajcarii, która nawet nie ma strony internetowej po polsku (podobnie jak Global Cyber Alliance). Ręce opadają.

CIEchoroba

Czas na optymistyczną wiadomość. 20 grudnia 2024 r. na stronach Rządowego Centrum Legislacji pojawił się projekt ustawy o uchyleniu ustawy o Centralnej Informacji Emerytalnej przygotowany przez Ministra Cyfryzacji. Od początku byłam przeciw CIE, a swoje wątpliwości dotyczące cyberbezpieczeństwa proponowanego systemu opisałam w numerze 3/2023 „Domeny".

Do projektu dołączono Ocenę Skutków Regulacji, zawierającą m.in. dwuczęściowe uzasadnienie. W pełni zgadzam się z pierwszą częścią przedstawioną przez projektodawcę:

„Ustawa z dnia 7 lipca 2023 r. o Centralnej Informacji Emerytalnej (Dz. U. poz. 1941), zwana dalej «ustawą o CIE», wprowadziła rozwiązania, które **nie zapewnią kompleksowej realizacji założonego celu**, jakim jest poprawa świadomości emerytalnej i zachęta do efektywnego oszczędzania na przyszłość. Jednocześnie rozwiązania te generują **bardzo wysokie koszty** dla budżetu państwa. Należy również wskazać, że to **Zakład Ubezpieczeń Społecznych** prowadzi działania w obszarze edukacji społeczeństwa w zakresie oszczędzania na cele emerytalne".

I na tym projektodawca mógł poprzestać. Postanowił jednak „docisnąć kolanem" i dopisał jakże zaskakującą drugą część:

„Dodatkowo, **proponowane rozwiązania systemu wymagają posiadania komputera lub smartfonu oraz kompetencji cyfrowych, co może wykluczyć część społeczeństwa z dostępu do informacji zgromadzonych w CIE**".

Będę to przypominać wszystkim ustawodawcom przy każdej okazji wpychania nam kolejnej obligatoryjnej usługi cyfrowej. Chyba, że stwierdzenie ma uzasadniać dalsze wydawanie dziesiątek milionów złotych na podnoszenie kompetencji cyfrowych Polaków bez oceny skuteczności podejmowanych działań.

Gdzie kucharek sześć

Na koniec kilka słów o cyfryzacyjnym blamażu Ministerstwa Cyfryzacji. 1 stycznia 2025 r. ruszyły e-Doręczenia, czyli krajowy system doręczeń elektronicznych listów poleconych za potwierdzeniem odbioru, obligatoryjny dla długiej listy podmiotów publicznych oraz wielu podmiotów niepublicznych.

Od czasu, gdy pracownicy Centralnego Ośrodka Informatyki zniszczyli mi dokument w systemie ePUAP, bacznie obserwowałam przygotowania do opracowania i wdrożenia nowego systemu komunikacji z administracją publiczną. Śledziłam projekty i same ustawy o doręczeniach publicznych. W numerze 3/2021 „Domeny" zwracałam uwagę na niespójności zapisów ustawy, które dotyczą zapewnienia bezpieczeństwa zastosowanych systemów teleinformatycznych. Zbierałam materiały wydawane przez różne podmioty oraz artykuły prasowe. W 2024 r. pomagałam moim jednostkom w przygotowaniu do stosowania e-Doręczeń. Moja intuicja i 45-letnie doświadczenie zawodowe podpowiadały mi cały czas, że system nie zadziała.

Pierwsze wpisy o kłopotach z systemem pojawiły się w internecie już 3 stycznia. Z dnia na dzień było gorzej do tego stopnia, że 22 stycznia Ministerstwo Cyfryzacji opublikowało niepokojący komunikat, w którym próbowało zrzucić winę za problemy na Pocztę Polską jako wykonawcy usług PURDE (doręczenie całkowicie elektroniczne) i PUH (doręczenie hybrydowe), jednocześnie wybielając siebie i Centralny Ośrodek Informatyki. Komunikat zakończono zdaniem: „W najbliższym czasie planowane jest dodatkowo spotkanie z udziałem wszystkich interesariuszy, aby usprawnić procesy związane z funkcjonowaniem e-Doręczeń". Rychło w czas… Kolejny komunikat z 27 stycznia obwieszczał, że „rozwiązano **większość** problemów, które pojawiły się w pierwszych dniach obowiązywania systemu". Zmroziło mnie, bo użycie słowa „**większość**" zwiastowało dalsze kłopoty. Popłoch panujący wśród użytkowników systemu najlepiej ilustruje komunikat Ministerstwa Finansów z 30 stycznia: „Zgodnie z przepisami Ordynacji podatkowej opóźnienie w akceptacji nadania korespondencji przez dostawcę usługi e-Doręczenia nie wpływa na zachowanie terminów prawa podatkowego".

Czy można było zapobiec kolejnej **nieudanej cyfryzacji**? Szczególnie zainteresowały mnie dwie kwestie: analiza ryzyka oraz rozliczalność. Zajrzałam do dokumentów projektu „e-Doręczenia – usługa rejestrowanego doręczenia elektronicznego w Polsce" przygotowanych przez Ministerstwo Cyfryzacji i dostępnych na stronie Komitetu Rady Ministrów do spraw Cyfryzacji (https://www.gov.pl/web/krmc). Znalazłam ryzyka wpływające na utrzymanie

efektów wpisane do pierwotnego opisu założeń projektu informatycznego (z 24.05.2019 r.) i do raportu końcowego z realizacji projektu informatycznego (z 11.07.2024 r.). Zidentyfikowano cztery ryzyka. Pierwsze dwa to wprowadzenie nieoptymalnego modelu finansowania usługi oraz samodzielne wdrożenie horyzontalnych rozwiązań teleinformatycznych dotyczących doręczeń elektronicznych.

Przyjrzałam się dwóm pozostałym, które się zmaterializowały:

Nazwa ryzyka	**Utrata zaufania do systemu w wyniku niedostępności systemu, niewystarczającego zapewnienia bezpieczeństwa danych**
Siła oddziaływania	średnia
Prawdopodobieństwo wystąpienia ryzyka	średnie
Sposób zarządzania ryzykiem	na początku (24.05.2019) m.in.: – **wykonanie testów** przed wprowadzeniem na środowisko produkcyjne
	na końcu (11.07.2024): ryzyko zostało zminimalizowane – **przeprowadzono testy** wydajności i bezpieczeństwa
Nazwa ryzyka	**Brak akceptacji społecznej i zainteresowania użytkowników końcowych wdrożonym rozwiązaniem**
Siła oddziaływania	duża
Prawdopodobieństwo wystąpienia ryzyka	niskie
Sposób zarządzania ryzykiem	na początku (24.05.2019) m.in.: – umocowanie projektu w przepisach prawa wraz z ustanowieniem obligatoryjności korzystania z produktów projektu – powiązanie procesów projektu z innymi procesami użytkowników końcowych
	na końcu (11.07.2024): Ryzyko może się zmaterializować, jeśli podmioty zobowiązane ustawowo do wdrożenia e-Doręczeń nie będą w pełni przygotowane na korzystanie z nowego systemu [...]. Ryzyko zostało zminimalizowane dzięki prowadzonym **działaniom wdrożeniowym wśród zobowiązanych podmiotów**.

30 stycznia Związek Powiatów Polskich opublikował listę problemów, z jakimi zmagają się starostwa powiatowe w związku z obowiązkiem korzystania z e-Doręczeń (https://wartowiedziec.pl/serwis-glowny/aktualnosci/75389-z-jakimi-problemami-zmagaja-sie-starostwa-powiatowe-w-zwiazku-z-obowiazkiem-korzystania-z-e-doreczen). Jej przegląd skłania do przypuszczenia, że wymienione w analizie ryzyka testy wydajności i bezpieczeństwa nie były wystarczające. Moimi wątpliwościami podzieliłam się 5 lutego 2025 r. podczas posiedzenia Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii Sejmu RP (https://www.sejm.gov.pl/Sejm10.nsf/PosKomZrealizowane.xsp?komisja=CNT#42). Przedstawiciel Ministra Cyfryzacji zarzekał się, że testy wydajności zostały wykonane przez NASK i ABW i że przeprowadzono siedem audytów dostępności. A jednak doszło do utraty zaufania do systemu i braku akceptacji, skoro 14 stycznia na posiedzeniu Zespołu do Spraw Społeczeństwa Informacyjnego Komisji Wspólnej Rządu i Samorządu Terytorialnego samorządowcy postulowali wyłączenie użytkowania systemu do e-Doręczeń do momentu dopracowania zgłoszonych problemów.

Z doniesień prasowych oraz oficjalnych komunikatów pojawiających się od początku roku w domenie publicznej wynika, że każdy podmiot zaangażowany w tworzenie i utrzymanie systemu e-Doręczeń zarządza swoją częścią, natomiast nie widać właściciela systemu, który by koordynował działania wszystkich zaangażowanych podmiotów i którego można rozliczać za całościowe działanie systemu.

> *Unia Metropolii Polskich w swoim stanowisku (wysłanym do PAP 29 stycznia) domagała się rzetelnego raportu lub audytu zewnętrznego, który wykaże faktyczne przyczyny trudności.*

Jak przepisy określają role i odpowiedzialność za system? Zgodnie z ustawą z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (z późniejszymi zmianami):

- minister właściwy do spraw informatyzacji prowadzi bazę adresów elektronicznych będącą rejestrem publicznym;
- minister właściwy do spraw informatyzacji udostępnia usługę sieciową umożliwiającą przekazanie przez operatora wyznaczonego danych za pomocą bezpośredniej wymiany danych między systemem teleinformatycznym operatora wyznaczonego a bazą adresów elektronicznych;
- minister właściwy do spraw informatyzacji oraz minister właściwy do spraw gospodarki zapewniają funkcjonowanie systemów teleinformatycznych umożliwiających użytkownikom dostęp do skrzynek doręczeń w systemie teleinformatycznym operatora wyznaczonego oraz dostęp do PURDE i PUH, a **operator obowiązany jest do zintegrowania swojego systemu z ich systemami**;
- operator wyznaczony jest obowiązany do świadczenia PURDE wraz z udostępnieniem skrzynek doręczeń oraz PUH;
- minister właściwy do spraw łączności wraz z ministrem właściwym do spraw informatyzacji określa warunki składania reklamacji;
- Prezes UKE zatwierdza regulaminy PURDE i PUH oraz cenniki usług.

Według dokumentów przedłożonych Komitetowi Cyfryzacji w 2019 r., wnioskodawcą projektu był Minister Cyfryzacji, zaś beneficjentem jest Ministerstwo Cyfryzacji. Są też partnerzy: Ministerstwo Przedsiębiorczości i Technologii oraz Urząd Komunikacji Elektronicznej sprawujący nadzór i kontrole nad operatorem wyznaczonym, czyli Pocztą Polską S.A.

Komunikat Poczty Polskiej z 27 stycznia:

- Poczta Polska odpowiada za system backendowy do realizacji usługi rejestrowanego doręczenia elektronicznego (tj. poprawną realizację wysyłki i generowanie dowodów jej dostarczenia) oraz dostarcza UA API i infrastrukturę odpowiadającą za działanie systemu;
- Ministerstwo Cyfryzacji wraz z Centralnym Ośrodkiem Informatyki (edoreczenia.gov.pl), Ministerstwo Rozwoju i Technologii (biznes.gov.pl) oraz dostawcy poszczególnych systemów kancelaryjnych, z których korzystają urzędy, odpowiadają za aplikacje frontendowe (interfejs użytkownika);
- Centralny Ośrodek Informatyki zapewnia wszystkim podmiotom uczestniczącym w procesie dostęp do testowego środowiska integracyjnego oraz dane do wykonywania testów usługi;
- integratorzy [w liczbie kilkudziesięciu – przyp. JK] implementują UA API, którego dostawcą jest Poczta Polska;
- ponad 40 tys. podmiotów publicznych przystąpiło do systemu e-Doręczeń [docelowo ponad 28 milionów podmiotów].

Podsumowując: po pierwsze sam ustawodawca zadbał o zagmatwanie rozliczalności, przydzielając zadania informatyczne związane ze sprawnym działaniem e-Doręczeń różnym resortom i podmiotom. Pojęcie odpowiedzialności pojawia się w ustawie, o dziwo, tylko w stosunku do operatora wyznaczonego i tylko jego dotyczy postępowanie reklamacyjne. Po drugie, podmiotów zaangażowanych we wdrożenie i utrzymanie systemu jest dużo więcej niż wymienione w ustawie. Po trzecie, nie wyznaczono właściciela systemu. W trakcie wspomnianego posiedzenia Komisji Cyfryzacji zapytałam przedstawiciela Ministra Cyfryzacji o to, kto jest właścicielem e-Doręczeń. Nie udzielił żadnej odpowiedzi.

Od lat wiadomo, jak należy zarządzać projektami informatycznymi. Są sprawdzone standardy, normy, metodyki i dobre praktyki. System e-Doręczeń nie jest ani pierwszym, ani najbardziej skomplikowanym systemem wdrażanym w administracji publicznej. Co zatem zawiodło? Odpowiedź jest prosta. Projekt nie był rządzony, czyli nie było „**governance**". Był jedynie zarządzany przez poszczególne podmioty. Ministerstwo Cyfryzacji było pomysłodawcą i beneficjentem projektu. To jemu powinno najbardziej zależeć na płynnym wdrożeniu systemu za ponad 70 mln zł z funduszy unijnych. Tak się nie stało.

Zamiana pióra na klawiaturę wcale nie usprawnia naszego codziennego funkcjonowania, tylko stopniowo je zmienia. Owszem, nie musimy już chodzić do urzędu czy firmy, by załatwić nasze sprawy – wystarczy mieć dostęp do internetu. Problemy – dużo większe niż w epoce analogowej – pojawiają się, gdy coś nie zadziała. Wtedy musimy użerać się z gryziklawiaturkami. Nie możemy mu czy jej spojrzeć w oczy, bo często są wirtualni, a czasami nawet – sztuczni. Boleśnie przekonujemy się o naszej niemocy, bo dla nich ważniejszy jest system w komputerze i co się w nim wyświetla niż obywatel, petent czy klient.

Wszystkie informacje zawarte w artykule są podane według stanu na dzień 15 lutego 2025 r.