POLSKIE TOWARZYSTWO INFORMATYCZNE

NUMER 1/2024

PRZYSZŁOŚĆ ZACZYNA SIĘ DZISIAJ

# Domena

ISSN 2720-6513

# Wyścig w eksaskali

## RODO do poprawki

**Mirosław Kutyłowski**
Regulacja CSAM bardziej niebezpieczna niż Pegasus

## Co dalej z polską AI?

## JAK UZDROWIĆ CYFROWE USŁUGI PUBLICZNE

# Spis treści




PTI Domena

**nr 1/2024**

**Wydawca:**
Polskie Towarzystwo Informatyczne

**Zarząd Główny:**
ul. Solec 38 lok.103
00-394 Warszawa
NIP: 522-000-20-38
tel.: +49 22 838 47 05
e-mail: pti@pti.org.pl

**Redaktor naczelna:**
Anna Kniaź
(anna.kniaz@pti.org.pl)

**Rada Programowa „Domeny”:**
Wiesław Paluszyński
– przewodniczący Rady
Marek Bolanowski
Marian Bubak
Beata Chodacka
Bogusław Dębski
Wojciech Kiedrowski

**Współpraca redakcyjna:**
Tomasz Kulisiewicz

**Korekta:**
Jolanta Jamiołkowska

**Skład i opracowanie graficzne:**
Agencja HEADOUT

Headout

Szanowni Państwo,

sztuczna inteligencja będzie, czy chcemy tego czy nie, istotnym elementem rzeczywistości. W tym numerze „Domeny" tematu AI dotykamy na różne sposoby. Anonsujemy powstanie w Polskim Towarzystwie Informatycznym Sekcji Aktualne Wyzwania Sztucznej Inteligencji, prezentując jej założycieli. Marek Hołyński, reagując na powołanie rządowego zespołu doradczego PL/AI Sztuczna inteligencja dla Polski, zastanawia się „Co dalej z polską AI?". Sztuczna inteligencja jest wątkiem bardzo ważnej dyskusji profesjonalistów: „Jak uzdrowić cyfrowe usługi publiczne". Nawet Michał Ogórek w swoim, jak zwykle przewrotnym, felietonie rozważa tezę, czy AI nas zaorze.

Ona jednak wcale nie czeka, aż ją oswoimy mentalnie, ukonstytuują się odpowiednie gremia, a prawnicy wyznaczą dopuszczalne prawem działania. Sztuczna inteligencja mości się po cichutku w coraz nowych miejscach, ba, coraz częściej doświadczamy jej efektów na co dzień.

Do tej pory klonowanie głosu kojarzyło się nam z filmikami na YouTubie, w których znani aktorzy posługiwali się biegle np. mandaryńskim. Zanurzeni w uniwersum „Gwiezdnych wojen" odnotowali zapewne, że zsyntetyzowano głos młodego Luke'a Skywalkera w „Mandalorianinie", a głos obecnego 93-latka Jamesa E. Jonesa użyczającego głosu postaci lorda Dartha Vadera będzie nadal wykorzystywany w innych produkcjach cyklu właśnie za sprawą sztucznej inteligencji. W obu przypadkach wykorzystano rozwiązania ukraińskiej firmy Respeecher, stosującej m.in. techniki uczenia maszynowego do naśladowania głosu.

Fani polskiego serialu „Rojst" w jego ostatnim sezonie także mogli doświadczyć efektów działań specjalistów Respeechera, którzy zmiksowali kwestie wypowiadane przez aktora Filipa Pławiaka (grającego młodego Kociołka, szefa hotelu) z głosem Piotra Fronczewskiego z lat 70. ub. w., grającego w serialu tę postać w wieku dojrzałym. Wszystko po to, żeby w oczach widzów uwiarygodnić ciągłość historyczną bohatera.

Tak uwodzeni widzowie są jednocześnie mimowolnymi świadkami zupełnie innego serialu – wieloodcinkowej walki twórców o tantiemy z tytułu prezentowania ich dzieł w streamingu. Te zmagania nie są pozbawione lokalnego kolorytu. Tylko u nas twórcy nie otrzymują tantiem z internetu, bo Polska dotąd nie wprowadziła unijnej dyrektywy, mimo że termin upłynął już w połowie 2021 r. Dziwnym zbiegiem okoliczności prace nad implementacją wstrzymano pod koniec 2022 r. po wizycie szefa Netflixa w Polsce i jego spotkaniu z ówczesnym premierem Morawieckim. Na początku lutego br. Stowarzyszenie Filmowców Polskich złożyło w prokuraturze zawiadomienie o podejrzeniu popełnienia przestępstwa przez funkcjonariusza państwowego. Sztuczna inteligencja z pewnością nie pisała tego scenariusza …

*Anna Kniaź*
redaktor naczelna

# Wyścig w eksaskali

**Najpotężniejsze superkomputery pozwalają modelować działanie broni jądrowej, projektować lepsze samoloty, odkrywać nowe materiały i tworzyć nieznane wcześniej substancje chemiczne i leki. Ich rosnącą rolę strategiczną odzwierciedla rozpoczęcie nowego etapu wyścigu w kategorii wydajności – tym razem w eksaskali, czyli szybkości liczonej w trylionach operacji na sekundę.**

Według listy TOP500 najszybszym obecnie komputerem na świecie jest uruchomiona w 2022 r. maszyna o nazwie Frontier, działająca w Oak Ridge National Laboratory. Kosztowała co najmniej 600 mln dolarów, jednak jej możliwości przekraczają daleko to, co oferują starsze superkomputery. Frontier jest pierwszym superkomputerem działającym w eksaskali, a jego moc obliczeniowa przekracza jeden eksaflops. Skrót FLOPS (Floating Point Operations per Second) oznacza operacje zmiennoprzecinkowe na sekundę – to obecnie standardowa miara wydajności obliczeniowej komputerów. Eksaflops (EFLOPS) to zatem wydajność przekraczająca granicę tryliona (10 do potęgi 18) operacji zmiennoprzecinkowych na sekundę.

**Piotr Kościelniak**
dziennikarz, popularyzator nauki

To wielkości wymykające się naszej normalnej, codziennej mierze rzeczy. „Gdyby każdy człowiek na Ziemi mógł wykonać jedno takie działanie na sekundę, wszystkim nam zajęłoby cztery lata, aby zrobić to, co ten komputer robi w jedną sekundę" – tłumaczy twórca listy TOP500, Jack Dongarra z Uniwersytetu Tennessee na łamach „MIT Technology Review".

Przekroczenie granicy jednego eksaflopsa pozwoli prowadzić symulacje i obliczenia wcześniej nieosiągalne dla naukowców – od modelowania złożonych zjawisk związanych z klimatem, przez interakcje białek, obliczenia astrofizyczne, po rozwijanie możliwości sztucznej inteligencji, medycyny, transportu, energetyki i uzbrojenia. To jednocześnie ogromny impuls rozwojowy dla nauki i gospodarki. Analizy makroekonomiczne wskazują, że w USA każdy dolar zainwestowany w takie systemy przynosi 47 dolarów w zyskach lub oszczędnościach.

Nic dziwnego, że instalacjami takimi interesują się praktycznie wszyscy. Amerykanom depczą już po piętach Chiny, które mimo obowiązującego embarga na najnowsze technologie konstruują superkomputery o najwyższej wydajności. Budzi się również Europa, dostrzegająca znaczenie analizy danych i pragnąca budować własne („suwerenne") instalacje. Wiele spośród projektowanych superkomputerów w eksaskali ma zostać oddanych do użytku w ciągu najbliższych 12 miesięcy. Dla wyścigu o dominację obliczeniową to właśnie 2024 r. będzie decydujący.

## Mój komputer jest większy niż twój

Na swój sposób wyścig superkomputerów przypomina wyścig supermocarstw w kosmosie – tyle że liczą się w nim USA i Chiny, a nie Rosja. Inwestowane są miliardy dolarów, angażowani najzdolniejsi naukowcy, a megakorporacje walczą o prawo dostarczania podzespołów do najnowszych konstrukcji.

> *Co jeszcze bardziej upodabnia wojny eksaskalowe do podboju kosmosu to fakt, że uczestniczą w nim de facto państwa – i to w sytuacji, gdy rakietami i pojazdami załogowymi już od dawna zajmują się w USA firmy prywatne.*

Na pierwszy rzut oka to zaskakujące – szarym skrzynkom z procesorami daleko do chwały i sławy lotów w kosmos. W rzeczywistości jednak, pomijając kwestie dumy narodowej, superkomputery niosą ze sobą dziś równie istotne, a może nawet większe implikacje dla bezpieczeństwa narodowego, energetycznego i postępu naukowego niż budowa komponentów stacji kosmicznych. To od szybkości obliczeń zależy, kto pierwszy odkryje możliwości egzotycznych materiałów, opracuje nowy typ akumulatora, skonstruuje mniejszy i wydajniejszy reaktor atomowy, stworzy bezpieczny algorytm szyfrowania.

Wiele superkomputerów zainstalowanych w ośrodkach administrowanych przez rządy państw pracuje obecnie nad symulacjami działania broni nuklearnej, co ponownie upodabnia wyścig eksaskalowy do wyścigu zbrojeń w latach 60. i 70. XX w. O ironio – przyczynił się do tego w 1996 r. Traktat o całkowitym zakazie prób z bronią jądrową (CTBT). Zamiast testować nowe rodzaje broni w warunkach rzeczywistych, naukowcy i wojskowi sięgnęli po symulacje. A do tych potrzebne były coraz szybsze superkomputery…

Najpotężniejsze superkomputery to również megaprojekty, choć nie projektują ich światowej sławy architekci ani nie ozdabiają artyści. Popatrzmy na maszynę o nazwie Summit, pięć lat temu najszybszy superkomputer świata, dziś wyprzedzony przez sześć innych maszyn. Dostarczony przez IBM superkomputer zainstalowany jest w Oak Ridge National Laboratory w Tennessee i należy do amerykańskiego Departamentu Energii. Zajmuje blisko 900 metrów kwadratowych, wymaga mocy 13 MW, 220 kilometrów bieżących okablowania, a przez jego układ chłodzenia przepływa 15 tys. litrów wody na minutę. Nic dziwnego – pracuje w nim 9216 procesorów IBM Power9 o 22 rdzeniach każdy, które wspierane są przez 27 648 procesorów Nvidia Tesla V100. Jego budowa zajęła cztery lata.

Budowa superkomputerów w nowej skali oznacza również ogromne koszty. Działający pod kontrolą amerykańskiego Departamentu Energii program ECP (Exascale Computing Project) zakładał na prace przygotowawcze (tzw. program PathForwards) sumę 258 mln dolarów. Koszty te podzieliły między siebie firmy AMD, Cray, HPE (Hewlett Packard Enterprise), IBM, Intel i Nvidia, co pokazuje, że wyzwanie budowy najszybszych komputerów świata traktowane jest raczej jako wyzwanie cywilizacyjne, narodowe niż jako kolejny projekt rynkowy.

Koszty to tylko część problemów, które pojawiają się podczas realizacji wyzwania w takiej skali. Architektura sieci, pamięci, magazynowanie danych, oprogramowanie systemu plików, zużycie energii, a nawet konkurencyjność kosztowa – wszystko to kwestie, które przy tej skali projektów trzeba rozwiązywać w zupełnie inny sposób niż przy mniejszych instalacjach.

„Wiele osób myśli, że budowanie superkomputerów to takie ćwiczenie w dziedzinie inżynierii sprzętowej, że jest to absolutnie trywialne. Ale istnieją pewne subtelności, z których te osoby nie zdają sobie sprawy. Na przykład jesteś administratorem systemu i w jakiś sposób zarządzasz

10 tysiącami węzłów. Czy masz ekran, który pokazuje, co się z nimi dzieje? W jaki sposób je porządkujesz, jak zarządzasz alertami? Jak zarządzasz działaniem systemu, w którym jest tyle informacji z każdego komponentu?" – tłumaczył Dave Turek z IBM w rozmowie z serwisem Data Centre Dynamics.

Frontier jest oficjalnie pierwszym eksaskalowym superkomputerem, jednak wkrótce pokonają go dwie kolejne amerykańskie maszyny. Z pełną mocą mają ruszyć w 2024 r. Pierwsza to uruchomiona w czerwcu 2023 r. z częścią projektowanych zasobów Aurora w Argonne National Laboratory w stanie Illinois. Pierwszym zadaniem tego superkomputera będzie symulacja działania neuronów w mózgu człowieka – coś, co jeszcze do niedawna wydawało się nieosiągalnym celem ze względu na złożoność połączeń między neuronami. Drugim superkomputerem będzie El Capitan w Lawrence Livermore Laboratory w Kalifornii. Ta maszyna ma służyć do symulacji działania broni nuklearnej. Oficjalnie – aby utrzymać zdolności bojowe Stanów Zjednoczonych bez konieczności prowadzenia rzeczywistych testów takiej broni.

## Przyczajony tygrys

Chiny zapowiedziały budowę własnego superkomputera nowej generacji w 2020 r., co dawałoby temu krajowi przewagę nad amerykańskimi konkurentami. Dziś wiadomo o co najmniej dwóch działających chińskich maszynach o tak dużej mocy obliczeniowej – Sunway TaihuLight w Narodowym Centrum Superkomputerowym w Wuxi i Tianhe-3 w Tiencin. Wcześniejsze wersje tych maszyn są uwzględniane w zestawieniu TOP500, jednak oczywiście z niższymi parametrami wydajności. Trzeci ma powstawać (być może już powstał i działa) w Shenzhen.

Według „Financial Times", o ile Amerykanie w tym roku chcą mieć trzy funkcjonujące superkomputery tej klasy, o tyle Chiny zamierzają dysponować aż dziesięcioma do końca 2025 r. Łączna moc obliczeniowa wszystkich chińskich maszyn ma w przyszłym roku przekroczyć 300 EFLOPS. Według sieci CNBC, obecnie szacunkowa łączna moc obliczeniowa chińskich superkomputerów to 190–200 EFLOPS. Wartość ta jest jednak szeroko dyskutowana przez ekspertów – nie potwierdzają jej na razie badania prowadzone na potrzeby TOP500.

Wątpliwości budzą również szacowane koszty takich inwestycji. Opierając się na przybliżonych kosztach budowy superkomputerów o wydajności przekraczającej 1 EFLOPS, takich jak Frontier czy El Capitan, dołożenie łącznej mocy obliczeniowej o wartości 100 EFLOPS wymagałoby nakładów o wartości od 30 do 50 mld dolarów.

Na nowej chińskiej strategii, ogłoszonej oficjalnie w październiku 2023 r., najbardziej skorzystają giganci, tacy jak Alibaba i Tencent. Plan rządu obejmuje skupienie się na udoskonaleniach pamięci masowej i ulepszonej infrastrukturze transmisji danych oraz utworzenie dodatkowych centrów danych. Zmiany te mają kluczowe znaczenie dla usług przetwarzania w chmurze – domeny kluczowej dla AI.

Nie jest jeszcze jasne, jaki rodzaj sprzętu zostanie wykorzystany do zbudowania ponad 100 EFLOPS dodatkowej mocy obliczeniowej w tak krótkim czasie. Te problemy to efekt nałożonych przez Stany Zjednoczone sankcji, które nadwyrężyły chiński łańcuch dostaw technologii, szczególnie w zakresie dostępu do procesorów takich firm, jak AMD, Intel i Nvidia. Chociaż największy chiński producent półprzewodników SMIC (Semiconductor Manufacturing International Corporation) jest w stanie zbudować dość wyrafinowane procesory dla smartfonów, nie ma możliwości zbudowania tak zaawansowanych układów, jak te Intela czy Nvidii wykorzystywane do budowy węzłów superkomputerów. W rezultacie eksperci uważają, że amerykańskie sankcje, zwłaszcza te wpływające na dostęp do najwyższej klasy chipów dla AI i HPC (*High Performance Computing*), w przyszłości nadal będą stanowić istotne przeszkody dla Chin.

To również jedna z przyczyn, dla których Chińczycy nie chwalą się swoimi najnowszymi superkomputerami na liście TOP500. „Obawiają się kolejnych sankcji w obszarze technologii nakładanych na chińskie firmy i nie chcą ujawnić, ile takich superwydajnych maszyn mają już teraz do dyspozycji" – przyznał Jack Dongarra w rozmowie z „MIT Technology Review".

Ten wzrost mocy obliczeniowej to nie tylko kwestia dumy narodowej. Rząd chiński uznaje kluczową rolę zaawansowanych obliczeń w różnych sektorach, zwłaszcza w finansach i edukacji. Sukcesy dotychczasowych przedsięwzięć w tym obszarze sugerują, że inwestycje Chin w infrastrukturę obliczeniową przynoszą znaczne zyski gospodarcze. Według analityków firmy Counterpoint każdy juan wydany na zwiększenie możliwości obliczeniowych kreuje zysk od trzech do czterech juanów.

## Europa odrabia straty

W pierwszej dziesiątce najnowszego wydania listy TOP500 (dane z lutego 2024 r.) zmieściły się trzy maszyny ulokowane w Unii Europejskiej. Najszybsza jest LUMI (zmierzona wydajność to 309 petaflopsów) zbudowana kosztem blisko 150 mln euro w fińskim Kajaani przez HPE. Na liście TOP500 jest obecnie na piątym miejscu. Tuż za LUMI plasuje się Leonardo (238 PFLOPS) we włoskiej Bolonii, zbudowany przez francuską firmę Atos Leonardo. Co ciekawe, mimo niższej wydajności, jest o blisko 100 mln dolarów droższy niż LUMI. Na ósmym miejscu listy TOP500 znajduje się MareNostrum 5 (138 PFLOPS) ulokowany w Barcelonie.

> *Wszystkie te superkomputery zbudowane zostały w ramach europejskiego programu European High-Performance Computing Joint Undertaking (EuroHPC JU) – partnerstwa publiczno-prywatnego, którego celem jest rozwój nowych technologii związanych z przetwarzaniem danych. Publicznym partnerem w tym przedsięwzięciu jest również Polska. Program dysponuje budżetem w wysokości 7 mld euro na lata 2021–2027.*

Środki te zostały zadeklarowane w Wieloletnich Ramach Finansowych oraz programach Digital Europe i Horizon Europe. Początkowo europejski program zakładał ulokowanie finansowanych przez siebie ośrodków obliczeniowych w ośmiu krajach. Oprócz wspomnianych już Finlandii, Włoch i Hiszpanii, to również Bułgaria, Czechy, Luksemburg, Portugalia i Słowenia. W 2022 r. ogłoszono kolejnych pięć państw członkowskich, które zyskają dostęp do finansowania superkomputerów: Grecja, Węgry, Irlandia oraz Polska. Piątym krajem są Niemcy – i nie powinno być dla nikogo niespodzianką, że to właśnie tam powstanie pierwszy europejski superkomputer w eksaskali. Maszyna o nazwie JUPITER (*Joint Undertaking Pioneer for Innovative and Transformative Exascale Research*) ma działać w Forschungszentrum Jülich między Düsseldorfem i Akwizgranem. Również ten projekt ma zostać uruchomiony w 2024 r.

## Polska w drugiej setce

Gdzie w tym wszystkim lokuje się Polska? Niestety – dość daleko.

Przed rokiem z wielką pompą uruchomiono w Centrum Kompetencji STOS w Gdańsku superkomputer Kraken. Ma służyć do prowadzenia prac nad rozwojem algorytmów sztucznej inteligencji, energetyką jądrową(!), medycyną, farmacją czy ochroną środowiska. Jego planowana moc obliczeniowa to 13,6 PFLOPS, co czyniłoby go najszybszym komputerem w Polsce i jednym z najszybszych w Europie. Według prognoz znalazłby miejsce w pierwszej setce listy TOP500.

Nawet jednak biorąc pod uwagę pojawienie się Krakena w jednym z kolejnych zestawień, pozycja Polski nie zmieni się znacząco. Wyścig w tej dziedzinie – i spodziewane korzyści naukowe i gospodarcze – możemy podziwiać z drugiego rzędu. I nie dotyczy to tylko wyścigu potęg – USA i Chin, lecz również wyzwań w skali lokalnej – europejskiej.

**Na liście z listopada 2023 r. (62. edycja) jeszcze Krakena nie ma. Według tego zestawienia do 500 najszybszych maszyn świat wchodzą tylko cztery polskie superkomputery. Najszybsza jest oddana do użytku w 2022 r. Athena (5,05 PFLOPS) w Akademickim Centrum Komputerowym Cyfronet AGH w Krakowie. Obecnie zajmuje ona 155. miejsce. Na 221. miejscu uplasował się Altair w Poznańskim Centrum Superkomputerowo-Sieciowym (PCSS) z wydajnością na poziomie 3,53 PFLOPS, a na 291. miejscu znalazł się kolejny superkomputer Cyfronetu – Helios (2,89 PFLOPS). Listę polskich maszyn w najnowszym wydaniu TOP500 zamyka Ares (miejsce 404 i wydajność 2,34 PFLOPS), także z ACK Cyfronet AGH. Oczywiście w Polsce działają również liczne mniejsze lub starsze superkomputery, które już nie mieszczą się na liście 500 najszybszych superkomputerów świata.**

## Po co nam ta moc

Wykorzystanie zasobów superkomputerów jest bardzo wysokie – na poziomie 90 proc. dostępnej mocy obliczeniowej. Opisywany Frontier pracuje z niemal pełną wydajnością 24 godziny na dobę, siedem dni w tygodniu, a zadania od zespołów naukowych przyjmuje przez internet. Dane i modele przechowywane są lokalnie w magazynach o pojemności ok. 700 petabajtów, co jest odpowiednikiem mniej więcej półtora miliona dysków w dzisiejszych laptopach.

Co robi taki eksaskalowy superkomputer na co dzień? Na przykład Evan Schneider z Uniwersytetu w Pittsburghu wykorzystuje go do zbudowania komputerowego modelu Drogi Mlecznej o wystarczająco dużej rozdzielczości, aby umożliwić przybliżanie poszczególnych eksplodujących gwiazd. Oznacza to, że model musi reprezentować elementy naszej galaktyki z wielką dokładnością, np. otoczenie supernowych w skali ok. 10 lat świetlnych. Przekładając to na „ludzką" skalę: to wyzwanie na miarę stworzenia fizycznie dokładnego modelu puszki piwa wraz ze znajdującymi się w niej pojedynczymi komórkami drożdży oraz wszystkimi interakcjami pomiędzy nimi.

Naukowcy korzystają również z mocy obliczeniowej superkomputera w eksaskali do symulacji kontrolowanej syntezy termojądrowej czy zachowania cząsteczek w koronie Słońca. Błędem byłoby jednak przekonanie, że super-

komputery rozwiązują problemy, które nie mają żadnego znaczenia dla codziennego życia zwykłych ludzi. Jednym z ich najczęstszych zastosowań jest modelowanie struktur chemicznych i biochemicznych, prowadzących do wytwarzania nowych materiałów czy kandydatów na nowe leki. Szczegółowe modelowanie pogody i zjawisk atmosferycznych pozwala natomiast precyzyjnie ocenić, w jaki sposób zmiany klimatu mogą wpływać na efektywność rolnictwa i całego przemysłu spożywczego.

Na superkomputerach prowadzone są także badania aerodynamiczne, materiałowe i hydrodynamiczne pozwalające konstruować lepsze skrzydła samolotów, czy kadłuby okrętów. Na przykład inżynierowie GE korzystają z mocy Frontiera do badania efektywności silników lotniczych. Już teraz uzyskano wyniki symulacji dotyczące rozmiaru i kształtu łopatek, które mogą całkowicie odmienić kształt silników odrzutowych i skrzydeł samolotów – będą bardziej efektywne energetycznie i cichsze. Wcześniej prowadzenie symulacji tego typu było niemożliwe, ponieważ superkomputery nie były w stanie odpowiednio modelować turbulencji (zaburzonego przepływu powietrza), których efekty mają decydujące znaczenie dla pracy silników lotniczych. Aby prowadzić takie badania, niezbędne było eksperymentowanie w tunelu aerodynamicznym. Superkomputer operujący w eksaskali jest w stanie przeprowadzić takie operacje w krótszym czasie i taniej.

Superkomputery wykorzystuje także Goodyear, projektując nowe mieszanki do opon oraz kształt bieżnika. Aby opracować i wprowadzić na rynek jeden model opony, firma wykonuje symulowane testy blisko 300 różnych prototypów. Analizy numeryczne wykonane przy użyciu superkomputerów umożliwiają szybsze opracowanie ostatecznego produktu oraz przetestowanie go, co przy użyciu konwencjonalnych metod byłoby niemożliwe lub dużo kosztowniejsze.

## Co dalej?

Powstaje jednak pytanie, jak długo jeszcze możliwe będzie konstruowanie coraz szybszych superkomputerów przy użyciu obecnie dostępnych rozwiązań. Problemem jest bowiem konieczność wykorzystywania coraz większej liczby rdzeni (procesorów), zużywających coraz więcej energii i wymagających kosztownych (i nieekologicznych) instalacji chłodzenia oraz systemów do zarządzania, jak również nowych technologii przesyłania i składowania coraz większych ilości danych.

Naukowcy z Oak Ridge National Laboratory już myślą o kolejnej generacji superkomputerów – pięć razy wydajniejszych niż Frontier. Największym problemem nie są jednak pieniądze ani ograniczenia procesorów, ale kolosalne zużycie energii. Już Frontier zużywa jej tyle, że wystarczyłoby to do zasilenia niewielkiego miasteczka, a około 4 proc. całego jej zużycia służy wyłącznie do… chłodzenia. To i tak lepszy wynik niż w przypadku maszyny wcześniejszej generacji – superkomputera Summit, który do 2020 r. był najszybszym na świecie (obecnie znajduje się na miejscu 7.). Summit zużywa 10 proc. całej energii wyłącznie na chłodzenie wody.

Gwałtowne przyspieszenie superkomputerów obiecuje jednak firma Tachyum. Twierdzi, że jej nowe procesory serii Prodigy zasilą projektowany obecnie superkomputer o mocy przetwarzania zbliżonej do 50 EFLOPS, czyli 25 razy szybszego niż budowane dziś superkomputery w rządowych ośrodkach badawczych w USA. Problem z zapowiedziami Tachyum polega jednak na tym, że procesorów Prodigy nikt nigdy nie widział – istnieją na razie tylko jako symulacje na innych komputerach.

## Kwantowy przypływ

Wszystkie te problemy wokół kolejnych generacji superkomputerów opartych na konwencjonalnej architekturze bledną jednak wobec nowej technologii wyłaniającej się już zza horyzontu. Chodzi o komputery kwantowe, które już teraz zaczynają zdobywać pozycję na rynku komercyjnym. Działają one w zupełnie inny sposób niż maszyny wykorzystujące półprzewodnikowe układy scalone (więcej o takich konstrukcjach można przeczytać w magazynie „Domena" nr 3/2022). W największym skrócie – takie komputery obliczają wszystkie warianty w jednym cyklu, podczas gdy w klasycznym rozwiązaniu komputery liczą wszystko po kolei. Najważniejsze jest jednak to, że komputery kwantowe są w stanie rozwiązywać pewne kategorie problemów w czasie nieporównywalnie krótszym niż najpotężniejsze superkomputery o tradycyjnej architekturze.

Komputery kwantowe, ze względu na charakterystykę działania, mogą znacznie skrócić symulacje różnych wariantów złożonych systemów, np. w biologii i chemii, co przekłada się na jeszcze szybsze odkrycia w dziedzinie inżynierii materiałowej i lekowej. Mogą również posłużyć do optymalizacji procesów w logistyce, zarządzaniu i finansach, a także wprowadzić systemy uczenia maszynowego (tzw. sztucznej inteligencji) na niespotykany wcześniej poziom.

Najwięcej emocji komputery kwantowe wzbudzają jednak wśród ekspertów ds. cyberbezpieczeństwa. Ich wykorzystanie w praktyce oznacza, że dotychczasowe metody szyfrowania stosowane w przesyłaniu i przechowywaniu danych w jednej chwili okażą się nieskuteczne. Dlatego ich wprowadzenie może przynieść w sferze IT większą rewolucję niż internet czy AI. Oczywiście nie brakuje również sceptyków, którzy wskazują (słusznie) na problemy w konstruowaniu i utrzymywaniu sprawności takich maszyn, potencjalne błędy w kalkulacjach czy trudności z dopasowaniem znanych algorytmów do całkowicie nowej zasady działania komputerów kwantowych.

Obecnie takimi urządzeniami dysponują m.in. firmy: IBM, D-Wave, Intel, Google, Rigetti czy IQM. Interesują się nimi również sieciowi giganci, tacy jak Amazon, Microsoft czy Baidu. W tej chwili jednak komputery kwantowe traktowane są raczej jako dowód na poprawność idei niż pełnoprawny instrument prowadzenia badań. Od tego momentu dzielą nas jednak nawet nie lata, ale miesiące. Już w 2019 r. Google AI Quantum ogłosił, że komputer kwantowy rozwiązał zadany problem ok. 3 mln razy szybciej niż najszybszy wówczas superkomputer Summit. Rok później chińscy naukowcy opublikowali wyniki obliczeń z dziedziny fizyki, które zajęły komputerowi kwantowemu ok. 20 sekund. Konwencjonalny superkomputer potrzebowałby na ich ukończenie – twierdzili Chińczycy – 600 mln lat.

Technologiami kwantowymi interesują się również polscy naukowcy – prace takie prowadzone są od dłuższego czasu w Poznaniu. W listopadzie 2023 r. otwarto koperty z ofertami w przetargu na dostawy komputera kwantowego dla Poznańskiego Centrum Superkomputerowo-Sieciowego w ramach inicjatywy finansowanej przez EuroHPC Joint Undertaking. Mogły w nim brać udział wyłącznie firmy z Europejskiego Obszaru Gospodarczego. Pierwsze dwa komputery kwantowe w ramach projektu EuroHPC JU – dla Francji i Niemiec – dostarczyła francuska firma Pasqal. W sumie do 2025 r. w Unii Europejskiej ma powstać sześć komputerów kwantowych finansowanych ze środków unijnych.

Jednocześnie jednak rząd wstrzymał dotacje w wysokości 200 mln zł na Centrum Nowych Technologii i Innowacji Politechniki Poznańskiej, gdzie również miały być prowadzone prace nad komputerem kwantowym, powołując się upolitycznienie decyzji o przyznawaniu wsparcia dla uczelni przez poprzednią ekipę. Trzeba mieć tylko nadzieję, że decyzja ta nie oznacza, że Polska ponownie, zamiast uczestniczyć w wyścigu, będzie się mu tylko przyglądać.

### Lista TOP500

**To najpoważniejszy i najszerzej uznawany ranking najszybszych komputerów świata. Powstał w 1993 r. jako odpowiedź na rosnące znaczenie superkomputerów i konieczność obiektywnego mierzenia ich wydajności. Służy do tego wzorcowy test Benchmark LINPACK opracowany przez Jacka Dongarrę z Uniwersytetu Tennessee, mierzący szybkość rozwiązywania równań liniowych, które odzwierciedlają standardowe zadania w pracach naukowych. Wynikiem jest liczba operacji zmiennoprzecinkowych na sekundę, czyli FLOPS. Metoda ta zastąpiła starszy sposób szacowania wydajności, oparty na milionach instrukcji na sekundę, czyli MIPS, stosowany jeszcze w latach 70. ubiegłego wieku.**

**Ostateczny ranking oparty na tych testach kompilowany jest przez Jacka Dongarrę oraz Ericha Strohmaiera i Horsta Simona z National Energy Scientific Computing Center i Lawrence Berkeley National Laboratory. Rankingi publikowane są dwukrotnie w ciągu roku – w czerwcu na International Supercomputing Conference oraz w listopadzie podczas ACM/IEEE Supercomputing Conference. Dane w tym artykule odnoszą się do 62. edycji rankingu, opublikowanego oficjalnie 13 listopada 2023 r.**

**Lista, jak wskazuje nazwa, obejmuje 500 superkomputerów – nie obejmuje natomiast systemów rozproszonych, maszyn, na których nie można uruchomić testów LINPACK, ani też superkomputerów, których administratorzy nie chcą testować i oficjalnie ogłaszać wyników. Sam ranking jest publicznie dostępny na stronie top500.org.**

**Co ciekawe, wzrost wydajności superkomputerów zajmujących pierwsze miejsca na liście Top500 potwierdza prawdziwość słynnego prawa Moore'a, mówiącego o liczbie tranzystorów w układzie scalonym podwajającej się w równych odstępach czasu oraz wniosku z niego, że moc obliczeniowa komputerów podwaja się co 24 miesiące (w przypadku pierwszego miejsca na liście to w rzeczywistości 14 miesięcy).**

**Na danych prezentowanych na liście TOP500 opiera się inny ranking superkomputerów – lista Green500. Prezentuje ona efektywność energetyczną superkomputerów (GFLOPS/waty). Obecnie najwydajniejszy pod tym względem jest superkomputer Henri, działający w amerykańskim Flatiron Institute. Innym sposobem oceniania wydajności superkomputerów jest test wykorzystywany w rankingu Graph500.**

# Jak uzdrowić cyfrowe usługi publiczne

*Od lewej: Marek Hołyński, Krzysztof Komorowski, Michał Przymusiński, Danuta Kajrunajtys, Tadeusz A. Grzeszczyk.*


*Od lewej: Jakub Groszkowski, Wiesław Paluszyński.*

**Od ponad 40 lat Polskie Towarzystwo Informatyczne próbuje na sprawy informatyki patrzeć szerzej niż tylko poprzez jakość wytwarzanego oprogramowania. Martwią nas jednak ewidentne problemy z cyfrowymi usługami publicznymi, dlatego tematowi jakości aplikacji poświęciliśmy pierwsze z cyklu planowanych spotkań branżowych. Mamy nadzieję, że głos profesjonalistów będzie pomocny w stopniowym poprawianiu sytuacji.**

Zaniepokojenie budzą nie tylko przesunięcia uruchomienia systemów e-doręczeń czy Krajowego Systemu e-Faktur (KSeF). – „Mamy do czynienia z wielowymiarowym problemem na poziomie państwa. Jest duży kłopot z jakością usług cyfrowych bazujących na aplikacjach, przy czym ta jakość oznacza nie tylko jakość techniczną czy w sensie *user experience* (czyli komfortu użytkownika), ale ma też głębsze aspekty. Niejednokrotnie mamy do czynienia z niejasnym albo sprzecznym wewnętrznie procesem biznesowym, który aplikacja ma prowadzić. Jak się na to nałoży oczywiste niechlujstwo w obszarze doświadczenia użytkownika, to jest on bez szans" – rozpoczął dyskusję prowadzący spotkanie Krzysztof Komorowski (informacja o uczestnikach debaty w ramce).

## Uczestnicy debaty

- **Jakub Groszkowski, zastępca Prezesa Urzędu Danych Osobowych**
- **Tadeusz A. Grzeszczyk, profesor uczelni w Politechnice Warszawskiej i Visiting Researcher w Sano Centre for Computational Medicine**
- **Marek Hołyński, absolwent Wydziału Elektroniki Politechniki Warszawskiej, profesor Uniwersytetu Bostońskiego oraz były samodzielny pracownik naukowy MIT i dyrektor Instytutu Maszyn Matematycznych w Warszawie**
- **Danuta Kajrunajtys, wieloletni nauczyciel akademicki i doradca biznesowy, rzeczoznawca Polskiego Towarzystwa Informatycznego, niezależny doradca w zakresie wykorzystania informatyki w zarządzaniu**
- **Krzysztof Komorowski, były fizyk jądrowy, w branży IT od końca XX w., prowadził działy konsultingowe w Computerlandzie i IBM, partner w firmie project-managerskiej i konsultingowej Eprom**
- **Wiesław Paluszyński, prezes PTI**
- **Michał Przymusiński, ekspert e-usług publicznych, wdrażał m.in. portal www.gov.pl, systemy obsługi pandemii COVID-19, zarządzania kryzysowego państwa oraz rozwiązania e-usługowe dla mediów m.in. TVP i HBO.**

Tym problemom towarzyszy rodzaj publicznej bezradności. Gdy most ma dziury lub się wali, obywatele alarmują, władza reaguje, wykonawca odpowiada karnie, jeśli zawinił. Natomiast jak nie działa usługa publiczna, to wprawdzie przyznajemy, że jest problem, ale za komentarz często służy słynne powiedzenie „taki mamy klimat".

Michał Przymusiński mógł obserwować, co się działo z usługami w pandemii, bo w Ministerstwie Cyfryzacji robiono wówczas rozwiązania centralne. – „Polska to nie Indie, kiedy mamy potężny ruch, to do obsłużenia w tym samym czasie jest ok. 150 tys. użytkowników.

Z inżynierskiego punktu widzenia jest to absolutnie wykonalne, jak to się więc dzieje, że nie możemy obsłużyć wpisów w KRS, kiedy przedsiębiorcy tego potrzebują?" – zastanawiał się i postawił diagnozę:

> *„Problem jest dwojaki. Po pierwsze jakość używanych rozwiązań, często bazujących na gotowych bibliotekach, których programiści nie znają i nie rozumieją, jak działają (co wpływa na wydajność). Po drugie – mentalnie skupiamy się na aplikacji, jej wyglądzie, interfejsie. Tymczasem tak naprawdę kluczowa jest prawdziwa cyfryzacja procesu".*

Efektywna cyfryzacja procesu czasem po prostu sprawia, że użytkownik nie musi niczego robić, nie musi korzystać z żadnej aplikacji, bo system wykonuje wszystkie operacje za niego.

### Pochodna słabości państwa

Danuta Kajrunajtys zwróciła uwagę, że usługi publiczne, przeznaczone dla osób fizycznych, nadal są projektowane i tworzone z perspektywy urzędnika, który dotąd fizycznie korzystał z systemu. – „Ja mam jeszcze inne wątpliwości. Nie widzę powodu, dlaczego akurat zarządzanie usługami publicznymi miałoby być na wyższym poziomie niż zarządzanie czymkolwiek innym w Polsce. Nie mamy strategii czy polityk praktycznie w żadnej dziedzinie. Usługi publiczne, o których tutaj mówimy, są tylko interfejsem do nieuporządkowanych obszarów państwa. Przykład: prawo podatkowe czy prawo ubezpieczeń społecznych liczą po kilkadziesiąt tysięcy stron często nieprecyzyjnych i niespójnych przepisów i w zasadzie przestały być algorytmizowalne" – diagnozował Krzysztof Komorowski.

– „Jeżeli chcemy coś zrobić, to najpierw określamy, dla kogo chcemy to zrobić, jakie są oczekiwania tego odbiorcy. Jakie są inne kryteria związane z tą usługą od strony kosztów, utrzymania, rozwoju? PTI powinno pracować na rzecz ugruntowania świadomości znaczenia dobrej analizy wymagań we wszystkich przedsięwzięciach" – podkreślała Danuta Kajrunajtys.

Na ostateczny rezultat rzutuje też brak badań przed uruchomieniem projektu cyfrowych usług publicznych, ale to nie tylko polska przypadłość. – „Zespół, którym kierowałem brał udział w spotkaniu w sprawie Single Digital Gateway (jednolitego portalu cyfrowego ułatwiającego dostęp online do informacji, procedur administracyjnych i usług pomocniczych, których potrzebują obywatele i przedsiębiorcy, aby prowadzić działalność w innym państwie UE). Delegacja polska zapytała o badania, które są istotne, bo przecież robimy centralny system usługowy dla obywateli Unii (który np. ma ułatwić uruchomienie biznesu w Polsce Portugalczykowi). To nie jest zadanie trywialne, my nie wiemy, jaką oni mają u siebie specyfikę. Okazuje się, że to

w ogóle nie zostało zbadane" – opowiadał Michał Przymusiński. I dodał, że z badaniami u nas nie zawsze jest tak źle. Swojego czasu intensywnie zajmował się badaniami obszaru edukacji i nauki. Wówczas w badaniach uczestniczyło 162 tys. respondentów podzielonych na 34 grupy – od ucznia szkoły podstawowej po rektora i w każdej z tych grup pytano o potrzeby. Z uzyskanych danych powstało 38 badań i ponad 70 raportów.

## Tęsknota za prawem budowlanym

– „Kiedyś na swoim profilu na LinkedIn napisałem, że powinno się wprowadzić w cyfrowych usługach publicznych takie prawo budowlane jak przy budowie mostu. Ten post miał 12 tys. odsłon i to był mój najlepszy wynik. Co więc możemy sensownego zrobić?" – pytał Krzysztof Komorowski.

– „Klęska e-faktur nie jest dla mnie zaskoczeniem, bo jako PTI robiliśmy ekspertyzę przy pierwszym wdrożeniu systemu w Ministerstwie Finansów. Mamy do czynienia z prymatem nieformalnych sposobów działania nad „prawem budowlanym" w informatyce, bo go nie ma.

> *Nie mamy w informatyce systemów nadzoru.*

Czy przy budowie elementów, od których zależy przyszłość obywateli, ich sposób działania, koszty przedsiębiorstw ta wolna amerykanka powinna dalej istnieć?" – zastanawiał się Wiesław Paluszyński.

Zdaniem Michała Przymusińskiego, gdyby istniał inżynier kontraktu, to zamawiane komponenty mogłyby być używane w wielu projektach, co przyniosło by potężną zmianę jakościową, bo uwspólnianie doświadczeń prowadzi do doskonalenia. – „Niedawno dostaliśmy do przejrzenia duży, nietani system publiczny. Mówimy administratorowi, że jedno z zapytań do bazy trwa 26 sekund, dlatego system nie działa dobrze. Okazało się, że wzięli gotową bibliotekę i nie zoptymalizowali, bo w ogóle nie wiedzą, jak ta biblioteka działa. Ktoś to rozwiązanie napisał, klient odebrał, więc ewidentnie zabrakło inżyniera nadzoru".

## Państwowa niechęć do mechanizmów rynkowych

Zdaniem Krzysztofa Komorowskiego, jednym z czynników ryzyka jest wytwarzanie oprogramowania przez państwo. – „Jeśli nawet państwo korzysta z usług zewnętrznych dostawców, to bez inżyniera kontraktu po swojej stronie. Gdy rozwiązanie testują koledzy z sąsiedniego departamentu to trudno mówić o właściwej weryfikacji" – wtórował mu Wiesław Paluszyński. – „To prawda, polska choroba polega też na tym, że za sposób rozwiązania problemu uznaje się zmiany ustawowe. Jest taka miara zmienności prawa wyrażana w metrach bieżących. Drukuje się całą działalność ustawodawczą w danym roku na papierze formatu A4, ustawia w stos i mierzy. Dwa lata temu miał on w Polsce 3 m, a Szwecji – 5 cm. To pokazuje, jaką mamy gigantyczną przewagę intelektualną nad Szwecją" – ironizował Krzysztof Komorowski.

Zdaniem Wiesława Paluszyńskiego państwo w zasadzie nie powinno budować warstwy usługowej, tylko sprawne systemy przetwarzania danych źródłowych, na podstawie których buduje się usługi. Zadaniem państwa jest prowadzenie wiarygodnych rejestrów. Sektor komercyjny umie lepiej zdiagnozować, co jest obywatelom potrzebne przy załatwianiu sprawy. To jest model, w którym z powodzeniem działają banki, stawiające na symbiozę z fintechami, bo usługi finansowe muszą szybko reagować na potrzeby rynku. Tak wykreowano bankowość mobilną, w której Polska jest potęgą. – „Taki model zastosowany w administracji mógłby przynieść przełom. Niech – przykładowo – minister finansów prowadzi rejestr podstawowy, ale usługi do tego rejestru niech budują w sposób przyjazny firmy komercyjne" – postulował Wiesław Paluszyński.

– „Pięć lat temu Gartner w swoim raporcie zwrócił uwagę na dwie strategiczne rzeczy w administracji publicznej. Pierwsza z nich to taka, że systemy administracji publicznej muszą ewoluować, bo w przeciwnym razie staną się zbędne lub nieużyteczne. A jakie szanse mamy na realizację tego postulatu, jeżeli zamawiamy je w długim przetargu? Zwykle prawie rok się robi samą dokumentację, a kolejne 2-3 lata buduje system. To, co wydawało nam się dobre 4 lata temu, już takie nie jest, a z powodu prawa zamówień publicznych nic nie można zmienić" – mówił Michał Przymusiński. Jego zdaniem model bodyleasingowy (stosowany nie tylko w Polsce, ale też z ogromnym sukcesem np. w Finlandii), polegający na ścisłej współpracy specjalisty z rynku z urzędnikiem, co ułatwia modyfikację projektu, jest dobry. – „Ale druga konkluzja tego raportu była taka, żeby nie budować systemu, tylko budować zasoby. Wyzwaniem w administracji publicznej jest utrzymanie najlepszych specjalistów, bo charakterystyczne dla niej są ciągłe zmiany kadrowe" – dodał.

Niechęć państwa do mechanizmów rynkowych sprawia, że nie powstają środowiska wykonawców. – „Miałem okazję obserwować powstanie takiego ekosystemu, gdy wybuchła AI w USA. Duże korporacje z silnymi grupami rozwojowymi były mechanizmem napędzającym, ale najtrudniejsze były detale, którymi obarczono małe i średnie przedsiębiorstwa. To nie była formuła zamówień czy przetargów, tylko spotkań nazywanych Developer Forum, na których jednego dnia korporacja mówiła o swoich planach, a kolejnego dnia małe firmy zgłaszały się z propozycjami swoich szczegółowych rozwiązań czy usprawnień" – opowiadał Marek Hołyński.

## Deficyt kompetencji

– „Zastanawia brak kompetencji rzemieślniczych w budowaniu oprogramowania. Od wielu lat prowadzę firmę, która zajmuje się głównie ratowaniem dużych projektów technologicznych. Brak kompetencji technicznych w sektorze publicznym nikogo nie dziwi, powody dawno zdiagnozowano. Dlatego to, co jest zamawiane przez instytucje publiczne w wielu przypadkach wynika z koncepcji dostawców, bo sama instytucja nie jest w stanie ani zdefiniować, ani stworzyć takiej koncepcji. W efekcie dostawcy przychodzą z koncepcją, potem z OPZ, potem z ofertą, a na końcu i tak nikt nie umie tego odebrać. Zdumiewa mnie jednak, że od 2-3 lat mamy dużo zleceń od znanych informatycznych firm komercyjnych, które proszą o pomoc w ratowaniu ich wewnętrznych projektów software'owych. Okazuje się, że te firmy nie wiedzą, jak się pisze oprogramowanie i to jest po prostu niewiarygodne" – skonstatował Krzysztof Komorowski.

– „Marzą mi się przeprowadzane co roku testy kompetencji w administracji. Interesem pracownika powinno być dokumentowanie posiadanych kwalifikacji. Dotyczy to także programistów, którzy piszą aplikacje nie wiedząc, jak działa komputer i bywa, że ich program większość czasu poświęca na obsługę samego siebie. Istotne są też kwestie bezpieczeństwa, nikt nie dochodzi, co jest w implementowanej bibliotece. Coraz częściej stosujemy narzędzia *open source*, a nie stosuje się sprawdzania bezpieczeństwa systemu na etapie wytwarzania, bo to słono kosztuje. Dlaczego jest cicho wokół systemu e-faktur? Bo to robiła spółka Ministra Finansów, komercyjny wykonawca nie wyszedłby z długów" – przekonywał Wiesław Paluszyński.

– „Istotne, żeby sobie uświadomić, że trzeba myśleć w dłuższej perspektywie, nie tylko o tym, żeby system się nie odmówił współpracy za tydzień. Ze strony organizacji oznacza to, że w zespołach muszą musi znaleźć się miejsce dla wybitnie wykwalifikowanych specjalistów od optymalizacji systemu, którzy będą odpowiadali za to, żeby system się nie przewrócił za pół roku. Ich rola to po trosze nieustanne wojny z programistami o jakość i bezpieczeństwo wytwarzanych rozwiązań. Kluczowa jest ciągłość kadr, bo przy dużej rotacji tracimy ludzi, którzy wiedzą to, czego żadna dokumentacja nie zapewnia. Wdrożenie równie wartościowych, ale nowych pracowników, wymaga sporo czasu, bo systemy są coraz bardziej rozbudowane, korzystają z wielu warstw" – podkreślał Michał Przymusiński.

– „Pomijamy w dyskusji aspekt potencjalnej roli sztucznej inteligencji w doskonaleniu usług publicznych. Są dostępne liczne rozwiązania, które mogą być użyteczne np. dla poprawy jakości usług medycznych, projektów badań klinicznych i kontaktów z pacjentami. Budowane przeze mnie modele mogą znaleźć praktyczne zastosowania. Sztuczna inteligencja pomaga także w programowaniu i popularne są narzędzia do generowania kodu, które ułatwiają pracę programistów lub w przyszłości mogą nawet ich zastąpić" – zwrócił uwagę Tadeusz A. Grzeszczyk.

– „Nie mam cienia wątpliwości, że sztuczna inteligencja zmieni podejście do usług: sposób ich budowy, działania, ich interfejs. Jednak powiem rzecz może niepopularną, ale usługi publiczne oferowane dotąd są niezwykle proste. Muszę coś oświadczyć, podpisać, państwo policzy, muszę zapłacić i ewentualnie coś złożyć. To są formularzowe usługi i do tego w ogóle nie potrzebujemy sztucznej inteligencji. I nie mówię tu oczywiście o pisaniu kodu przy jej użyciu, bo to – chcemy tego czy nie – już się dzieje (różne badania wskazują, że na GitHubie już ponad 40% kodu jest wygenerowane przez sztuczną inteligencję). Taki kod oczywiście można by wykorzystywać, tyle tylko, że modele nie były trenowane na najbardziej zaawansowanych niskopoziomowych kodach, więc nie znajdziemy tam rozwiązań przełomowych choćby pod względem wydajności czy bezpieczeństwa.

Z drugiej strony, sztuczna inteligencja wywraca stolik. Jak robiliśmy w pandemii infolinię do rejestracji, mieliśmy 30 tys. jednocześnie dzwoniących osób i musieliśmy to połączyć bardzo prostą automatyką z i wieloma pracownikami *call center*, była też możliwość obsługi rejestracji na szczepienia przez SMS-y i formularze w internecie. Teraz byśmy to na pewno zrobili *voicebotem*, bo te rozwiązania niezwykle się rozwinęły w ciągu roku". – odpowiedział Michał Przymusiński.

## Nobody is perfect

– „Niewiele cyfrowych usług publicznych udaje się zrealizować w czasie i budżecie i z założoną funkcjonalnością (co złośliwi nazywają zasadą nieoznaczoności), ale trzeba uczciwie powiedzieć, że są systemy, które dobrze działają: podatkowe, archiwów państwowych" – tonował dyskusję Marek Hołyński.

– „Jeden z moich ulubionych projektów, które nadzorowałem, to system obsługi Państwowej Inspekcji Sanitarnej. W punkcie startu mieliśmy ponad 300 stacji powiatowych, w których pracowały osoby niecyfrowe. Jeśli były komputery, to z lat 90. Na początku pandemii ludzie spali w pracy, żeby obsłużyć kryzys, jakim była pandemia. Po roku wszystkie procesy były obsługiwane cyfrowo. Udało się – w ścisłym porozumieniu z pracownikami Sanepidu, którzy po prostu mówili nam czego potrzebowali i chętnie się szkolili – fundamentalnie poprawić sytuację. Udało się nawet zmienić przepisy, żeby uruchomić powiadomienia telefoniczne zamiast drogi papierowego powiadomienia. Efekt? System otrzymał Nagrodę Narodów Zjednoczonych dla najlepszego systemu na świecie obsługującego procesy rejestracji kwarantanny i innych mających miejsce na styku obywatel –państwo w związku z pandemią COVID-19" – z dumą informował Michał Przymusiński.

– „Tam, gdzie nie ma zaszłości jest łatwiej. Tam, gdzie funkcjonuje zasiedziałe towarzystwo zwykle nie ma rozwiązań syste-

mowych – jest grupa wzajemnie sprzecznych interesów politycznych i technicznych" – polemizował Wiesław Paluszyński.

– „Pamiętajmy jednak, że nie wszystko jest perfekcyjne. Testy wychodzą dobrze, a po udostępnieniu pierwszej wersji pojawia się strumień pretensji i żądań. Człowiek się zastanawia, dlaczego ja nie pomyślałem o tym, że ktoś może to tak interpretować albo znaleźć taką kombinację wymagań, której nikt z projektantów systemu nie przewidział. My jesteśmy psychicznie przygotowani na to, że system informatyczny będzie miał wadę (do czego Microsoft nas systematycznie przyzwyczaja). Kluczowy jest czas usuwania tych błędów" – precyzował Marek Hołyński.

Zdaniem Wiesława Paluszyńskiego CEiDG (Centralna Ewidencja i Informacja o Działalności Gospodarczej) to przykład systemu, który był budowany wzorcowo, bo ponad rok poświęcono na zebranie oczekiwań przedsiębiorców i samorządów, jak taki system centralnej ewidencji gospodarczej działalności gospodarczej powinien wyglądać. Przy projekcie był powołany zespół interesariuszy, włączony zarówno w proces określania wymagań, jak i odbioru tego systemu.

## Warto słuchać profesjonalistów

Natomiast problemy z systemem e-doręczeń w dużej mierze wynikają z chybionej koncepcji. – „Eksperci z branży próbowali przekonać ministra, że system nie zadziała. A jest to akurat krwiobieg administracji publicznej, bo ona polega na dokumentowaniu wpływu i wysyłki dokumentów. Klęska tego systemu oznacza klęskę cyfryzacji usług w administracji publicznej. Nikt na świecie tak tego nie robi, żadne kolejne skrzynki na poczcie nie są potrzebne. Na domiar złego proteza analogowa też nie wchodzi w grę, bo poczta nie działa i wrzucenie listu do skrzynki jest samobójstwem.

Funkcjonują proste komercyjne systemy, które rozwiązują sprawę za nieduże pieniądze. Mam umowę, wysyłam, otrzymuję ścieżkę potwierdzeń niezaprzeczalnych, zgodnych z prawem unijnym. Nie trzeba budować za ciężkie miliardy złotych jakiegoś własnego systemu. Po co państwo ma być pocztą? Państwo robi przetarg i ogłasza, z której platformy chce korzystać. I tak jest nawet bezpieczniej, bo ma od kogo dochodzić ewentualnych roszczeń. Natomiast w przypadku samodzielnego wytwarzania nie ma regresu na jakość" – tłumaczył Wiesław Paluszyński.

Jakub Groszkowski, zastępca Prezesa Urzędu Ochrony Danych Osobowych zadeklarował w imieniu prezesa UODO, Mirosława Wróblewskiego, otwartość na dialog z sektorem publicznym i prywatnym. – „UODO od kilku lat prowadzi kontrole sektorowe z zakresu przetwarzania danych osobowych przy użyciu aplikacji mobilnych i internetowych, w tym roku ta kontrola będzie kontynuowana. Podzielę się z państwem dobrą informacją, że jakość zapewnienia bezpieczeństwa przetwarzania danych osobowych poprawiła się w części prywatnej. Jak tylko pojawią się wnioski pokontrolne, chętnie się nimi podzielimy – zapowiedział Jakub Groszkowski.

– „Moim zdaniem wracamy do początku naszej dyskusji, jeśli nie ma prawa „budowlanego" to cała reszta jest pochodną działania polityki" – podsumował Wiesław Paluszyński.

Uczestnicy debaty podkreślali, że jej celem nie jest piętnowanie kogokolwiek, tylko wskazanie kierunków sanacji cyfrowych usług publicznych.

**Należy wszystkimi dostępnymi kanałami prowadzić lobbing w przestrzeni publicznej na rzecz najistotniejszych działań. Należą do nich:**

1. **Zmiana przekonania, że państwo jest zawsze dobrym software housem. To jest myślenie rodem ze słusznie minionego systemu, niedawno przekonaliśmy się, jak państwo świetnie buduje samochody elektryczne.**
2. **Obowiązkowe wprowadzenie po stronie państwa profesjonalnego inżyniera kontraktu, bo zamawianie jest procesem, który decyduje o efektach wdrożenia rozwiązania. Nie można robić cyfryzacji w administracji publicznej bez odpowiednich kompetencji nadzorczo-kontrolnych.**
3. **Wdrożenie choćby szkieletowego prawa „budowlanego" w obszarze usług i kompetencji budowy usług publicznych. Można by zacząć od wprowadzenia nakazu, że od pewnego poziomu ważności czy skali usługi instytucja zamawiającą musi mieć inżyniera nadzoru. Obowiązkiem takiego inżyniera byłoby nie tylko dbanie o rzemieślniczą poprawność technologiczną budowy, ale również o przestrzeganie wszystkich norm.**
4. **Wymuszenie zmian w kulturze stosowania prawa zamówień publicznych. Chodzi o prawo wyboru wizji architektonicznej systemu wynikającej z potrzeb jednostki i niezmuszanie do zachowania neutralności technologicznej przy skomplikowanym środowisku (vide ZUS). Potrzebne jest także wzmożenie czujności w zakresie cyberbezpieczeństwa (dostawcy wysokiego ryzyka).**

„Domena" będzie jednym z kanałów propagowania rekomendacji PTI.

*Anna Kniaź*


Autorem niepokojących totemów – symboli nagrody – jest rzeźbiarz Paweł Jackowski.

# Konkurs na ANTYaplikację rozstrzygnięty

Nagroda dla Najgorszej Aplikacji udostępniającej usługi publiczne została w tym roku przyznana przez PTI po raz pierwszy. Konkurs na ANTYapilkację był krzykiem rozpaczy przeciwko endemicznej bylejakości usług cyfrowych dostępnych publicznie oferowanych przez instytucje i publiczne i prywatne. Bylejakość ta ma wymiary społeczne, informatyczne, logiczne, biznesowe, estetyczne (patrz zapis dyskusji „ Jak uzdrowić cyfrowe usługi publiczne").

**Jury w składzie: Wiesław Paluszyński, Piotr Kociński, Paweł Dobrowolski, Marek Hołyński, Krzysztof Komorowski – było przytłoczone ogromem tragicznych aplikacji kwalifikujących się do tego wyróżnienia. Postanowiono więc uhonorować nie tyle bardzo złe usługi czy aplikacje (tych było mnóstwo), co aplikacje całkowicie mijające się w ocenie jury z potrzebami społecznymi.**

I tak **w kategorii usług publicznych uhonorowano MEN** zalecający używanie aplikacji typu „cyfrowy dziennik". Nagrodę przyznano za:

- stwarzanie pozoru uczestnictwa rodziców w procesie edukacyjnym dziecka, skupiając się maniakalnie tylko na drugorzędnych, mierzalnych artefaktach procesu kształcenia, a całkowicie zaniedbując i odwracając uwagę od najważniejszych jego aspektów: dojrzałości, rozwoju społecznego, dobrostanu, zagrożeń wychowawczych itp.
- całkowite odarcie z intymności życia ucznia.

Polecamy lekturę niezwykle poruszającego osobistego uzasadnienia tego wyboru pióra Piotra Kocińskiego (**https://portal.pti.org.pl/konkurs-na-najgorsza-aplikacje-rozstrzygniety/**).

**W kategorii usług komercyjnych nagrodę przyznano TVP** za całkowitą nieumiejętność wykorzystania swojego gigantycznego potencjału w obszarze udostępniania przebogatych i bardzo popularnych zasobów cyfrowych. Zachwyt jury wzbudziły zarówno aspekty biznesowo-marketingowe, jak i techniczne tej nieudolności. Mimo że TVP jest bytem poniekąd publicznym, nagrodę przyznano za dokonania w sferze komercyjnej.

W tym roku nie przyznano – z powodów humanitarnych – nagrody honorowej za całokształt działań skutkujących wystawieniem szczególnie odrażających aplikacji.

# Mamy powody do dumy, radości i świętowania




**Hanna Mazur**
przewodnicząca Komitetu Organizacyjnego Konkursu, członek Oddziału Dolnośląskiego PTI, pracownik dydaktyczny Politechniki Wrocławskiejl

**Organizowany nieprzerwanie od 40 lat ogólnopolski konkurs na najlepsze prace magisterskie z zakresu informatyki i jej zastosowań przyczynia się do poprawy poziomu prac, a wielu uczestnikom otwiera drogę do kariery naukowej.**

Wiele uczelni w Polsce zajmuje się kształceniem studentów na kierunkach informatycznych. Każda z nich promuje swoje osiągnięcia. Udział studentów w konkursach i olimpiadach informatycznych umożliwia porównywanie kształcenia i wiedzy na poziomie krajowym i międzynarodowym.

Coroczny konkurs na najlepsze prace magisterskie z informatyki, organizowany przez Polskie Towarzystwo Informatyczne od 1984 r., ma właśnie na celu umożliwienie wymiany i porównania doświadczeń i osiągnięć szkół wyższych poprzez prezentację najlepszych prac magisterskich z informatyki, motywowanie do podnoszenia ich poziomu, a także propagowanie PTI wśród studentów. Od 40 lat konkurs niezmiennie organizuje Dolnośląski Oddział PTI z siedzibą we Wrocławiu.

## Jubileuszowa edycja konkursu

Do XL konkursu przyjęto 53 prace wykonane w roku akademickim 2022/2023 w 20 krajowych wyższych uczelniach. Najwięcej prac (po 10) nadesłały Politechnika Krakowska i Akademia Górniczo-Hutnicza w Krakowie. Politechnika Wrocławska zagłosiła 7 prac, Uniwersytet Warszawski – 5, Politechnika Poznańska – 4, a Uniwersytet Jagielloński i Uniwersytet Wrocławski – po 2. Pozostałe uczelnie: Politechnika Białostocka, Politechnika Częstochowska, Politechnika Opolska, Politechnika Śląska, Szkoła Główna Gospodarstwa Wiejskiego, Uniwersytet Ekonomiczny w Katowicach, Uniwersytet Ekonomiczny w Poznaniu, Uniwersytet Gdański, Uniwersytet Kazimierza Wielkiego w Bydgoszczy, Uniwersytet Mikołaja Kopernika w Toruniu, Uniwersytet Morski w Gdyni, Uniwersytet Szczeciński, Wojskowa Akademia Techniczna nadesłały po jednej pracy.

**Komisja konkursowa XL edycji:**

- **dr hab., prof. ucz. Zygmunt Mazur – przewodniczący**
- dr hab. inż. Maciej Antczak
- dr inż. Marek Bolanowski
- dr inż. Anna Felkner
- prof. dr hab. inż. Zbigniew Huzar
- prof. dr hab. inż. Marek Kisiel-Dorohinicki
- dr hab. inż., prof. ucz. Lech Madeyski
- dr hab., prof. ucz. Marcin Paprzycki
- dr hab., prof. ucz. Jakub Swacha
- dr inż. Zbigniew Szpunar – sekretarz
- dr hab. inż. Bartosz Walter

## Laureaci XL Konkursu Prac Magisterskich

**Pierwszą nagrodę**, w wysokości **10000 zł**, otrzymał
**mgr Szymon Tworkowski**
za pracę: ***Fine-tuning large language models for long context utilization***

wykonaną w Uniwersytecie Warszawskim (Wydział Matematyki, Informatyki i Mechaniki, Instytut Informatyki).

Promotor pracy dr hab. prof. ucz. Piotr Miłoś otrzymał nagrodę specjalną – ustanowioną po raz pierwszy z okazji jubileuszu konkursu – w wysokości 7000 zł.

**Drugą nagrodę**, w wysokości **8000 zł**, otrzymał
**mgr inż. Adam Wojciechowski**
za pracę: ***Explaining Image Classification in Natural Language***

wykonaną w Politechnice Poznańskiej (Wydział Informatyki i Telekomunikacji, Instytut Informatyki; promotor: dr inż. Mateusz Lango).

**Trzecią nagrodę**, w wysokości **6500 zł,** otrzymał
**mgr Maciej Mikuła**
za pracę: ***Neural premise selection for automated theorem proving***

wykonaną w Uniwersytecie Warszawskim (Wydział Matematyki, Informatyki i Mechaniki, Instytut Informatyki; promotor: dr hab., prof. ucz. Marek Cygan).

**Trzy równorzędne wyróżnienia**, po **4500 zł**, otrzymali:
**mgr inż. Karolina Bąk**
za pracę: ***Selected cryptographic schemes implemented in the blockchain system***

wykonaną w Politechnice Wrocławskiej (Wydział Informatyki i Telekomunikacji, Katedra Podstaw Informatyki; promotor: dr hab. inż., prof. ucz. Łukasz Krzywiecki);

**mgr inż. Szymon Mazurek**
za pracę: ***Epilepsy seizure detection and dynamical brain connectivity via machine learning***

wykonaną w Akademii Górniczo-Hutniczej im. Stanisława Staszica w Krakowie (Wydział Elektrotechniki, Automatyki, Informatyki i Inżynierii Biomedycznej; promotor: dr hab. inż., prof. ucz. Maciej Malawski);

**mgr inż. Mateusz Woźny**
za pracę: ***Techniki neutralizacji postów typu clickbait w sieciach społecznościowych metodami przetwarzania języka naturalnego***

wykonaną w Politechnice Poznańskiej (Wydział Informatyki i Telekomunikacji, Instytut Informatyki; promotor: dr inż. Mateusz Lango).

**Laureatom konkursu serdecznie gratulujemy oraz życzymy pomyślności i sukcesów w pracy zawodowej!**

Fundatorami nagród byli Partnerzy XL Konkursu: NASK i Fundacja Cyfrowa Przyszłość.

W tym roku prace oceniało 85 niezależnych recenzentów pochodzących z innych ośrodków niż nadesłana praca, za co należą się ogromne podziękowania, tym bardziej, że recenzje są wykonywane nieodpłatnie. Poziom nadesłanych prac jest, zdaniem recenzentów, wysoki. – *Niektórzy recenzenci podkreślali, że wyniki przedstawione w pracach magisterskich mogą być podstawą rozpraw doktorskich* – powiedział podczas uroczystości wręczania nagród Zygmunt Mazur, przewodniczący Komisji Konkursowej.

Uroczystości towarzyszyła sesja naukowa z 4. prelekcjami:

- *Transformery i długi kontekst* – **dr hab., prof. ucz. Piotr Miłoś** – Uniwersytet Warszawski oraz IMPAN
- *Metody klasyfikacji obrazów oferujące wyjaśnienia w języku naturalnym* – **mgr inż. Adam Wojciechowski** – Politechnika Poznańska
- *Metody uczenia reprezentacji grafów* – **dr inż. Piotr Bielak** – Politechnika Wrocławska
- *Badania humanistyczne wyzwaniem dla przetwarzania języka naturalnego* – **dr hab. inż., prof. ucz. Maciej Piasecki** – Politechnika Wrocławska

Beata Laszkiewicz, prezes Oddziału Dolnośląskiego przedstawiła historię konkursu. Inicjatywę jego organizacji zgłosił w 1983 r. Zygmunt Mazur. Zgodnie z panującą w PTI zasadą – *masz pomysł, to go zrealizuj, a my ci w tym pomożemy* – pomysłodawca opracował regulamin i zasady konkursu, które obowiązują do dzisiaj.

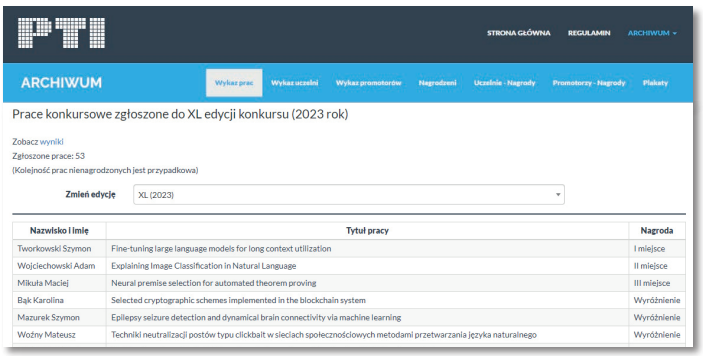
Całą pracę organizacyjną związaną z przeprowadzeniem konkursu wykonywano we Wrocławiu. Przez wiele lat prace dyplomowe były przesyłane przez autorów pocztą tradycyjną w wersji papierowej. Prace te następnie wysyłano do recenzentów, którzy po ocenie odsyłali je do Wrocławia, a po zakończeniu konkursu praca była odsyłana do autora. Nie trudno sobie wyobrazić, z jakimi problemami się borykano, by zdążyć ze wszystkim na czas. Nigdy jednak nie przekroczono żadnego terminu, wyniki zawsze były znane do końca grudnia każdego roku. Odbyły się wszystkie edycje konkursu, także w stanie wojennym, w którym problemem było nawet wydrukowanie plakatu wysyłanego z listem przewodnim do wydziałów prowadzących kierunki informatyczne wszystkich polskich uczelni. Dzisiaj ten proces został znacznie uproszczony dzięki komunikacji elektronicznej i wdrożeniu systemu informatycznego.

## Własny system konkursowy

Od 2017 r. konkurs jest przeprowadzany z wykorzystaniem systemu informatycznego opracowanego przez zespół w składzie: Hanna Mazur (kierownik projektu), Mikołaj Nowak, Kamil Raczycki i Filip Szenborn. System dostępny jest pod adresem kpm.pti.org.pl i umożliwia pełną obsługę konkursu online:

- autorom – elektroniczne zgłaszanie prac na konkurs,
- recenzentom – dostęp do recenzowanej pracy i formularza recenzji,
- członkom jury – przeglądanie prac i recenzji,
- organizatorom – zakładanie kont i nadawanie uprawnień użytkownikom systemu, wysyłanie e-maili do recenzentów z informacją o terminach i przedzielonych pracach, generowanie statystyk itp.

Niezwykle cenną częścią systemu jest archiwum konkursu zawierające dane zgromadzone od 1984 r. System udostępnia wyniki i statystyki oraz dodatkowe informacje (m.in. plakaty i wysokości nagród) ze wszystkich dotychczasowych edycji konkursu.




### Konkurs w statystykach

W czterdziestu edycjach (w latach 1984-2023) do konkursu zakwalifikowano 1223 prace z 56 uczelni, nagrodzono i wyróżniono 250 prac, przy czym 214 nagrodzonych prac pochodzi z 7 uczelni: Akademii Górniczo-Hutniczej (41), Politechniki Wrocławskiej (41), Politechniki Poznańskiej (37), Uniwersytetu Warszawskiego (35), Politechniki Warszawskiej (24), Uniwersytetu Wrocławskiego (22) i Politechniki Gdańskiej (14).

Przyjmując, że każda praca ma tylko 1 cm grubości, to stos ułożony ze wszystkich przyjętych na konkurs prac miałby 12,23 metrów wysokości, a więc wysokość 4-piętrowego budynku.

| Uczelnia | Liczba nagrodzonych | Liczba wyróżnionych | Liczba laureatów |
|---|---|---|---|
| AGH | 23 | 18 | 41 |
| UW | 21 | 14 | 35 |
| PWr | 18 | 23 | 41 |
| PP | 16 | 21 | 37 |
| PW | 14 | 10 | 24 |
| UWr | 11 | 11 | 22 |
| PGd | 8 | 6 | 14 |

## Powód do dumy

Wielu laureatów wcześniejszych edycji konkursu uzyskało stopnie naukowe doktora i doktora habilitowanego i tytuły naukowe profesora. Wielu z nich jest pracownikami wyższych uczelni lub instytucji naukowych i kształci kolejne pokolenia autorów prac i laureatów konkursu.

Laureaci konkursów, którzy następnie zostali promotorami nagrodzonych prac:

| Laureat | Rok | Lokata | I | II | III | wyr | inne | RAZEM |
|---|---|---|---|---|---|---|---|---|
| dr Sas Jerzy | 1984 | wyróżnienie | | 1 | | | | 1 |
| dr inż. Chrząszcz Jerzy | 1986 | II miejsce | | | | 1 | 5 | 6 |
| prof. dr hab. inż. Stefanowski Jerzy | 1987 | wyróżnienie | | 3 | | 1 | 6 | 10 |
| mgr inż. Kowalski Henryk | 1987 | III miejsce | | | | | 4 | 4 |
| mgr inż. Mazur Grzegorz | 1987 | wyróżnienie | 1 | | | | 1 | 2 |
| dr inż. Lebiedź Jacek | 1987 | III miejsce | | | | | 1 | 1 |
| prof. ndzw. dr hab. Tyszkiewicz Jerzy | 1988 | wyróżnienie | | | | | 1 | 1 |
| dr Stpiczyński Przemysław | 1989 | wyróżnienie | | | 1 | | 4 | 5 |
| prof. dr hab. inż. Unold Olgierd | 1989 | wyróżnienie | | | | | 3 | 3 |
| dr Król Zdzisław | 1990 | wyróżnienie | | | | 1 | 1 | 2 |
| dr Walukiewicz Igor | 1991 | I miejsce | | 1 | | | | 1 |
| dr inż. Piasecki Maciej | 1993 | II miejsce | | | | 1 | 4 | 5 |
| dr inż. Sobaniec Cezary | 1997 | wyróżnienie | | | | 1 | 1 | 2 |
| dr inż. Czajka Adam | 1997 | wyróżnienie | | | | | 1 | 1 |
| dr Gawkowski Piotr | 1998 | I miejsce | | | | | 1 | 1 |
| dr hab. inż. Czarnul Paweł | 1999 | III miejsce | | | | 1 | 3 | 4 |
| dr hab. inż. Nalepa Grzegorz Jacek | 1999 | II miejsce | | | | | 1 | 1 |
| dr hab. Bojańczyk Mikołaj | 2000 | II miejsce | | | | | 2 | 2 |
| dr inż. Rycerz Katarzyna | 2001 | I miejsce | 2 | | 2 | 1 | 5 | 10 |
| dr Chlebiej Michał | 2002 | wyróżnienie | | | | | 2 | 2 |
| dr inż. Jarzębowicz Aleksander | 2002 | III miejsce | | | | | 2 | 2 |
| dr inż. Jabłoński Bartosz | 2003 | II miejsce | | | | 1 | 3 | 4 |
| dr hab. Rządca Krzysztof | 2004 | II miejsce | 1 | | | | 2 | 3 |
| dr hab., prof. ucz. Iwanicki Konrad | 2006 | II miejsce | 2 | | | 2 | 2 | 6 |
| dr inż. Czech Wojciech | 2007 | I miejsce | | | | | 1 | 1 |
| dr hab. Cygan Marek | 2008 | I miejsce | | | 1 | | 1 | 2 |
| dr hab. Pilipczuk Marcin | 2008 | I miejsce | | | | | 1 | 1 |
| dr inż. Szubert Marcin | 2009 | II miejsce | | | | | 1 | 1 |
| dr inż. Nalepa Jakub | 2011 | II miejsce | | | | | 1 | 1 |
| dr inż. Saganowski Stanisław | 2011 | wyróżnienie | | | | | 1 | 1 |
| dr inż. Lango Mateusz | 2015 | II miejsce | | 1 | | 1 | 1 | 3 |

| Promotor | I | II | III | wyr | Inna | Razem |
|---|---|---|---|---|---|---|
| dr inż. Bubak Marian | 2 | | 1 | 3 | 10 | 16 |
| dr hab. Bała Piotr | | | | 1 | 12 | 13 |
| dr hab. inż. Czech Zbigniew | | 1 | | 2 | 10 | 13 |
| prof. ndzw. dr hab. inż. Błażewicz Jacek | | | | 1 | 10 | 11 |
| prof. dr hab. inż. Zieliński Krzysztof | 2 | | 3 | 3 | 3 | 11 |
| dr inż. Kwiatkowski Jan | 2 | 1 | | | 7 | 10 |
| prof. ndzw. dr hab. inż. Morzy Tadeusz | | 1 | 1 | 3 | 5 | 10 |
| dr inż. Rycerz Katarzyna | 2 | | 2 | 1 | 5 | 10 |
| dr hab. inż. Stefanowski Jerzy | | 3 | | 1 | 5 | 9 |
| dr hab. inż. Huzar Zbigniew | | | | 4 | 4 | 8 |
| prof. ndzw. dr hab. inż. Kubale Marek | 4 | 1 | 1 | | 2 | 8 |

***Uwaga:*** *stopnie i tytuły naukowe promotorów zgodne z zapisem w bazie podczas ostatniego zgłoszenia pracy na konkurs.*

W swoim wystąpieniu Arkadiusz Wójs, rektor Politechniki Wrocławskiej, goszczącej od wielu lat uczestników uroczystości konkursu, powiedział: „każda politechnika, uczelnia szczyci się swoją informatyką, bo to jest bardzo potrzebny kierunek i obszar badań w dzisiejszych czasach. Jesteśmy dumni, że mamy ogromny wydział, studentów i profesorów informatyki. Nie do końca chyba wiem, czym jest informatyka, wiem natomiast, że podłączanie drukarki to nie jest informatyka. Przez całą swoją karierę z fizyki robiłem obliczenia komputerowe – to podobno też nie jest informatyka. Kiedyś, gdy byłem dziekanem, zapytałem o to jednego naszego doktora z informatyki teoretycznej. Wytłumaczył mi na przykładzie. Wyobraź sobie problem z poszukiwaniem żony. Musimy odpowiedzieć na pytanie, ile osób trzeba sprawdzić, zanim się natrafi na tę właściwą i już więcej nie należy sprawdzać – to jest właśnie problem z obszaru informatyki. Myślę, że celem dzisiejszego spotkania jest to, żebyśmy się dowiedzieli, co dzisiaj jest ważne w informatyce. I to nam nasi nagrodzeni pokażą".

I rzeczywiście, laureaci w swoich wystąpieniach przedstawili tezy swoich prac magisterskich, problemy które udało im się rozwiązać oraz wyniki swoich prac. Z perspektywy 40 lat widać, że dyplomanci polskich uczelni podejmują bardzo ciekawe i trudne tematy prac magisterskich, umiejętnie formułują cele i je osiągają.

To jest powód do dumy. Równolegle jednak dumą i radością napawa myśl o czterdziestoletniej, nieprzerwanej w żadnym roku organizacji konkursu. Docenił to także Zarząd Główny PTI, który uhonorował pomysłodawcę konkursu, a zarazem przewodniczącego Komisji konkursu i organizatora – Zygmunta Mazura. Dyplomy uznania otrzymały także inne osoby zaangażowane w prace na rzecz konkursu: Zbigniew Huzar, Lech Madeyski, Hanna Mazur, Zbigniew Szpunar oraz twórcy systemu: Hanna Mazur, Mikołaj Nowak, Kamil Raczycki i Filip Szenborn.

Historia konkursu w publikacji PTI dostępna w wersji elektronicznej: **https://portal.pti.org.pl/wp-content/uploads/2019/01/30-lat-PTI-wyd.-II-1.pdf** (strony 85-86).

# Agora sztucznej inteligencji

**Jakiej debaty na temat sztucznej inteligencji brakuje w Polsce? Jak poradzić sobie z obawami, zrozumieć zagrożenia i możliwości AI? Jakie są największe wyzwania tej technologii? Odpowiedzi na te pytania będzie próbowała udzielić nowa w PTI Sekcja Aktualne Wyzwania Sztucznej Inteligencji (AWSI). Rozmawiamy z jej założycielami: Marią Ganzhą, Przemysławem Bieckiem i Michałem Nowakowskim.**

**dr hab. Maria Ganzha**

prezeska Oddziału Mazowieckiego PTI, profesor Politechniki Warszawskiej z tytułem magistra matematyki i doktora nauk matematycznych (Moskiewski Uniwersytet Państwowy). W 2013 r. uzyskała stopień doktora habilitowanego nauk informatycznych, nadany przez Polską Akademię Nauk. Autorka ponad 200 publikacji. Jej badania skupiają się na systemach rozproszonych, ze szczególnym uwzględnieniem technologii agentowych i Internetu Rzeczy, technologii semantycznych oraz uczenia maszynowego. Koordynatorka techniczna w projekcie H2020 ASSIST-IoT oraz koordynatorka zespołu IBSPAN w projekcie HE aerOS.

**prof. dr hab. inż. Przemysław Biecek**

matematyk i informatyk, profesor nauk inżynieryjno-technicznych o specjalności sztuczna inteligencja. Prowadzi zespół badawczy MI2.AI realizujący wiele projektów badawczych skupionych na red teaming modeli podstawowych, analizie modeli językowych typu LLaMA, GPT, modelowaniu obrazów 3D, np. obrazów z tomografii komputerowej oraz analizie wyjaśnialnej modeli predykcyjnych. Autor ponad 150 artykułów oraz 5 monografii związanych z analizą danych. Ekspert w grupie roboczej Responsible AI międzynarodowej inicjatywy Global Partnership on Artificial Intelligence (GPAI). W czasie wolnym rozwija materiały upowszechniające matematykę i informatykę w postaci przygód rodzeństwa Bety i Bita.

**dr Michał Nowakowski**

radca prawny – ekspert w dziedzinie wdrażania oraz rozwijania systemów sztucznej inteligencji (uczenie maszynowe, głębokie, LLM) z perspektywy biznesowej, technologicznej oraz prawnej, a także zarządzania ryzykiem ICT. Współautor opinii prawnej dla *shadow rapporteur* w zakresie AI Act z 2021 r. Współzałożyciel i CEO spółki GovernedAI dbającej o bezpieczne, odpowiedzialne i etyczne wdrażanie rozwiązań AI. Autor m.in. książki „Sztuczna inteligencja. Praktyczny przewodnik dla sektora FinTech" (2023) i wielu artykułów naukowych. Prowadzi kolumnę „Sztuczna inteligencja w praktyce" w „Rzeczypospolitej". Wykładowca prawnych i etycznych aspektów wdrażania systemów AI. Prezes Sekcji Aktualne Wyzwania Sztucznej Inteligencji.

### Skąd pomysł stworzenia sekcji?

**Maria Ganzha:** Rodził się krok po kroku… Po „wybuchu" popularności ChatGPT i innych modeli Generatywnej AI zaczęłam dostawać zaproszenia na panele, dyskusje i wykłady. Zdobyte tam doświadczenia uświadomiły mi, że wiedza o AI jest bardzo niepełna. Właściwie nawet samo pojęcie AI jest bardzo mgliście zdefiniowane i różnie rozumiane.

Równocześnie AI coraz aktywniej uczestniczy w naszym życiu. Ludzie zaczynają podejmować istotne decyzje na podstawie jej „porad", czyli oddają podejmowanie decyzji różnorodnym, coraz bardziej autonomicznym systemom. Taka sytuacja zaczyna być niepokojąca. Po kolejnym spotkaniu doszłam do wniosku, że trzeba coś robić. Jak zwykle pomógł los. Na jednym z paneli poznałam Michała. Czekając na rozpoczęcie wydarzenia, zaczęliśmy niezobowiązująco rozmawiać przy bilardzie... Szybko okazało się, że podobnie myślimy i nie boimy się działań, co dało początek rozmowom o tym, co możemy zrobić razem, aby edukować szeroko rozumiane społeczeństwo na temat AI. Natomiast Przemek jest moim kolegą „drzwi w drzwi" na Politechnice Warszawskiej. Mieliśmy wielokrotnie okazję rozmawiać o AI, a zwłaszcza o wyjaśnialnej AI, dlatego zaprosiłam go do współtworzenia nowej Sekcji AWSI. Formalne powołanie władz w ramach PTI nastąpiło jesienią 2023 r.

### Jakie cele chcecie osiągnąć?

**MG:** U źródła działań sekcji legł wspomniany niepokój dotyczący niewielkiej wiedzy o AI i wielu mitów, które są krzywdzące i dla sztucznej inteligencji, i dla człowieka. Ponadto istotna jest refleksja na temat tego, jak małe jest również całościowe rozumienie rewolucji, która się wokół nas dokonuje. Nie chodzi tylko o pralkę, która upiera się, że wie lepiej, jak należy wyprać moje pranie. Dotyczy to również prób zapanowania nad gwałtownymi zmianami, których jesteśmy świadkami. Dlatego – posłużmy się przykładem – dla większości ludzi powstający właśnie AI Act jest kompletną abstrakcją, kolejnym nudnym dokumentem, który wymyśliła Unia. Podczas jednego z paneli, w którym brałam udział, przedstawiciel dość dużej firmy przekonywał, że ten dokument jest szkodliwy dla rozwoju firm, bo będzie blokować innowacje. Dlatego należy zacząć na serio rozmawiać o tym, co się wokół nas dzieje. Taka rozmowa musi być dopasowana do wiedzy, stanowiska, potrzeb i wymagań uczestników. Myślę, że dla mnie jest to główny cel sekcji. Należy podkreślić, że taka rozmowa nie powinna być tylko i wyłącznie reaktywna. Myślę tu również o poruszaniu tematów proaktywnie, czyli zanim „coś się stanie".

**Przemysław Biecek:** Sztuczna inteligencja w ostatnich latach przeżywała szalenie intensywny rozwój, który tylko przyspieszył po publicznym udostępnieniu ChataGPT przez Open AI ponad rok temu. Tak radykalna zmiana generuje zarówno wiele obaw, jak i możliwości. Warunkiem poradzenia sobie z obawami i skorzystania z możliwości jest wymiana doświadczeń pomiędzy grupami interesariuszy, zarówno twórców modeli AI, ich użytkowników, entuzjastów, jak i sceptyków. Tak ja postrzegam misję AWSI, jako platformę wymiany doświadczeń pozwalającą rozwiewać obawy i wykorzystać możliwości.

**Michał Nowakowski:** Pochodzimy z różnych środowisk i każde z nas nieco inaczej patrzy na sekcję i jej główne cele. To, co jednak nas łączy, to chęć promowania i rozwijania „dobrej" sztucznej inteligencji – to określenie rzucił Grzegorz Gwardys, który jest też członkiem sekcji oraz racjonalnym komentatorem i kontestatorem dynamicznie pojawiających się pomysłów.

> *Innymi słowy, zależy nam na budowaniu otoczenia, w którym do AI podchodzi się w sposób rozważny i odpowiedzialny, a człowiek jest w samym centrum. Chcemy to osiągnąć, realizując pomniejsze cele, które z pewnością będą ewoluowały w czasie, podobnie jak sama technologia, którą się zajmujemy.*

### Co wyróżnia sekcję wśród innych podobnych inicjatyw?

**MG:** Dla mnie fascynujące było jedno z pierwszych spotkań członków sekcji, na którym poprosiłam o parę słów autoprezentacji. Wówczas dotarło do mnie, że nawet nie marzyłam o tak różnorodnym składzie założycieli sekcji. To właśnie jest dla mnie najważniejsze – rzeczywiste zainteresowanie bardzo różnych środowisk. Istotne jest również nasze wspólne rozumienie, że taki stan rzeczy, z jakim mamy do czynienia (jeżeli chodzi o różne aspekty stosowania i rozwijania AI w Polsce i na świecie), jest nieakceptowalny.

> *Myślę, że to właśnie wyróżnia Sekcję AWSI – powstanie platformy wymiany myśli dostępnej dla każdego, kto chce wiedzieć więcej i jest gotów dzielić się swoją wiedzą.*

**PB:** Inne inicjatywy networkingujące wokół AI, które znam, są bardziej jednolite. To albo konferencje naukowe dla naukowców pracujących nad AI, albo konferencje biznesowe skupiające firmy sprzedające AI, albo grupy eksperckie pracujące nad regulacjami wokół AI. AWSI jest bardziej różnorodne niż każda z tych grup, mamy przed-

stawicieli uczelni, biznesu, instytucji publicznych, którzy spotykają się po godzinach pracy, bo mają dużo energii, by zrobić coś fajnego.

**MN:** Wyróżniamy się przede wszystkim interdyscyplinarnością i połączeniem biznesu, nauki i administracji. Mamy różne kompetencje i doświadczenia i to jest największą wartością. Uważamy, że AI to zagadnienie multidyscyplinarne, a nie zarezerwowane dla inżynierów. Oczywiście, ma to też swoje małe „wady", gdy dochodzi do spięć wynikających z różnych perspektyw.

> *Nie ma chyba jednak drugiego takiego forum, na którym inżynier rozmawia swobodnie z prawnikiem, a filozof z programistą.*

**MN:** Pracujemy nad konkretną ofertą dla naszych członków oraz działaniami, które podejmiemy. Zachęcamy do obserwowania naszej strony i profilu na LinkedIn. Dzisiaj jest to przede wszystkim forum dla wymiany doświadczeń i myśli, a także miejsce, gdzie można swobodnie porozmawiać z autorytetami w dziedzinie AI.

**Nawiązując do nazwy sekcji: jakie – Waszym zdaniem – są aktualne wyzwania w obszarze rozwoju i stosowania sztucznej inteligencji?**

**MG:** Jest ich sporo… Powiem o takich, które bardzo mnie martwią z powodów oczywistych. Pierwszy – ekologia. Systemy Generatywnej AI są nie tylko bardzo kosztownie energetycznie (wymagają ogromnych mocy obliczeniowych i do trenowania, i do stosowania), lecz również zużywają olbrzymie ilości wody (do chłodzenia serwerów). Poświęcamy więc czystość powietrza dla „pogaduszek z komputerem" (wiem, że trochę upraszczam, ale generalnie tak to wygląda). Jeśli chodzi o te pogaduszki, to kiedy uruchomiony został odpowiednik Google Store dla aplikacji bazujących na Large Language Models, okazało się, że użytkownicy stworzyli tam dziesiątki „przyjaciółek" i „przyjaciół". Leczenie samotności kosztem ekologii nie wydaje się dobrym pomysłem.

Drugim wyzwaniem są dane i związane z tym problemy (prawa autorskie, prywatność, manipulacje…). Wczoraj sztuczny (fake'owy) Joe Biden „dzwonił" do wyborców w New Hampshire – czyli użyto głosu rzeczywistego człowieka, bo nie ma prawa, które by tego zabroniło. Prawa, które byłoby konsekwentnie stosowane w takich i podobnych przypadkach. Równocześnie, i to chyba jest najważniejsze, nie ma jednoznacznego stanowiska społeczeństwa, twardego, słyszalnego sprzeciwu. Czy takiego świata chcemy? Tak, my w jakiś sposób zgadzamy się na „oddanie" naszych danych dużym firmom takim jak Google, bo mamy Google Maps, Google Calendar, Google Mail itp. Ponieważ dostarczane przez te firmy serwisy są przydatne, znacznie upraszczają i usprawniają nasze życie…Tu pojawia się pytanie – jak pogodzić dostęp do serwisu z ochroną prywatności?

To problem nie ogranicza się tylko do dużych firm. Trzeba zdawać sobie sprawę z tego, że nasze państwo (rząd) również ma olbrzymią ilość danych, które systematycznie dostarczamy mu na różnych etapach życia (narodziny, ślub, wyroki sądowe, przekroczenia drogowe itd.). W tym obszarze również istnieją niezbędne mechanizmy, które regulują wykorzystanie tych danych nawet w najbardziej szczytnych celach (bezpieczeństwo itp.) i potrzebujemy takich rozwiązań dla modeli AI.

**Czy należy się więc bać AI?**

**MN:** Narracja, której pojawia się coraz więcej w mediach, sugeruje, że sztuczna inteligencja jest zagrożeniem, że za rogiem czai się samoświadomy komputer, który zacznie po kolei eliminować wszystkich, którzy stoją na jego drodze. No może nieco przesadziłem, ale z pewnością jest coś w tym, że zamiast edukować i uspokajać, media zaczynają wzbudzać w nas niepokój. Prawda leży gdzieś pośrodku, bo choć nie ma uzasadnionych podstaw do twierdzenia, że sztuczna inteligencja osiągnie poziom ludzkiego umysłu, to jednocześnie jej wykorzystanie – nawet na obecnym etapie – może generować ryzyka. Te ryzyka są jednak związane z tym, jak projektowane, rozwijane i wykorzystywane są narzędzia korzystające z uczenia głębokiego, przetwarzania języka naturalnego czy rozpoznawania mowy, a więc z tym, jak podchodzi do nich człowiek. Tym zajmuje się też rozwojowa dziedzina odpowiedzialnej czy godnej zaufania sztucznej inteligencji, która koncentruje się na tym, jak powinna wyglądać AI służąca dobru ludzkości. Obejmuje ona myślenie o danych i ich jakości, uwzględnianie zasad etycznych, a także „twarde" IT, które pomaga realizować założenia związane z tymi systemami. W centrum zainteresowania pozostaje człowiek, który jest bezpośrednim beneficjentem, ale i potencjalnym poszkodowanym w związku z działaniem systemu. Odpowiedzialna AI wyraża odpowiedzialność człowieka za człowieka, a realizuje się poprzez odpowiednie decyzje projektowe, nadzór i kontrolę oraz wykorzystywanie AI. Wszystko to powinno się odbywać w zgodzie z ustalonymi zasadami (wyrażonymi m.in. w formie przepisów zawartych w rozporządzeniu AI Act, które będzie obowiązywać w UE), nad którymi trwa międzynarodowa dyskusja.

**PB:** AI zmieni wiele obszarów naszego życia – od edukacji przez pracę „białych kołnierzyków". To niesie olbrzymie możliwości i musimy szybko nauczyć się z nich korzystać. Żyjemy w kulturze, która ceni bezpieczeństwo i na gwałtowną zmianę reaguje dużym niepokojem, a czasem nawet paniką. Widać to w wypowiedziach i wywiadach celebrytów AI, którzy straszą, czy to utratą pracy czy przejęciem kontroli przez AGI (*Artificial General Intelligence*

– ogólna sztuczna inteligencja). Naszym wyzwaniem jest opanować ten lęk i zacząć się uczyć, jak wykorzystać i jak tworzyć nowe rozwiązania bazujące na AI.

**MN:** Wyzwaniami są: brak świadomości, czym jest AI i jakie niesie ze sobą ryzyka; szum informacyjny, który sprowadza dyskusję i debatę na niewłaściwe tory; brak aktywnych działań w obszarze odpowiedzialnej i godnej zaufania sztucznej inteligencji; niedostateczne inwestycje w AI i inicjatywy wokół; brak kompetencji w sektorze publicznym; niepewność prawna.

**Czy uważacie, że obecna debata publiczna na temat sztucznej inteligencji podąża we właściwym kierunku?**

**MG:** Najczęściej mamy do czynienia ze straszeniem – jak AI odbierze nam pracę i ostatecznie zrobi to, o czym opowiadają takie filmy, jak „Terminator"… Nikt nie mówi, że Google Maps to też jest AI. Ważne jest zrozumienie olbrzymiej różnorodności oprogramowania, które można nazwać *AI-based*. W takim sensie AI bywa różna i takiej debaty chyba jednak nie ma lub prawie nie ma.

**PB:** W Polsce praktycznie nie ma debaty nad możliwościami sztucznej inteligencji. Nie ma żadnego globalnego planu zwiększania kompetencji w obszarze stosowania AI w społeczeństwie, a przecież w innych krajach takie inicjatywy mają miejsce, wystarczy tylko te dobre pomysły kopiować.

**MN:** Za mało mówimy o etyce, w tym kwestiach środowiskowych oraz budowaniu twardych i miękkich kompetencji. Wykorzystywanie przez sektor publiczny AI w ogóle nie podlega szczególnym regułom, a to już spore zagrożenie. Powinniśmy skierować debatę na te tory.

**Jak widzicie możliwość osiągnięcia równowagi między postępem a bezpieczeństwem w rozwoju AI?**

> ***Przemysław Biecek:*** *Obecnie w Polsce nie rozwijamy AI ani na poważnie, ani w dużej skali. Może to i jest bezpieczne, ale nieracjonalne. Do osiągnięcia równowagi potrzebujemy znacznych inwestycji w przedsięwzięcia innowacyjne wysokiego ryzyka oraz w akcje edukacyjne zwiększające poziom umiejętności AI-owych w całym społeczeństwie. Tylko w ten sposób zaczniemy rozwijać technologie wykorzystujące AI w skali, przy której jest sens myśleć o bezpieczeństwie.*

**MN:** Pytanie, czy musimy rozwijać AI za wszelką cenę. Ostatnio Sam Altman powiedział, że rozwój AI będzie wiązał się z jeszcze większymi inwestycjami w superkomputery i tym samym z większym wykorzystaniem energii. Czy naprawdę musimy poświęcać dobro nasze i naszej planety, żeby spełniać czyjeś marzenia? AI ma być dla ludzi, a nie człowiek dla AI. I podstawowa kwestia – czym jest bezpieczna AI, taka, za pomocą której nie wyrządzimy krzywdy? Do tego potrzeba zarówno budowania postaw etycznych, jak i wdrażania twardych przepisów, które posłużą jako bat na tych, którzy chcą ją wykorzystać dla osiągnięcia własnych korzyści kosztem innych. No i może wcale nie potrzebujemy takiego postępu? Może wystarczy nam to, co mamy?

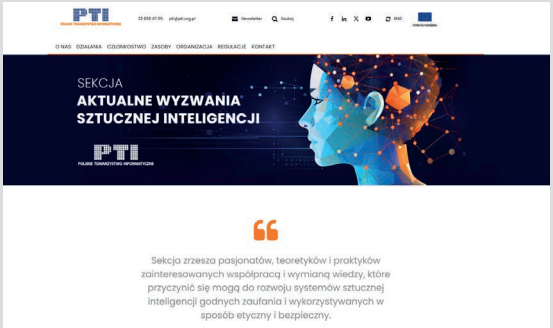
**PB:** Chciałbym, by działanie naszej sekcji zwiększyło liczbę pozytywnych przykładów, jak poprawnie, bezpiecznie i produktywnie stosować narzędzia sztucznej inteligencji, oraz ograniczało zasięg osób straszących nierealnymi wizjami wrogiej AI.

**MN:** Potrzebna nam jest odpowiedzialna, etyczna i godna zaufania sztuczna inteligencja, nie jako kolejny „washing", ale jako realnie i operacyjnie wdrażana koncepcja.

*Agata Cupriak,*
*specjalistka ds. promocji Sekcji AWSI PTI*

**Zapraszamy do współpracy**

**Członkami sekcji mogą zostać zarówno członkowie PTI, jak i osoby niezrzeszone. Do przystąpienia zachęcamy zarówno osoby z wykształceniem technicznym, jak i prawników, psychologów czy socjologów, naukowców, nauczycieli akademickich, etyków i wszystkich tych, którym bliska jest idea tworzenia i wykorzystywania systemów sztucznej inteligencji w sposób odpowiedzialny i godny zaufania. Więcej informacji o Sekcji na stronie: pti.org.pl/awsi**



# Co dalej z polską AI?

**Z zaciekawieniem przyjęliśmy powołanie przez wicepremiera Krzysztofa Gawkowskiego zespołu doradczego PL/AI Sztuczna inteligencja dla Polski. Na początek zespół określił obszary, w których AI może się najbardziej przydać. Są wśród nich bezpieczeństwo, edukacja, zdrowie publiczne, funkcjonowanie państwa oraz kierunki rozwojowe (te, w których AI potrafi wiele zmienić). Wytypowano propozycje rozwiązań i wstępnych projektów, ale na razie (w lutym 2024) brak o nich szczegółowych informacji. Natomiast na stronie zespołu https://aidla.pl można zgłaszać własne propozycje.**

Rozgłos towarzyszący AI spowodował, że w wielu krajach pośpiesznie tworzone są instytucje próbujące podjąć wyzwanie. Nie zawsze są one inspirowane przez rządy, ale zwykle działają zgodnie z powtarzalnym schematem. Na początek starają się zgromadzić jak najwięcej zainteresowanych pod jednym parasolem. Rozległość pokrywanego przez AI obszaru i rozmaitość zastosowań wymaga uczestnictwa przedstawicieli nauki, biznesu, administracji, prawników, etyków, kognitywistów, a – jak się ostatnio przekonaliśmy – nawet artystów. A jeśli chce się uzyskać wymierne rezultaty choćby na skalę krajową, to warto zmobilizować wszystkie dostępne środowiska. Wiedząc już, jakimi siłami się dysponuje, zwykle opracowuje się strategię, poddaje pod publiczną dyskusję i po jej akceptacji realizuje krok po kroku. Czyli raczej mierząc zamiar podług sił, bez romantycznych ekscesów.

> *PL/AI proponuje jednak inny model działania, więc rodzą się pytania. Podsumujmy: konstytuuje się grupa ekspertów (głównie od wdrożeń). Działać mają pro bono, co jest szlachetne i zgodne z patriotycznym etosem, ale na dłuższą metę mało efektywne.*

Zespół wydaje się pełen energii, z zagranicznym otarciem i jest stosunkowo młody. To zaleta, bo pewnie nie pamięta o podejmowanych narodowych przedsięwzięciach w obszarze IT, w których początkowy entuzjazm stopniowo się wy-

**Marek Hołyński**

absolwent Wydziału Elektroniki Politechniki Warszawskiej, profesor Uniwersytetu Bostońskiego i samodzielny pracownik naukowy Massachusetts Institute of Technology. Lata 90. spędził w Dolinie Krzemowej, projektując graficzne stacje robocze oraz opracowując algorytmy grafiki komputerowej. Członek-założyciel PTI, obecnie członek Zarządu Głównego PTI.

czerpywał w zmaganiach z technologicznymi, finansowymi i administracyjnymi barierami, a w końcu spadał do zera.

## Nie zaczynamy od zera

Jak się do takiej inicjatywy odnieść? Czy utworzenie zespołu powinniśmy traktować tylko jako nowe otwarcie po zmianie władzy? I co z działającą od paru lat w strukturach rządowych Grupą Roboczą ds. Sztucznej Inteligencji, która została „utworzona z myślą o wskazaniu działań służą-

cych zapewnieniu w Polsce odpowiednich warunków dla rozwoju zastosowań AI". Zakresy zatem są podobne, choć Grupy wydaje się nieco szerszy. Na swoim portalu Grupa przygotowała kilka raportów, m.in. o wykorzystaniu sztucznej inteligencji w różnych dziedzinach, o relacji między przygotowywanym unijnym AI Act a polskimi regulacjami prawnymi, o zagadnieniach etyki AI.

Formuła Grupy Roboczej jest otwarta i podobno w jej pracach uczestniczyło do tej pory kilkaset osób. Wspierających instytucji zebrało się niewiele, to głównie agendy i fundacje rządowe, więc trudno mówić o szerokiej reprezentacji rynku. Może więc Grupa Robocza nie spełniła pokładanych w niej oczekiwań? Jeśli tak, to czy PL/AI ma ją zastąpić? Albo obie powinny się uzupełniać?

PL/AI też deklaruje otwartość i liczy, że dołączą do niej kolejni uczestnicy. Dołączą? A jeśli nie, bo uznają, że skoro od początku nie zostali zaproszeni, to nie doceniono ich dotychczasowych osiągnięć i poczują się marginalizowani. Lub, co gorsza, dojdą do wniosku, że ktoś bezceremonialnie próbuje zawłaszczyć teren, który dotąd uważali za swój.

Przecież jako kraj nie zaczynamy od zera. W Polsce prace nad AI rozpoczęto ponad 50 lat temu i przez ten czas powstało wiele ciekawych projektów. Polskie uczelnie biorą udział w międzynarodowych programach badawczych, stworzono parę inkubatorów wspierających innowacyjne pomysły w tej dziedzinie. Są gotowe narzędzia do szkolenia zaawansowanych modeli językowych, rozwiązania wykorzystujące AI w medycynie, w detekcji deepfake'ów, a zwłaszcza w grach, które stały się naszą specjalnością. A co z firmami, które już odniosły biznesowy sukces, jak choćby Algolytics, CodiLime czy Landing AI?

## Nosorożec i syte ptaszki

Jak to robią inni, którym się udało? Co złego by nie mówić o kulturze korporacyjnej, przyznać jednak trzeba, że to właśnie wielkie korporacje były kołem zamachowym obecnego tryumfu AI. Nie dość, że stworzyły własne silne grupy badawcze, to jeszcze wykombinowały, jak wypracować istotne mechanizmy wsparcia dla realizacji własnych zamierzeń.

W inicjatywach tej skali ważne było wsparcie w drobiazgach. A te zapewniły małe i średnie firmy. Spotykają się raz czy dwa razy w roku na imprezach zwanych np. Developers Forum. Jednego dnia korporacja mówi o swoich planach, drugiego stowarzyszone firmy i firemki oferują rozwiązania detali, drogi na skróty lub dodatki powodujące, że przygotowywany produkt stanie się bardziej atrakcyjny. Obie strony na tym korzystają. Nosorożec tylko rozdziawia paszczę i ma czyste zęby, a małe ptaszki znajdują w niej pod dostatkiem resztek jedzenia, żeby komfortowo przeżyć.

Niestety, ta oczywista naturalna symbioza umknęła kolejnym polskim oficjalnym strategiom. Wahadło państwowego wsparcia od czasu do czasu przeskakuje skokowo z narodowych potentatów na małe i średnie przedsiębiorstwa, a potem modne staje się znowu hasło „czebole". A przecież od lat funkcjonują systemy, w których to się da pogodzić i zachować równowagę ku satysfakcji obu stron. Otoczkę deweloperów pewnie dałoby się zgromadzić, tylko kto miałby przejąć u nas rolę nosorożca? Krajowego giganta informatycznego się nie dorobiliśmy. Orlen i KGHM mają może kapitał, ale też inne absorbujące sprawy na głowie.

## Pół tygodnia na uczelni, drugie pół w biznesie

Dobrym pomysłem okazała się też dla korporacji współpraca z uczelniami. Na początku traktowano akademickie próby stworzenia „sztucznego mózgu" z pobłażaniem, bo nie kończyły się niczym przydatnym. W połowie lat 70. jednak powstawać zaczęły tzw. systemy ekspertowe dla konkretnych obszarów wiedzy. Okazało się, że w wąskich tematach typu rozpoznawania chorób roślin lub identyfikowania obiektów na zdjęciach satelitarnych AI radzi sobie całkiem nieźle. Nie zastępuje jeszcze człowieka, ale jest dość pomocna.

Nie jest więc niczym zaskakującym, że profesorowie renomowanych uczelni bywają jednocześnie przez dwa, trzy dni w tygodniu pracownikami badawczymi korporacji. Finansowo na tym dobrze wychodzą, a oba miejsca zatrudnienia też nie mają powodów do narzekań. Korporacje zyskały zewnętrzne rzesze studentów i doktorantów, którzy z zapałem podejmują trudne zadania. Przy okazji wyławiają talenty, które po dyplomie warto zatrudnić. Uniwersytety też są zadowolone, bo nie muszą wymyślać sztucznych tematów badawczych, dostają solidne materialne wsparcie i mogą zaoferować studentom atrakcyjną ścieżkę rozwoju zawodowego.

Niby nic nowego. W polskich strategiach rozwoju nauki konieczność współpracy nauki i przemysłu jest postulowana od lat. Gorzej z jej realizacją. Nauka w zasadzie jest chętna, ale biznes grymasi. Narzeka na odziedziczoną po poprzednim systemie bizantyjską hierarchię stopni akademickich, przechył teoretyczny oraz punktozę, które zachęcają do pozoranctwa i nadmuchiwania mało praktycznie istotnych rezultatów. Ten impas próbował z ograniczonym skutkiem przełamać Comarch, ale wynikało to z profesorskiej przeszłości jego prezesa.

## Towarzysze, ludzie to nasz największy skarb

„Polska ma szansę wykorzystać rewolucję sztucznej inteligencji i stać się jednym z 10 najbogatszych krajów na świecie do połowy tego stulecia" – twierdzi inicjator zespołu

PL/AI. Czyżbyśmy znowu zyskali szansę stania się drugą Japonią? To brzmi trochę jak reklamiarski kit wciskany inwestorom przez ubiegające się o fundusze startupy. W dodatku wsparty obietnicami, że da się za pomocą AI uzdrowić wiele trapiących kraj problemów.

Kolejne efektowe marketingowe zaklęcie: „najważniejszym zasobem Polski nie są złoża surowców, tylko programiści". To prawda, że mamy dobrych programistów, którzy zdobywali laury na międzynarodowych konkursach. Spora ich część pracuje już jednak w renomowanych firmach i placówkach badawczych. Czy większość z nich pójdzie w ślady kolegów z zespołu PL/AI i wróci, by pracować za mniejsze albo żadne pieniądze dla dobra kraju?

Nowych absolwentów informatyki przybywa u nas co roku mniej niż ich do bieżących zadań potrzeba.

> *Ambitna wizja dołączenia dzięki AI do pierwszej dziesiątki najbogatszych krajów wymagałaby setek, jeśli nie tysięcy specjalistów z rozmaitych dziedzin. I to najlepszych na świecie, bo jak się zatrudni drugi garnitur, to efekt też będzie drugiej jakości i nie wytrzyma rynkowej konkurencji.*

Sami programiści nie wystarczą, a część nawet może okazać się zbędna, bo AI sama wkrótce będzie zdolna wytworzyć niezłej jakości oprogramowanie.

Koniecznego potencjału ludzkiego nie mieliby nawet Amerykanie, którzy zresztą w Dolinie Krzemowej nie przeważają w sposób zdecydowany. Zatrudnieni są tam eksperci różnych narodowości, którzy chcą pracować w miejscu, gdzie reflektory świecą najmocniej. Gdzie można się wykazać swoimi nieprzeciętnymi umiejętnościami, a ponadto jest kreatywne środowisko, dość pieniędzy na odlotowe projekty i fajna atmosfera. A na dodatek plaże nad oceanem o pół godziny jazdy i w zasięgu po przeciwnej stronie góry Sierra Nevada z topowymi ośrodkami narciarskimi.

## O czym dżentelmeni mówią szeptem?

Niewiele z ministerialnego komunikatu można się dowiedzieć o najważniejszym, czyli zamierzeniach finansowego wsparcia działań wynikających z inicjatywy PL/AI. Na poważne prace rozwojowe i wdrożeniowe w AI wydawane są na świecie ogromne pieniądze – oceny analityków co parę miesięcy wzrastają o kolejne miliardy dolarów. W obecnym budżecie państwa ciężko się takiej pozycji doszukać. Trudno więc nie zadać podstawowego pytania: mamy kasę?

Zarobki dobrego specjalisty AI są teraz mniej więcej na poziomie 7 według hierarchii wynagrodzeń korporacyjnych działów *human resources*. To oznacza płacowe widełki od miliona dolarów do dwóch rocznie, uwzględniając w tym standardowe apanaże typu stock options (możliwość zakupu akcji firmy po atrakcyjnej cenie), firmowy samochód i opiekę medyczną. Wybitni eksperci, od których zależy sukces projektu, mogą oczekiwać dodatkowo przedpłaty na dom i pokrycia kosztów relokacji łącznie z przewozem fortepianu.

Ściągnięcie takich ludzi do Polski nie byłoby łatwe. Miejsce zostało wadliwie zaprojektowane: morze umieszczono na północy, co nie zachęca do kąpieli, a w górach na południu śnieg szybko topnieje i nie da się często pojeździć. Zamienienie tych lokalizacji byłoby trudne nawet po przesunięciu na ten cel niewykorzystanego budżetu Centralnego Portu Komunikacyjnego. A potrzebna jest jeszcze dyspozycyjna pula rodzinnych domków na przedmieściach i angielskojęzycznych szkół dla dzieci przybyszów. No i przydałaby gwarancja, że idąc po zakupy nie oberwie się kijem bejsbolowym ze względu na kolor skóry.

## Siła napędowa informatyki

Powyższe uwagi mogą wyglądać na typowy decel, ale warto mieć świadomość tego, z jak trudnym zadaniem przyszłoby się zmierzyć, żeby się, jak zwykle, nie skończyło po amatorsku.

AI rozwijała się falami i przy każdym wzmożonym zainteresowaniu próbowano u nas zmierzyć się z tym tematem, zatem obecnie inicjatywy nie zaskakują. Pierwsze próby podjęto akurat w mało sprzyjających czasach, bo priorytetem było zastosowanie komputerów do sterowania obrabiarkami. Z tamtej perspektywy AI wydawała się kosztownym marnotrawstwem na pograniczu *science fiction*.

W drugiej połowie lat 70. pierwsze światowe sukcesy systemów eksperckich spowodowały, że potencjał AI trochę w Polsce doceniono. Miesięcznik „Informatyka" był wtedy jedynym pismem w naszej branży, więc to na jego łamach zadebiutował stały dział pod nazwą „Sztuczna inteligencja". Tam właśnie pojawiła się relacja ze spotkania 24 maja 1978 r. w auli Wydziału Elektroniki Politechniki Warszawskiej zatytułowana „Siła napędowa informatyki" (ten buńczuczny tytuł odnosił się właśnie do AI).

Ciekawa w obecnym kontekście może być konkluzja tamtej narady pionierów AI sprzed 45 lat. „Zagadnienia sztucznej inteligencji są realnymi i przydatnymi w praktyce tematami badawczymi. Z satysfakcją stwierdzić też można istnienie w Polsce dość licznej grupy osób, która się tymi sprawami zajmuje i ma spore osiągnięcia. Mniej przyjemny jest brak mecenasa – instytucji, która mogłaby nadzorować i koordynować te prace." Skoro mamy teraz Ministerstwo Cyfryzacji, to może tym razem taką instytucję uda się wyznaczyć.

# E-doręczenia na rozdrożu

**Po kolejnym przesunięciu terminu uruchomienia krajowego systemu doręczeń elektronicznych na nowo rozgorzała dyskusja na temat braku gotowości poczty i narzekania na pomysł wprowadzenia płatnego maila. To tylko odpryski znacznie poważniejszej sprawy: samej koncepcji i jej hermetycznej realizacji.**

**Michał Tabor**

partner i członek Zarządu Obserwatorium.biz. Od 2002 r. zajmuje się wdrażaniem rozwiązań podpisu elektronicznego i identyfikacji elektronicznej. Autor wielu rozwiązań z zakresu uwierzytelnienia, podpisu elektronicznego i dokumentu elektronicznego funkcjonujących w Polsce (w szczególności mechanizmu składania deklaracji podatkowych i Profilu Zaufanego ePUAP). Uczestniczył w procesie legislacji i wdrażania rozporządzenia Parlamentu Europejskiego i Rady w sprawie identyfikacji elektronicznej i usług zaufania (eIDAS). Kierował zespołem odpowiedzialnym za przygotowanie projektu Krajowego Schematu Identyfikacji Elektronicznej, a także koncepcji węzła identyfikacji elektronicznej w Polsce. Członek Komitetu Technicznego ESI ETSI zajmującego się standaryzacją mechanizmów podpisu elektronicznego, odpowiedzialny za opracowanie standardów technicznych dla interfejsów europejskiego portfela cyfrowej tożsamości oraz standardów dla wykorzystania certyfikatów na potrzeby dyrektywy PSD2. Rzeczoznawca PTI, ekspert PIIT w zakresie identyfikacji, uwierzytelnienia i podpisu elektronicznego, ekspert Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji ENISA. Posiadacz certyfikatu CISSP.

Doręczenia elektroniczne nie są polskim pomysłem. Obowiązujące od 2016 r. rozporządzenie eIDAS określa ramy prawne dla funkcjonowania e-doręczeń w całej Unii Europejskiej i wprowadza definicję rejestrowanego doręczenia elektronicznego, kwalifikowanego rejestrowania doręczenia elektronicznego oraz uznanie prawne dla dowodów wystawianych przez tę usługę. Już od ośmiu lat możemy korzystać z usług zaufania doręczeń elektronicznych w całej Unii Europejskiej, a sądy są zobowiązane akceptować dowody z takiego doręczenia, co więcej – jeżeli doręczenie jest realizowane za pomocą kwalifikowanej usługi, to niosą skutek prawny taki sam, jak dla listu poleconego.

Na przekór wszystkim, którzy próbują porównywać doręczenia elektroniczne do działania e-maili, posłużę się innym przykładem: rozwiązaniem, z którego wszyscy korzystamy i nie wyobrażamy sobie bez niego funkcjonowania rynku, czyli elektronicznym przelewem bankowym. Jeszcze 30 lat temu prawie wszyscy pracownicy odbierali swoje pensje w okienku u księgowej, dziś korzystamy z dobrodziejstwa przelewów elektronicznych. Posługiwanie się bankowością, – dziś praktycznie całkowicie elektroniczną, wymaga kilku nieskomplikowanych czynności. Musimy zarejestrować się w dowolnym banku, otrzymać numer konta bankowego, pobrać hasła i zainstalować aplikację do bankowania. Otrzymywanie i wykonywanie przelewów wymaga podania numeru konta bankowego (IBAN) adresata przelewu. Nieważne, w którym banku w Unii Europejskiej adresat przelewu ma konto, wykonujemy przelew w swoim banku i najdalej w kolejnym dniu roboczym adresat otrzyma pieniądze na własnym koncie we własnym banku. Zarówno wysyłający przelew, jak i jego odbiorca mają możliwość potwierdzenia informacji o wysłanym i otrzymanym przelewie. Nadzór nad systemem bankowym zapewnia bezpieczeństwo i pewność naszych transakcji, a dzięki szybkim usługom bankowym mógł rozwinąć się nowoczesny biznes, w tym handel elektroniczny i usługi online.

W środowisku informatyków koncepcja e-doręczeń jest raczej znana (już trzy lata temu w ówczesnym „Biuletynie PTI" Wacław Iszkowski pisał o nadmiernie skomplikowanej realizacji systemu – przyp. red.). Tytułem przypomnienia krótkie wprowadzenie, czym są elektroniczne przesyłki rejestrowane i jaką funkcję mają pełnić w bezpieczeństwie obrotu gospodarczego i procesach administracji. Przebieg procesu doręczenia elektronicznego pokazujemy na rys. 1.

## E-doręczenie jak list polecony

Usługę e-doręczenia można porównać do notariusza, potwierdzającego przekazanie przesyłki elektronicznej pomiędzy uczestnikami komunikacji. List polecony od listu zwykłego różni wydanie potwierdzenia nadania i doręczenia.

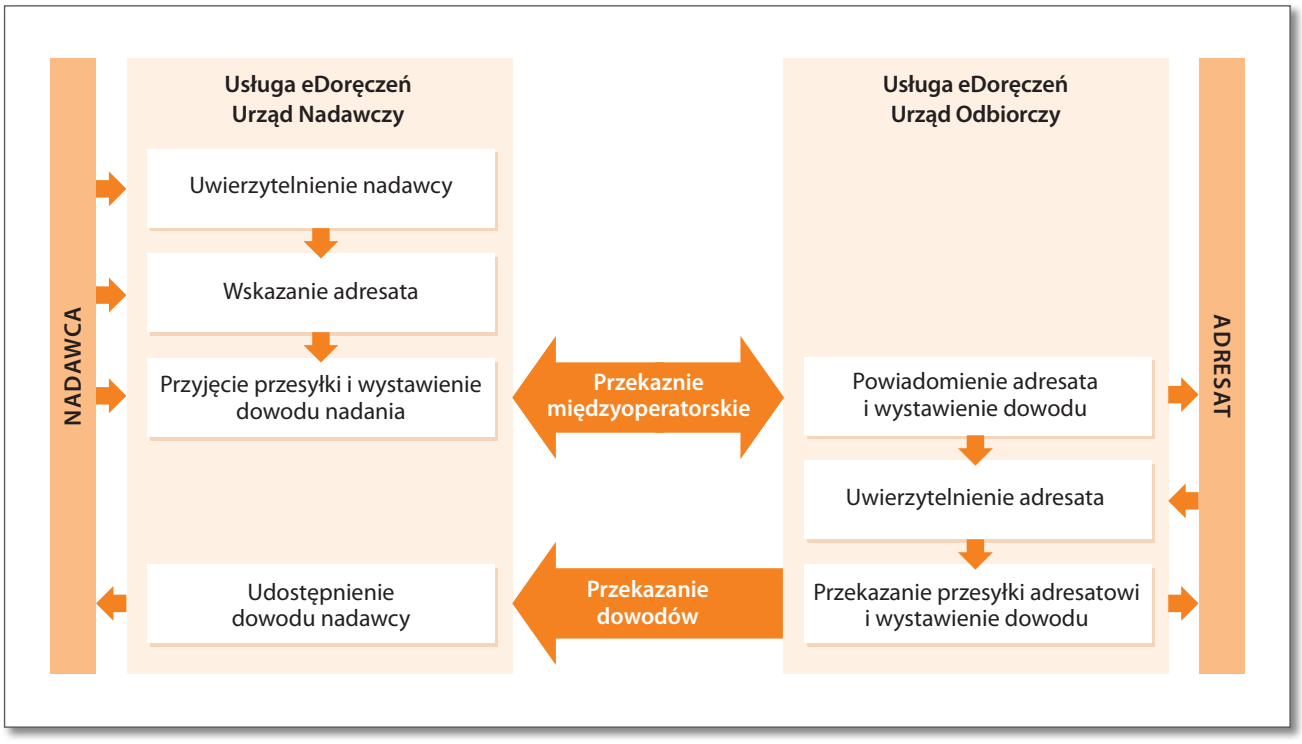
czenia jako dokumentów potwierdzających czynności faktyczne, dowody te uznają sądy. Doręczenie elektroniczne też dostarcza dowody nadania i doręczenia, a także wiele dowodów dodatkowych, takich jak potwierdzenie notyfikacji adresata o oczekującej przesyłce. Prawnie dowody doręczenia elektronicznego uznawane są przez sądy w całej UE, natomiast dowody z kwalifikowanych usług doręczenia są traktowane tak, jak te pochodzące z listów poleconych.

Dowód doręczenia zawiera dane nadawcy i odbiorcy, dokładny czas wystawienia dowodu oraz czynności, którą potwierdza. Pozwala na potwierdzenie integralności przesyłki, uniemożliwia wyparcie się, że dowód dotyczy innej przesyłki lub innej treści. Każdy dowód zawiera pieczęć elektroniczną dostawcy usługi oraz jest oznaczony kwalifikowanym znacznikiem czasu. Weryfikacja dowodów jest możliwa za pomocą publicznie dostępnych narzędzi – tych samych, które służą do weryfikacji podpisów elektronicznych.

Przepisy prawa i normy techniczne wymagają, aby usługa doręczenia elektronicznego zapewniała poufność każdej przesyłki, uniemożliwiającą osobom innym niż strony komunikacji zapoznanie się z jej treścią. Jednocześnie dostawcy usługi są zobowiązani do zapewnienia ochrony przed utratą oraz jakąkolwiek nieupoważnioną zmianą w treści przesyłki. Bardzo ważnym wyróżnikiem, który stanowi o bezpieczeństwie usługi, jest obowiązkowa identyfikacja stron transakcji, która powoduje, że odbiorca zawsze będzie wiedział, kto jest nadawcą przesyłki, a także nadawca może mieć pewność, że przesyłka trafi do zdefiniowanego odbiorcy.

## Dlaczego się potykamy?

Skoro od 8 lat funkcjonują przepisy europejskie dotyczące doręczeń elektronicznych, warto zadać sobie pytanie, dlaczego nie udało się wdrożyć systemu e-doręczeń w Polsce. Głównym powodem jest brak powszechnego obowiązku akceptacji doręczeń elektronicznych przez podmioty publiczne i firmy. Aby e-doręczenia mogły funkcjonować, zarówno nadawca, jak i adresat takiego doręczenia muszą być zarejestrowani w systemie doręczeń elektronicznych i mieć możliwość nadawania oraz odbierania przesyłek. Zarówno nadawca, jak i adresat są zidentyfikowanymi uczestnikami systemu doręczeń elektronicznych, nie ma mowy o ich anonimowości. Warto jeszcze raz podkreślić, że nadawcą i adresatem może być osoba prawna, bez wskazywania osoby fizycznej działającej w jej imieniu. W celu zapewnienia jednolitego modelu identyfikacji przyjęto, że zarówno nadawcom, jak i adresatom będzie nadawany identyfikator – nazywany adresem do doręczeń elektronicznych. Identyfikator ten jest unikatowy i jednoznacznie wskazuje nadawcę lub adresata oraz pozwala na określenie dostawcy usługi zaufania, który utrzymuje konto nadawcy lub odbiorcy. Adres do doręczeń elektronicznych to nie jest adres email, bardziej przypomina IBAN; ważną jego cechą jest to, że adres do doręczeń nie może zmienić właściciela – zawsze jest przypisany do tej samej osoby fizycznej lub prawnej. W Polsce wydawaniem adresów do doręczeń elektronicznych zajmuje się minister właściwy do spraw informatyzacji, co więcej – prowadzi bazę adresów elektronicznych, która pozwala urzędom wyszukać adres główny – służący do komunikacji z urzędami.




Rys. 1. Przebieg procesu doręczenia elektronicznego

Warunkiem powszechnej akceptacji doręczeń elektronicznych jest ustanowienie obowiązku posiadania konta umożliwiającego odbieranie doręczeń elektronicznych przez każdy podmiot publiczny oraz każdego przedsiębiorcę.

## Czy e-doręczenia mają sens

Odpowiedzi na to pytanie należy szukać w doświadczeniach innych krajów Unii Europejskiej. Dobrym przykładem jest włoski system doręczeń elektronicznych, w którym każda firma musi posiadać zarejestrowane konto doręczeń elektronicznych (nazywane elektronicznym adresem firmy i równorzędne z adresem fizycznym). Konto takie może być obsługiwane przez dowolnego z osiemnastu dostawców usługi *Posta elettronica certificata*. Przepisy zobowiązały firmy we Włoszech do posiadania dostępu do e-doręczenia oraz do przekazywania faktur za pomocą tego systemu. Obecnie doręczenia elektroniczne są podstawowym medium komunikacji gospodarczej w tym kraju, wszystkie faktury przesyłane pomiędzy partnerami gospodarczymi muszą być przekazywane za pomocą systemu e-doręczeń. Obowiązek korzystania z nich dotyczy także wielu innych dokumentów służbowych i administracyjnych. Do włoskiego systemu doręczeń podłączonych jest ponad 15 mln podmiotów, które rocznie wysyłają ponad 3 mld przesyłek.

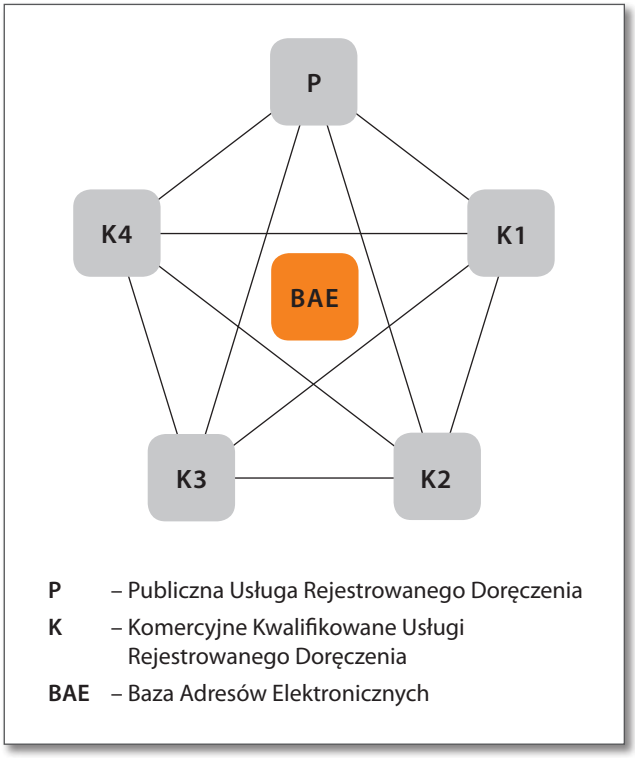
W innych krajach Unii Europejskiej, w szczególności we Francji i Hiszpanii, także rozwinęły się usługi doręczeń elektronicznych, głównie związane z obrotem gospodarczym i obowiązkowym przekazywaniem dokumentów gospodarczych pomiędzy podmiotami biznesowymi.

## E-doręczenia po polsku

W Polsce obowiązki związane ze stosowaniem doręczeń elektronicznych wprowadziła ustawa o doręczeniach elektronicznych z 18 listopada 2020 r. Głównym jej założeniem jest obowiązek posiadania adresu do doręczeń elektronicznych przez wszystkie podmioty administracji publicznej oraz poprzez spółki zarejestrowane w Krajowym Rejestrze Sądowym. Obowiązek ten miał wejść w życie pod koniec grudnia 2023 r., został jednak przesunięty na ostatni kwartał roku 2024.

Świadczenie usług doręczeń elektronicznych w Polsce może być realizowane przez kwalifikowanych dostawców tej usługi, a także przez operatora wyznaczonego, którym jest Poczta Polska. Do czasu powstania tego artykułu następujące podmioty potwierdziły gotowość do świadczenia usługi rejestrowanego doręczenia elektronicznego:

| Dostawca | Usługa | Status |
|---|---|---|
| Poczta Polska S.A. | PURDE | publiczna usługa |
| Poczta Polska S.A. | Q-Doręczenia | usługa kwalifikowana |
| Asseco Data Systems | CERTUM e-Doręczenia | usługa kwalifikowana |
| KFJ Inwestycje Sp. z o.o. | Elektroniczne doręczenia | usługa kwalifikowana |
| Autenti Sp. z o.o. | e-Doręczenia Autenti | usługa kwalifikowana |
| PWPW S.A. | eDO Post | potwierdzony audyt usługi kwalifikowanej |




Rys. 2. Krajowy system doręczeń elektronicznych

Generalne założenia funkcjonowania e-doręczeń w Polsce przedstawia rys. 2. Wszystkie usługi rejestrowanego doręczenia elektronicznego podłączone do systemu komunikują się między sobą i umożliwiają wzajemną wymianę informacji. Każda z usług posiada dostęp do Bazy Adresów Elektronicznych umożliwiającej wyszukanie podmiotów publicznych oraz firm, a także do rejestru umożliwiającego wskazanie, która z usług obsługuje adresata doręczeń elektronicznych.

Co do zasady przepisy ustawy nie wprowadzają monopolu dla doręczeń elektronicznych i każdy przedsiębiorca może korzystać z dowolnej usługi wybranej na rynku. Natomiast podmioty publiczne nie mają wyboru i muszą korzystać z publicznej usługi rejestrowanego doręczenia. Jednocześnie publiczna usługa zapewnia możliwość darmowego podłączenia się przedsiębiorców i osób fizycznych w celu wysyłania przesyłek do i z podmiotów publicznych.

To wyróżnienie usługi publicznej i tworzenie ułomnych kont do doręczeń, które nie pozwalają na szerokie kontaktowanie się w systemie doręczeń, jest jednym z głównych powodów opóźnienia w realizacji projektu.

Założenie projektowe zbudowania usługi publicznej przez Pocztę Polską, jako spółkę skarbu państwa, miało być ważnym krokiem do wdrożenia doręczeń elektronicznych. Inicjatywa w tym zakresie stanowiła sygnał, że – niezależnie od zainteresowania podmiotów komercyjnych – usługa powstanie. Zasadne jest jednak pytanie, czy w przyszłości właściwe będzie utrzymanie tego monopolu dla usług publicznych, a nie dywersyfikacja i dopuszczenie nadzorowanych podmiotów komercyjnych.

Uważam również, że publiczna usługa powinna być Kwalifikowaną Usługą Rejestrowanego Doręczenia, ponieważ dopiero ten status gwarantuje właściwe wykonywanie zadań podmiotu, odpowiedni model bezpieczeństwa oraz sprawowanie nadzoru przez Ministra Cyfryzacji.

## Wąskie gardło

Ministerstwo Cyfryzacji przez ostatnie cztery lata budowało interfejs dostępu do publicznej usługi doręczeń elektronicznych i mechanizmy obsługi darmowych kont. Wymyślało kolejne ulepszenia, które miały pomóc w rozwoju usługi z definicji ułomnej, bo nieumożliwiajacej szerokiego wykorzystania biznesowego. Praktycznie Minister Cyfryzacji nie budował systemu doręczeń elektronicznych obejmującego wielu dostawców, a skupił się jedynie na współpracy z Pocztą Polską oraz rozbudowie usług własnych, realizowanych przez Centralny Ośrodek Informatyki.

Do **niedawna** w dyskusji na temat e-doręczeń pomijany **był** fakt, że e-doręczenia to nie tylko usługa Ministra Cyfryzacji i Poczty Polskiej. Warto zauważyć zmianę w podejściu ministra Michała Gramatyki, zapowiedzianą w artykule https://www.gazetaprawna.pl/firma-i-prawo/artykuly/9458811,gramatyka-beda-wazne-zmiany-w-e-doreczeniach-chodzi-o-terminy.html

Tak silne skupienie się na usłudze publicznej i jej promocji ogranicza możliwość rozwoju usług komercyjnych. Należy jednocześnie zwrócić uwagę, że barierą rozwoju usługi publicznej jest ograniczenie dostępu do niej jedynie do interfejsów udostępnianych przez Ministra Cyfryzacji. To interfejsy świadczą o doświadczeniu użytkownika, jego odbiorze, wymagają ciągłych badań i szybkiego adresowania bieżących potrzeb, co zawsze było domeną usług komercyjnych, a nie decyzji urzędniczych.

## Co dalej?

W Parlamencie Europejskim uchwalono właśnie nowelizację rozporządzenia eIDAS, która wprowadza wiele nowych rozwiązań, takich jak Europejski Portfel Tożsamości Cyfrowej oraz usługi atrybutów. Jednocześnie nowelizacja wskazuje na konieczność powstania aktów implementujących interoperacyjność usługi doręczenia elektronicznego, które ma się stać paneuropejską siecią wymiany elektronicznej korespondencji rejestrowanej. Doręczenia elektroniczne staną się narzędziem nie tylko do wymiany przesyłek krajowych, lecz także formalnej korespondencji pomiędzy partnerami zagranicznymi.

Wdrażane w Polsce rozwiązania stanowić będą podstawę rozwoju europejskiej sieci, a polskie firmy mogą być znaczącymi graczami w dziedzinie doręczeń elektronicznych. Chodzi o to, aby za pomocą e-doręczeń mógł się kontaktować każdy pracownik ze swoim pracodawcą i każdy konsument ze swoim telekomem, dostawcą mediów lub bankiem. Rzecz idzie także o to, żeby podmioty publiczne nie drukowały pism wysyłanych do firm i innych urzędów.

Nie ulega wątpliwości, że dostępność e-doręczeń elektronicznych powinna być powszechna. Wzajemna interoperacyjność musi gwarantować, że przesyłka dotrze do adresata. Dlatego niezbędna jest współpraca wszystkich zainteresowanych stron, wymiana informacji, wspólne testowanie i rzeczywisty nadzór organów powołanych do wdrożenia systemu e-doręczeń.

Bardzo ważne w tym modelu jest zachowanie równości partnerów w Krajowym Systemie Doręczeń Elektronicznych, nadzór Ministra Cyfryzacji i dialog, w którym ustalanie standardów jest działaniem kolektywnym. Krokiem w dobrą stronę jest zapowiedź Ministra Cyfryzacji współpracy z rynkiem dostawców kwalifkowanych usług zaufania rejestrowanego doręczenia elektronicznego.

Końcowy sukces zależy od tego, czy użytkownicy będą mieli swobodę wyboru zależną od ich preferencji, ułatwień i usług dodanych.

# Cyber–raporty

**Zgodnie ze standardami obowiązującymi audytorów systemów informatycznych certyfikowanych przez międzynarodową organizację ISACA, raport z audytu – by był wiarygodny – ma być sporządzony w sposób dokładny, jasny, zwięzły, obiektywny, konstruktywny i terminowy, zaś przedstawione ustalenia muszą być poparte dostatecznymi i odpowiednimi dowodami opartymi na uznanych kryteriach oceny.**

Jestem certyfikowanym audytorem i pisząc moje artykuły również stosuję standardy raportowania. Od autorów raportów dotyczących w różnym stopniu cyberbezpieczeństwa oczekuję równej staranności w przedstawianiu swoich ustaleń i wynikających z nich rekomendacji.

## Raport MIT

We wrześniu 2023 r. NASK pochwaliła się na swojej stronie szóstym miejscem Polski w rankingu „The Cyber Defense Index 2022/23" opublikowanym przez MIT Technology Review, dwumiesięczniku założonym w 1899 r., będącym własnością prestiżowej uczelni Massachusetts Institute of Technology (https://www.technologyreview.com/2022/11/15/1063189/the-cyber-defense-index-2022-23/). W ocenie poziomu cyberbezpieczeństwa uwzględniono cztery kategorie: infrastruktura krytyczna, zasoby cyberbezpieczeństwa, zdolności organizacyjne oraz regulacje i otoczenie prawne w tym obszarze. Dane użyte w analizie pochodziły – jak zaznaczyli autorzy – z wielu publicznie dostępnych zasobów instytucji międzynarodowych i globalnych oraz ankiety przeprowadzonej wśród ponad tysiąca osób kadry kierowniczej odpowiedzialnych za cyberbezpieczeństwo w swoich organizacjach.

Ponieważ raporty NIK, które przywołałam w moim artykule w nr 4/2023 Domeny, oraz inne publicznie dostępne polskie opracowania nie wskazują na tak optymistyczny stan polskiego cyberbezpieczeństwa, napisałam do autorów raportu, by podali *primary and secondary sources of information about Poland's cybersecurity* wykorzystane w rankingu. Ku mojemu zaskoczeniu odmówili podania listy dokumentów źródłowych i innych danych, na podstawie których ocenili cyberbezpieczeństwo w Polsce. Uznałam raport za niewiarygodny i nie zamierzałam do niego wracać. Niestety, pozycja Polski w rankingu jest bezrefleksyjnie przytaczana w domenie publicznej, chociażby w audycji „Czy istnieją skuteczne metody ochrony naszych danych osobowych w sieci?" na portalu GEEKWEEK (https://geekweek.interia.pl/nauka-co-slychac/news-cyfrowy-swiat-nam-zagraza-warto-postawic-na-bezpieczenstwo,nId,7248689).

## Raporty polskie

W związku z powołaniem nowego rządu, różne organizacje pozarządowe przygotowały swoje raporty poświęcone cyfryzacji, poruszające także kwestie cyberbezpieczeństwa. Jeden z nich był prezentowany 16 stycznia br. na posiedzeniu Komisji Cyfryzacji Sejmu RP (https://www.sejm.gov.pl/Sejm10.nsf/PosKomZrealizowane.xsp?komisja=CNT#5). Dokument o nazwie „Raport otwarcia w polityce cyfrowej" zawiera bardzo ogólne przemyślenia autorów dotyczące wybranych zagadnień cyfryzacji oraz ich rekomendacje na lata 2024–2027 (https://law4growth.com/raport-otwarcia-w-polityce-cyfryzacji/). W kwestii cyberbezpieczeństwa oprócz banalnych stwierdzeń typu „Zagrożenia cybernetyczne nie znają granic" czy „W XXI wieku inwestycje w cyberbezpieczeństwo są niezbędne" autorzy rekomendują transpozycję dyrektyw EKŁE i NIS2 oraz stworzenie Krajowego Centrum Przetwarzania Danych jako remedium na wszystkie cyber-zagrożenia. O ochronie danych osobowych nie wspominają zaś ani słowem. Autorzy nawet nie zanotowali, że zamiast przywołanego przez nich GIODO mamy obecnie UODO. W dokumencie nie znajdziemy też żadnej listy materiałów

źródłowych i referencyjnych. Toteż żadna z osób obecnych na posiedzeniu nie pochwaliła raportu. Wręcz przeciwnie, wielu uczestników, którzy zabrali głos, ocenili go bardzo krytycznie. Moja generalna uwaga była jedna: zanim autorzy napiszą kolejny raport o cyfryzacji i cyberbezpieczeństwie, niech popracują pół roku przy wdrożeniu i utrzymaniu średniej wielkości systemu informatycznego, najlepiej w jednostce samorządowej. Przekonają się na własnej skórze, jak praktyczne są ich zalecenia.

Drugi raport o nazwie „Państwo podmiotowej cyfryzacji. Diagnoza i kierunki niezbędnych działań" (https://www.batory.org.pl/publikacja/panstwo-podmiotowej-cyfryzacji--diagnoza-i-kierunki-niezbednych-dzialan/) został przedstawiony osobiście nowemu Ministrowi Cyfryzacji (https://www.gov.pl/web/cyfryzacja/koniec-pierwszej-serii-konsultacji-w-ministerstwie-cyfryzacji). Zawiera zestaw postulatów odnoszących się do cyfryzacji państwa, w tym „potrzeby poprawy zarządzania procesem cyfryzacji i wdrażania technologii". Jest w nim bardzo dużo o sztucznej inteligencji. Niestety ani razu nie pojawia się słowo „cyber" z jakimkolwiek rozwinięciem. Autorzy sygnalizują tylko potrzebę wprowadzenia mechanizmów zabezpieczających przed nieuprawnionym dostępem instytucji publicznych do danych obywateli i obywatelek. Są odwołania do innych dokumentów, ale tylko autorstwa zaprzyjaźnionych organizacji. Trzy razy użyto słowa „należy", z kolei słowa „powinien" z odmianami użyto 17 razy na zaledwie dziewięciu stronach publikacji. Mnie szczególnie zaintrygował zapis, że stworzenie organu ds. dostępu do danych dotyczących zdrowia przywróci zawiedzione zaufanie do państwa w obszarze ochrony zdrowia – wszystko przy zachowaniu wysokich standardów ochrony prywatności. Autorzy nie podają jednak, jakie to są standardy. Za to zaznaczają, że Urząd Ochrony Danych Osobowych obecnie nie jest w stanie sprostać nawet zadaniom wynikającym z RODO, a od 2024 r. powinien dodatkowo realizować zadania wynikające z DSA.

Obszaru ochrony zdrowia dotyczy trzeci raport „Dane medyczne w pracy lekarza – stan obecny & pożądane zmiany", przygotowany przez NIL IN – Sieć Lekarzy Innowatorów stworzoną przy Naczelnej Izbie Lekarskiej (https://nil.org.pl/uploaded_files/art_1707132900_raport-dane-medyczne--w-pracy-lekarza.pdf). Dokument prezentuje zagadnienia dotyczące regulacji prawnych w obszarze przetwarzania danych medycznych w Polsce. Tym razem jest wiele odwołań do innych opracowań, w tym raportów NIK. Jest też dużo o cyberbezpieczeństwie oraz statystyka, która podaje w wątpliwość ocenę polskiego cyberbezpieczeństwa wystawioną przez MIT, przynajmniej w sektorze zdrowia: „Pomimo szeregu wymogów związanych z ochroną danych medycznych, dostępne badania wskazują, że nie są one egzekwowane w zadowalającym stopniu. Jak wynika z analizy Centrum e-Zdrowia, w ponad połowie podmiotów zidentyfikowano potrzeby w zakresie cyberbezpieczeństwa (55,9%), przy czym najczęściej zgłaszały je szpitale (86,1%). Wskazywane potrzeby badanych placówek w zakresie cyberbezpieczeństwa to przede wszystkim odporność na cyberataki (68,9%), zwiększenie ochrony danych osobowych (65,9%) oraz poprawa stanu wiedzy o zagrożeniach informatycznych wśród pracowników/kierownictwa jednostki (59,4%)". Zastanawia rekomendacja zapisana w rozdziale 4. „Dane medyczne w pracy lekarza – jak być powinno?", w podrozdziale 4.4 Bezpieczeństwo: „Zasadniczy ciężar związany z zapewnieniem wysokiego poziomu ochrony danych powinien spoczywać na dostawcach sprzętu i oprogramowania, którzy są podmiotami wyspecjalizowanymi, znającymi bieżący stan wiedzy technicznej. Odpowiedzialność lekarza powinna ograniczać się do wyboru sprzętu i oprogramowania, którego dostawca zapewnia spełnianie takiego standardu. Lekarz powinien mieć w związku z tym dostęp do dokumentów, które pozwolą mu zweryfikować i łatwo ocenić dostawców oraz zakres ich odpowiedzialności."

Czyżby autorzy raportu, którzy są prawnikami, bazowali na stanowisku wyrażonym przez WSA w Warszawie w wyroku II SA/Wa 2259/21 z 19 kwietnia 2022 r. ? Dla przypomnienia: sąd w składzie trzyosobowym w uzasadnieniu wyroku uznał, że wybór usługi świadczonej przez profesjonalny podmiot, jakim jest pewna renomowana korporacja, z całą pewnością gwarantuje stosowanie przez ów podmiot przetwarzający odpowiednich środków organizacyjnych i technicznych ochrony danych osobowych wymaganych przez RODO (o sprawie napisałam w nr 1/2023 Domeny). Pozostaje pytanie, jakie dokumenty zostaną uznane – i przez kogo – za wystarczające do weryfikacji i łatwej oceny dostawców. Na razie tylko jedna korporacja amerykańska ma uznanie sądu.

## Raporty RODO

W raporcie NIL IN-u zamieszczono tabelę z postulatami związanymi z wykorzystywaniem danych w pracy lekarza. Jako sposoby osiągnięcia postulatu „Dane przetwarzane przez lekarza powinny być bezpieczne", podano m.in.:

- zrealizowanie działań w obszarze bezpieczeństwa, takich jak te przewidziane w Programie rozwoju e-zdrowia w Polsce do 2027 r.;

- wypracowanie krajowej implementacji dyrektywy NIS2 w konsultacji ze środowiskiem medycznym, by nowe wymogi mogły być skutecznie wdrożone przez podmioty wykonujące działalność leczniczą;

- stosowanie kodeksu postępowania z art. 40 RODO.

Zgodnie z RODO kodeks postępowania wymaga wdrożenia odpowiednich mechanizmów monitorowania i egzekwowania zgodności z rozporządzeniem m.in. środków i procedur, o których mowa w art. 24 i 25, oraz środków zapewniających bezpieczeństwo przetwarzania, o których mowa w art. 32. Mechanizmy obejmują regularne przeprowadzanie audytów, których wynikiem jest stosowny raport.

**Przejrzałam kodeksy przyjęte dla małych placówek medycznych i szpitali oraz kodeksy dla doradców podatkowych, firm badania opinii i rynku, centrów handlowych, biobanków i branży hotelarskiej złożone do zatwierdzenia. W kwestii środków technicznych i organizacyjnych zapewnienia odpowiedniego stopnia bezpieczeństwa danych osobowych:**

- **kodeks postępowania dla sektora ochrony zdrowia dotyczący podmiotów wykonujących działalność leczniczą i podmiotów przetwarzających, zwany kodeksem dla szpitali, odwołuje się do uznanych norm/standardów międzynarodowych, w tym norm PN-ISO/IEC z serii 27000 dotyczących systemów zarządzania bezpieczeństwem informacji (lista jest zawarta w załączniku nr 6);**
- **kodeks dla biobanków odwołuje się do Rozporządzenia o Krajowych Ramach Interoperacyjności i polskiej normy PN-ISO/IEC 27001 oraz przedstawia własne zalecenia techniczne;**
- **kodeks dla firm badania opinii i rynku obejmuje własny Program Kontroli Jakości Bezpieczeństwa Informacji;**
- **pozostałe kodeksy podają własne listy zabezpieczeń.**

Dlaczego audytorzy mają problem? Otóż zgodnie ze standardem audytu 1008 Kryteria, audytorzy są zobowiązani dla badanego przedmiotu sprawy wybierać kryteria oceny, które są obiektywne, kompletne, relewantne, wiarygodne, mierzalne, powszechnie uznawane oraz zrozumiałe przez lub dostępne dla wszystkich czytelników i użytkowników raportu. W sferze cyberbezpieczeństwa podstawowe zasady są uniwersalne i identyczne dla wszystkich branż i sektorów na całym świecie i są zawarte w powszechnie uznawanych standardach, normach i dobrych praktykach opracowanych przez wiodące organizacje zrzeszające specjalistów z całego świata. Audytorzy sięgną po nie w pierwszej kolejności. Dopiero w drugiej lub trzeciej wykorzystają kodeksowe programy czy listy, chyba że okażą się niekompletne bądź nieadekwatne.

## Raport o laptopach

Od samego początku programu „Laptop dla ucznia" zwracałam szczególną uwagę na kwestię cyberbezpieczeństwa rozdawanych laptopów. Na posiedzeniu Komisji Cyfryzacji w dniu 14 grudnia 2022 r. podsekretarz stanu w KPRM Paweł Lewandowski zapowiadał, że laptopy będą przekonfigurowane przez dostawców sprzętu, „aby samorządy nie musiały jakoś szczególnie zaprzątać sobie głowy dodatkowym instalowaniem różnego softu czy konfigurowaniem dodatkowym tych komputerów". Zapytałam o zestaw oprogramowania, który będzie instalowany i czy obejmuje środki bezpieczeństwa/cyberbezpieczeństwa. Pan Lewandowski odpowiedział, że wykaz oprogramowania będzie w rozporządzeniu projektowanym przez Ministerstwo Edukacji i Nauki, zaś laptopy będą musiały „posiadać oprogramowanie, które będzie przynajmniej w sposób podstawowy chroniło przed zagrożeniami, jakie czekają na użytkownika Internetu".

Program antywirusowy nie znalazł się na liście oprogramowania instalowanego na pamięci masowej lub udostępnianego do nieodpłatnego pobrania przy rozpoczęciu użytkowania, zawartej w załączniku do Rozporządzenia Ministra Edukacji I Nauki z dnia 28 grudnia 2022 r. zmieniającego rozporządzenie w sprawie podstawowych warunków niezbędnych do realizacji przez szkoły i nauczycieli zadań dydaktycznych, wychowawczych i opiekuńczych oraz programów nauczania (Dz.U. z 2022 r. poz. 2811). Wpisano tylko wymóg techniczny wbudowanych mechanizmów bezpieczeństwa dostępu do danych. Ostatecznie Ministerstwo Cyfryzacji i Centrum Obsługi Administracji Rządowej, które prowadziło przetarg, zrezygnowali z wymogu instalowania jakiegokolwiek oprogramowania na zamówionych laptopach, by uniknąć zarzutów o wgrywanie przy okazji aplikacji szpiegującej.

Dzieci dostały fabrycznie nowy sprzęt z systemem operacyjnym MS Windows 11 Pro Edu i wygrawerowanym orzełkiem oraz portal www.laptopdlaucznia.gov.pl, prowadzony przez NASK-PIB, gdzie w Centrum informacji umieszczono Bazę wiedzy, obejmującą m.in. listę darmowego oprogramowania do wykorzystania na laptopach. O proponowanym programie pocztowym BlueMail napisałam w numerze 4/2023 Domeny.

Reszta listy nie obejmuje programu antywirusowego. Nie ma nawet informacji, czy jest potrzebny. Wprawdzie MS Windows 11 ma wbudowany moduł zabezpieczeń, jednak warto o nim poinformować beneficjentów programu i podpowiedzieć, jak skonfigurować różne opcje zabezpieczeń udostępnionych przez firmę Microsoft.

Jedyny poradnik „ABC Cyberbezpieczeństwa" do pobrania w sekcji „Edukacja" portalu zawiera ponad 150 alfabetycznie ułożonych haseł wraz z definicjami. Już widzę, jak dziesięciolatki i ich rodzice rzucają wszystko i biorą się za lekturę 105-stronicowego opracowania, zanim uruchomią swój nowy sprzęt. Nie rozumiem, dlaczego do każdego pudełka z laptopem nie włożono ulotki formatu A4 z podstawowymi zasadami cyberbezpieczeństwa. Mam całą kolekcję różnych materiałów o cyberbezpieczeństwie opracowanych dla dzieci przez NASK i inne podmioty za pieniądze publiczne (krajowe i unijne). Szczególny wysyp nastąpił w pandemii. Wystarczyło wybrać, dostosować, wydrukować i rozdać,

a wersję elektroniczną udostępnić na portalu. Wszystkie media powielałyby informację i samą ulotkę. Zasięgi byłyby niebotyczne. Cóż, zabrakło wyobraźni, myślenia i prawdziwej chęci uświadamiania o cyber–zagrożeniach.

**Pojawiło się już pierwsze podsumowanie Programu „Laptop dla ucznia" (https://www.gov.pl/web/cyfryzacja/program-laptop-dla-ucznia-nie-mial-zabezpieczonego-finansowania). Jak podało Ministerstwo Cyfryzacji w komunikacie z 8 lutego 2024 r., problemy merytoryczne programu „Laptop dla ucznia" obejmują:**

- **brak przygotowania systemowego do wykorzystywania urządzeń przez dzieci w szkole oraz w domu – brak strategii cyfryzacji edukacji przygotowanej przez poprzednie kierownictwo MEiN. Brak wytycznych dla nauczycieli i szkół, jak wykorzystywać komputery przez dzieci;**
- **brak przygotowania szkół do włączenia komputerów w działania edukacyjne – brak infrastruktury LAN, infrastruktury przyłączy elektrycznych, brak bezpiecznego systemu przechowywania laptopów, które stanowią własność rodziców;**
- **brak wsparcia uczniów w zakresie higieny cyfrowej.**

**Informacja na temat realizacji programów „Laptop dla ucznia" oraz „Laptop dla nauczyciela" została także przedstawiona 22 lutego 2024 r. na burzliwym posiedzeniu wspólnym Komisji Edukacji i Komisji Cyfryzacji Sejmu RP.**

Laptopy są własnością rodziców/opiekunów prawnych uczniów IV klas oraz nauczycieli. Korzystanie z prywatnego sprzętu do nauki zdalnej zostało już wypracowane w pandemii. Tym razem laptopy są przekazywane z ewidentnym założeniem, że będą noszone z domu do szkoły i ze szkoły do domu. W związku z tym konieczne jest wyjaśnienie m.in. następujących kwestii:

- Czy regulamin Ogólnopolskiej Sieci Edukacyjnej dopuszcza podłączanie do OSE prywatnych laptopów?
- Czy Polityka Bezpieczeństwa Informacji i Ochrony Danych Osobowych szkoły dopuszcza podłączanie prywatnych laptopów do sieci szkolnej i jej zasobów?
- Czy opieka nad prywatnymi laptopami jest w zakresie obowiązków informatyka szkolnego wynikającym z jego/jej umowy o pracę, umowy o dzieło bądź umowy o świadczeniu usług?
- Co z ochroną danych osobowych na prywatnych laptopach uczniów i nauczycieli?

Przypomnę, że w samym Ministerstwie Edukacji wprowadzono ścisłe reguły pracy zdalnej:

- pracownikom na czas pracy zdalnej udostępniono laptopy służbowe; pracownicy mieli też możliwość zabrania stacjonarnych komputerów służbowych do domu; mogą również pracować w domu na laptopach prywatnych, po uprzednim skonfigurowaniu ich przez pracowników zespołu IT (odpowiedź na interpelację nr 3268);
- praca w miejscu zamieszkania może odbywać się wyłącznie z wykorzystaniem komputera (laptopa) służbowego oraz zgodnie z zasadami wynikającymi z obowiązującego Systemu Zarządzania Bezpieczeństwem Informacji w MEN (odpowiedź na interpelację nr 9654).

Szkoły zasługują na cyberbezpieczeństwo wzorowane na zasadach wprowadzonych w ministerstwie. Ministerstwo Cyfryzacji zapowiedziało w przywołanym komunikacie, że w przyszłym roku uczniowie otrzymają urządzenia mobilne, zaś rodzaj sprzętu, niezbędne oprogramowanie i zabezpieczenia będą przedmiotem analizy oraz dyskusji z partnerami społecznymi i rodzicami. Do dyskusji warto włączyć lokalnych administratorów sieci szkolnych i inspektorów ochrony danych placówek oświatowych.

Wielokrotnie pisałam o cyfrowym zaufaniu, czyli *digital trust*.

> *Zaufanie do cyfryzacji obejmuje także zaufanie do publikowanych raportów o cyfryzacji i o stanie cyberbezpieczeństwa.*

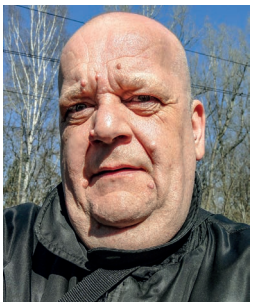
Ich wiarygodność jest istotna, skoro mają nam pomagać w podejmowaniu decyzji i inicjowaniu działań w celu zabezpieczenia naszych danych, zapewnienia naszej prywatności i właściwego korzystania z technologii informatycznych. Tym bardziej w dobie internetu pełnego dezinformacji i fake newsów.

Wszystkie informacje zawarte w artykule są podane według stanu na dzień 23 lutego 2024 r.

*Joanna Karczewska*

# Znikający GPS

**Konflikt Rosji z Ukrainą zmienił nasze postrzeganie wielu zagadnień, zwłaszcza w obszarze wojny elektronicznej. Bezprecedensowe działanie Rosji zmierzającej od początku wojny do całkowitego zakłócenia cywilnej i wojskowej łączności telekomunikacyjnej na Ukrainie nie tylko pokazało, że agresor nie liczy się z żadnymi skutkami swoich działań, lecz także ujawniło duże możliwości Rosjan w tym zakresie operacji wojennych.**



**Jacek Grabowski**

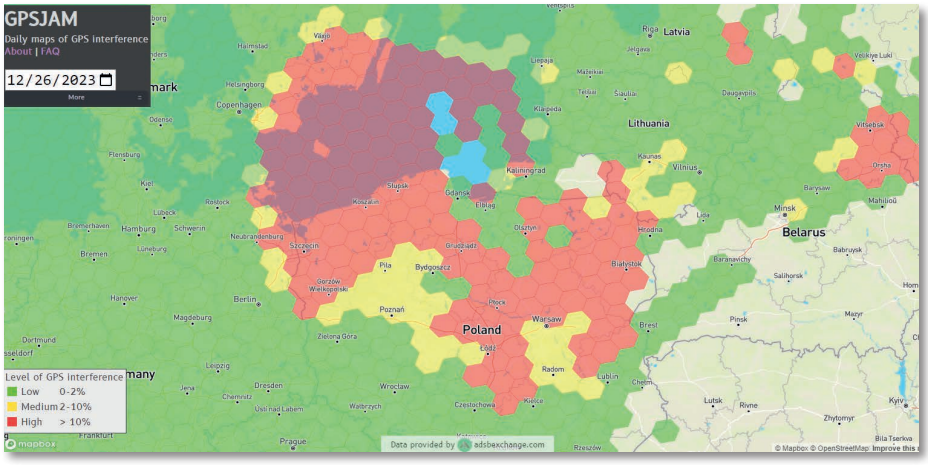
z wykształcenia specjalista gazownictwa i górnictwa naftowego, przygodę z informatyką rozpoczął w końcu lat 80. XX wieku od współpracy z wydawnictwem „Lupus", gdzie publikował teksty głównie w dwutygodniku „PCkurier" i miesięczniku „Enter". Współtwórca pierwszego w Polsce informatycznego czasopisma B2B „MRK" (1997). Były redaktor naczelny miesięcznika „Reset", współpracownik wielu innych tytułów (magazyn „WWW", „IT Reseller", „Komputer Świat"). Obecnie freelancer, współpracuje m.in. z warszawską komunikacją miejską.

Eskalacja napięcia poprzez deklarację przystąpienia do NATO krajów skandynawskich spowodowała szybki „odwet" Rosji objawiający się zakłóceniami sygnału GPS nad Finlandią. Już 5 marca 2022 r. fińscy piloci cywilni odnotowali poważne problemy z nawigacją. Na szczęście ich samoloty były wyposażone w alternatywne względem GPS systemy nawigacyjne, które pozwoliły kontynuować lot. Litewskie linie lotnicze musiały jednak z powodu zakłóceń odwołać kilka lotów do Finlandii i z powrotem. Sporadyczne zakłócenia GPS w obszarze Morza Bałtyckiego zdarzały się od tego czasu coraz częściej. Rosja nigdy oficjalnie nie przyznała się do prowadzenia działań utrudniających krajom NATO dostęp do systemu nawigacyjnego. Tym niemniej kolejna eskalacja zakłóceń nastąpiła w okolicy świąt Bożego Narodzenia 2023 r. Wtedy też anomalie sygnału GPS na rozległym terenie zauważono wtedy także nad Polską.

## Od Olsztyna do Lublina

Głównym źródłem informacji o zakłóceniach sygnału GPS stał się internetowy serwis *gpsjam.org*, który pokazuje na mapie obszary, gdzie występują nieprawidłowości w odbiorze sygnału GPS. 26 grudnia 2023 r. po raz pierwszy na mapie zakłóceń pojawiły się czerwone plamy na terenie Polski.

Tego dnia zakłócenia objęły olbrzymi obszar od Danii przez Morze Bałtyckie do praktycznie całego zachodniego wybrzeża morskiego Polski. Wdarły się głęboko na teren naszego kraju, zahaczając o Warszawę i Mazowsze, na południu dochodząc aż na wysokość Częstochowy i Lublina. Po tym incydencie przez pewien czas panował względny spokój, lecz już 10 stycznia 2024 r. znów obszar zakłóceń nad Polską sięgnął na południe aż do Łodzi, a na wschodzie znowu do Lublina. Przez kolejne dni zakłócenia GPS w Polsce występowały „wyspowo", w znacznie mniejszym zakresie, ale 19 stycznia br. znów doszło do nasilenia i obszar zakłóceń ponownie sięgnął od Danii aż do Gorzowa, Łodzi i Lublina.




*Źródło: hjttps://gpsjam.org*

**Poniższe linki ilustrują największe zakłócenia GSP nad Polską:**

**14/02/2024** https://gpsjam.org/?lat=52.29651&lon=19.43511&z=4.2&date=2024-02-14

**10/02/2024** https://gpsjam.org/?lat=52.29651&lon=19.43511&z=4.2&date=2024-02-10

**02/02/2024** https://gpsjam.org/?lat=52.29651&lon=19.43511&z=4.2&date=2024-02-02

**19/01/2024** https://gpsjam.org/?lat=52.29651&lon=19.43511&z=4.2&date=2024-01-19

**16/01/2024** https://gpsjam.org/?lat=52.29651&lon=19.43511&z=4.2&date=2024-01-16

**10/01/2024** https://gpsjam.org/?lat=52.29651&lon=19.43511&z=4.2&date=2024-01-10

**26/12/2024** https://gpsjam.org/?lat=52.29651&lon=19.43511&z=4.2&date=2023-12-26

Po kilku dniach spokoju sytuacja powtórzyła się 2 lutego, a następnie 10 i 14 lutego. Gdy kończyłem tekst, mapa *gpsjam.org* nad Polską była chwilowo czysta.

Ujawnienie informacji o zakłóceniach w grudniu ubiegłego roku spowodowało wysyp różnych komentarzy. Radio Zet łączyło przyczynę zakłóceń z odbywającymi się w tym okresie manewrami NATO, inne media donosiły także o „ćwiczącym" w rejonie królewieckim oddziale wojsk walki elektronicznej wyposażonych m.in. w system Borisoglebsk-2, w skład którego wchodzą dwa pojazdy dowodzenia oraz cztery pojazdy ze stacjami zagłuszającymi wyposażone w anteny.

Borisoglebsk

*Źródło: Wikimedia Commons*

System taki z powodzeniem może zakłócić sygnały radiowe na sporym obszarze, wymaga tylko podłączenia do źródła prądu, by po 15 minutach przygotowań zacząć pracę.

Kształt mapy zakłóceń pokazuje dużą powtarzalność granic terytorium objętego anomaliami sygnału. Mniemanie, że generuje je jakiś system umieszczony w rejonie królewieckim nie jest więc pozbawione podstaw. Tym niemniej do dzisiaj nie ma żadnego oficjalnego potwierdzenia, kto i w jaki sposób zakłócał GPS w naszym kraju i okolicach. Na Rosję wskazuje jednak nie tylko obszar zakłóceń, lecz także wiele innych poszlak.

## Rosja straszy czy się boi?

John Wiseman, ekspert z portalu *gpsjam.org*, zwrócił uwagę, że skala zakłóceń jest bezprecedensowa. Według niego wskazuje to, że są one praktycznie na pewno wynikiem celowych prób zagłuszania sygnału lub ćwiczeń wojskowych. Szef szwedzkiej Wojskowej Służby Wywiadu i Bezpieczeństwa MUST generał broni Thomas Nilsson w grudniu ubiegłego roku mówił: „obserwacji dotyczących zakłóceń GPS dokonywaliśmy już wcześniej w związku z rosyjskimi ćwiczeniami wojskowymi. Uważam, że jest to przykład działania hybrydowego, którego celem jest tworzenie niepewności". Z kolei pułkownik Joakim Paasikivi, wykładowca z Zakładu Strategii Szwedzkiej Akademii Obrony, powiedział, że „za zakłóceniem działania systemu GPS w regionie Bałtyku mogła stać Rosja, której celem było pokazanie, że potrafi przeprowadzać tego rodzaju akcje". Stwierdził też, że Rosja już wcześniej ingerowała w północnoeuropejski system GPS. Również pułkownik Eero Rebo z estońskich wojsk obrony terytorialnej wysnuł zbliżoną teorię: „Rosja prawdopodobnie nie ma wystarczającej obrony powietrznej, więc aby uspokoić swój naród, zdecydowała się po prostu na działania zastępcze". Rebo zaznacza, że stwarza to dodatkowe ryzyko w lotnictwie, a także w żegludze i nawiązując do niedawnych ataków ukraińskich dronów na infrastrukturę w Rosji dodaje: „tłumienie sygnału GPS w rzeczywistości nie wpływa na działania dronów. Reżim Putina robi to raczej po to, aby pokazać, że robi się coś, by bronić kluczowych dla niego aktywów".

Także służby niemieckie przyznały, że od pewnego czasu w rejonie Morza Bałtyckiego poważnie zakłócany jest sygnał nawigacji GPS. W związku z tym Bundesnetzagentur (Federalna Agencja ds. Sieci), odpowiedzialna m.in.

za ochronę elektromagnetyczną, wszczęła dochodzenie w porozumieniu z Bundeswehrą. Niemieckie służby mają zdolność precyzyjnego zlokalizowania źródeł zakłóceń, jednak żadne informacje dotyczące wyników ich badań nie są udostępniane publicznie. Podobnie jak w przypadku wspomnianych służb szwedzkich i estońskich, podejrzenia Niemców kierują się w stronę Rosji, która prawdopodobnie chroni swoje miasta pewnego rodzaju tarczą zagłuszającą, mającą skutecznie zabezpieczać przed atakami, takimi jak te przeprowadzane przez Ukrainę za pomocą dronów. Dla rosyjskiej armii zakłócenia GPS nie mają znaczenia, gdyż korzysta ona z własnego systemu nawigacji satelitarnej GLONASS, wspieranego w zakresie synchronizacji naziemnym radiowym systemem Czajka, a do prowadzenia działań wojskowych może ona również używać dużej liczby rozproszonych w sieci Internet TCP/IP publicznych serwerów NTP (NTPPOOL). Od wybuchu wojny ich widoczna liczba wzrosła ze 150 do 200 (25 proc.) i nadal wzrasta. Eksperci ze Szwecji szacują, że liczba ta może być 2–3-krotnie większa, ponieważ Rosjanie umiejscawiają swoje serwery NTP również poza granicami Rosji i pod domenami zagranicznych firm (źródło: https://gist.github.com/mutin-sa/eea1c396b1e610a2da1e5550d94b0453).

## Jamming i spoofing

Choć istnieje wiele teorii i prób wytłumaczenia domniemanego postępowania Rosji prowadzącego do błędnego działania NATO-wskiego system nawigacyjnego, to w rzeczywistości oficjalnie nie znamy nawet rodzaju zakłóceń, które występowały na naszym terenie. Istnieją bowiem dwie metody zakłócania GPS: zagłuszanie sygnału (*jamming*) i fałszowanie wskazań odbiorników poprzez podawanie nieprawdziwych danych (*spoofing*).

Głównym celem zagłuszania jest uniemożliwienie dekodowania jakiegokolwiek sygnału GPS przez odbiorniki. Zakłócenia mogą jednak doprowadzić nawet do uszkodzenia odbiornika. Najprostszą metodą *jammingu* jest nadawanie fali elektromagnetycznej na częstotliwości nośnej L1 (1575,42 MHz). Przeprowadzone badania pokazują, że zależnie od tego, czy emitowane zakłócenia mają charakter ciągły czy impulsowy oraz czy częstotliwość fali zakłócającej pozostaje niezmienna, czy też lekko zmienia się w czasie, *jamming* może być bardziej lub mniej efektywny. Niezależnie jednak od tego, jakiego sygnału użyjemy, skutek pozostaje ten sam – odbiornik nie jest w stanie podać nam czasu UTC ani swojej pozycji. Obie wielkości są ze sobą ściśle związane, ponieważ aby wyznaczyć pozycję, odbiornik musi najpierw pozyskać z systemu satelitarnego GPS czas. Wiele wskazuje na to, że zakłócenia GPS obserwowane na terytorium Polski były spowodowane właśnie przez *jamming*.

Warto zauważyć, że Rosja ma niemałe doświadczenie w zagłuszaniu fal radiowych. Już pod koniec minionej dekady Izrael doświadczał podobnych zakłóceń GPS, które docierały tam z sąsiedniej Syrii, objętej wojną domową, wspieraną przez siły zbrojne Putina. Zakłócenia ruchu lotniczego i silnie zautomatyzowanego przemysłu oraz rolnictwa w Izraelu były bolesnym doświadczeniem. Tradycja zakłócania sygnałów radiowych przez Rosję jest jednak znacznie dłuższa. Już w czasach „zimnej wojny" dysponowała rozległą siecią „zagłuszarek" skutecznie eliminujących z eteru wiadomości nadawane przez zachodnie i amerykańskie stacje radiowe typu „Radio Wolna Europa" czy „Głos Ameryki". Choć oficjalnie „zagłuszarki" wyłączono w 1989 r., pracujący w nich specjaliści znaleźli łatwo zatrudnienie w armii. W efekcie Rosja dysponuje kilkoma różnego rodzaju systemami zagłuszania i zakłócania fal radiowych, których kryptonimy budzą respekt wśród ekspertów NATO. Poza wspomnianym już systemem Borisoglebsk-2 jest to np. system Krasucha C-4 użyty w Syrii i w Ukrainie do zagłuszania telefonii komórkowej.

Krasucha

*Źródło: Wikimedia Commons*

Są to systemy stacjonarne, rozmieszczone na samochodach lub ciągnikach gąsienicowych, jednak wiadomo, że Rosjanie dysponują także co najmniej jednym przenośnym systemem zagłuszającym mieszczącym się w plecaku.

W *spoofingu* Rosjanie również okazują się mistrzami. W 2017 r. francuski tankowiec Atria płynący do rosyjskiego portu Noworosyjsk napotkał niespodziewane problemy z nawigacją GPS. Urządzenia nawigacyjne tankowca wskazywały, że znajduje się on na lądzie, na terenie lotniska w pobliskim uzdrowisku Gelendżyk. Inne statki na Morzu Czarnym również zgłaszały niejednokrotnie podobne anomalie. Ponieważ (według Aleksandra Nawalnego) w Gelendżyku znajduje się tajna rezydencja Putina, Amerykanie wysnuli z tego zdarzenia teorię, że naziemne

stacje spoofingowe chronią przed „namierzeniem" miejsca przebywania rosyjskiego prezydenta. Przypuszcza się także, że powodem spoofingowania GPS w tamtej okolicy może być port w Noworosyjsku, ważny z punktu widzenia wojskowego. To, co chroni, może również służyć do ataku jako broń ofensywna. Zbyt zależna dziś od GPS automatyka przemysłowa jest podatna na desynchronizacje. Okazuje się, że źródło czasu i synchronizacja opierają się najczęściej na GPS, a są one niezbędne dla każdej rozproszonej architektury IT. Jest to szczególnie ważne dla telekomunikacji, w energetyce, transporcie (kierowanie ruchem lotniczym i kolejowym). Z GPS do synchronizacji korzysta: administracja publiczna, banki, wojsko i policja. Jej desynchronizację można wywołać *jammingiem* i *spoofingiem* sygnałów GPS. Działa to jak arytmia serca. Może boleć (incydent bezpieczeństwa) lub prowadzić do złego samopoczucia obniżającego naszą wydajność pracy, ale może również prowadzić do poważnych zapaści, a nawet śmierci. Za pomocą desynchronizacji można wywołać poważne awarie prowadzące do blackoutu w energetyce i telekomunikacji.

## Co z tym zrobić?

Przeciętnemu człowiekowi zakłócenia GPS mogą wydawać się właściwie mało szkodliwe, efektowne czerwone plamy na mapie, ciekawe jako sensacja wojenna w mediach, ale mające mały wpływ na życie. Czasami przy okazji zakłóceń GPS zauważyć możemy, jak nasz samochód „znosi z drogi" i podążamy poza jej obszarem. Na mapach telefonów komórkowych obserwować możemy dziwne skoki naszej pozycji.

> *W rzeczywistości system nawigacyjny GPS jest podstawą wielu systemów gospodarki cywilnej, dawcą czasu wzorcowego UTC, istotnym elementem wszystkich form transportu publicznego i indywidualnego.*

Nawigacja GPS zastępuje żyroskopy i używa się jej: do stabilizacji torów jazdy, w medycynie nuklearnej, odpowiada za stabilność komunikacji radiowej, wspiera systemy informacyjne. Stosuje się ją w komunikacji miejskiej, na kolei, w żegludze i lotnictwie. Często nie zdajemy sobie sprawy, że od czasu z GPS zależą nawet systemy baz danych SQL i ich archiwizacja.

Tak więc zakłócenia GPS występujące na dużym obszarze i z taką intensywnością mogą budzić poważny niepokój. Nie są to zakłócenia występujące stale, ale ich powtarzalność i losowe momenty występowania osłabiają dziś zaufanie do GPS-u, powoli „podmywają" fundamenty współczesnej informatyki (IT) i przemysłu OT (technologie operacyjne), które dziś bazują wyłącznie na rozproszonej architekturze. Sam system GPS trudno byłoby dziś ad hoc czymś zastąpić.

Niepokój budzi również to, że w Polsce głównym źródłem informacji o zakłóceniach tak istotnego dla naszej gospodarki systemu nawigacyjnego stał się internetowy serwis *gpsjam.org* stworzony w sumie amatorsko przez jedną osobę na podstawie publicznych danych zgłaszanych przez linie lotnicze!

> *Siłą rzeczy nasuwa się pytanie, czy nasz kraj dysponuje systemem umożliwiającym wykrycie anomalii działania GPS-u, a jeśli nie, to czy taki system nie powinien w obecnej sytuacji być jak najprędzej zakupiony.*

System taki, o nazwie ARGOS, proponuje i może w trybie pilnym wdrożyć w Polsce firma ELPROMA (https://www.elpromaelectronics.com/category/elproma-time/) – polski producent serwerów czasu NTP/PTP, którego urządzenia posiadają atestacje NATO. Proponowane rozwiązanie posiada funkcję generowania alarmów z powiadamianiem wskazanego centrum zarządzania kryzysowego, które powiadomi przedmiotowe dla NIS2 infrastruktury krytyczne energetyki, telekomunikacji, transportu, banki i GPE o trwającym ataku radiowym *jamming/spoofing* GPS, wskazując siłę i zakres terytorialny ataku. To pozwoli uruchomić procedury cyberbezpieczeństwa i zapewni autonomię pracy systemów informatycznych, odcinając je od GPS na czas trwania ataków radiowych zakłócania.

Są jeszcze dwie ważne kwestie. Pierwsza to mało znany fakt istnienia dyrektywy prezydenckiej G.W. Busha z 2004 r., umożliwiającej wyłączenie amerykańskiego systemu GPS Navstar w dowolnym regionie świata, a więc również nad Polską. Świadomość takiej możliwości daje Polsce długi czas, który krajowa gospodarka powinna wykorzystać na przygotowanie się do pracy w rzeczywistości, którą dziś nakreśla nowa światowa geopolityka i ataki radiowe zakłócania GPS. Druga to miła niespodzianka i fakt, że na dwa tygodnie przed pierwszym incydentem GPS nad Polską, Główny Urząd Miar RP oddał do użytku na początku grudnia 2023 r. naziemny system synchronizacji czasu o nazwie eCzasPL. Jest to nieodpłatna dla krajowego przemysłu usługa naziemnej synchronizacji UTC z użyciem protokołów NTP i PTP IEEE1588. Głównym wykonawcą systemu jest firma ELPROMA, która wcześniej zrealizowała narodowe systemy czasu i synchronizacji, w tym obsługę synchronizacji energetyki i telekomunikacji w Europie, w krajach Azji i w Afryce.

# Jak chronić infrastrukturę krytyczną przed desynchronizacją?

**Konflikt między Rosją a Ukrainą zmienił nasze postrzeganie wojny elektronicznej. Wydaje się, że umiejętne zakłócanie sygnałów GPS może być bardzo skuteczną bronią cybernetyczną, ponieważ pozwala blokować podstawowe funkcje PNT (*Positioning, Navigation and Timing*) każdego odbiornika satelitarnego. Umożliwia to skutecznie destabilizowanie infrastruktury krytycznej państwa, bo zależność systemów informatycznych IT i przemysłowych OT od funkcjonalności PNT, a zwłaszcza od systemów GPS, wzrasta.**

Okazuje się, że obecnie łatwiej jest destabilizować pracę całych systemów IT/OT niż włamywać się do dobrze zabezpieczonych i odizolowanych od internetu sieci wewnętrznych. Najważniejsze sieci infrastrukturalne używają precyzyjnego czasu, którym można manipulować.

## Zagrożenia dla infrastruktury krytycznej

Desynchronizacja, czyli rozsynchronizowanie zegarów w rozproszonych systemach, jest w stanie zaburzyć parametry pracy na różnych poziomach sprzętu, oprogramowania systemowego i aplikacji.

> *Desynchronizacja sieci infrastrukturalnych IT/OT, objętych dyrektywą NIS2, może prowadzić do awarii o nieprzewidywalnych konsekwencjach. Coraz częściej pojawiają się ostrzeżenia przed wielką awarią, która może wywołać efekt domina.*

Rozsynchronizowanie czasu w urządzeniach sieciowych prowadzi też do zaburzenia obliczeń opóźnień w przepływie informacji siecią TCP/IP. W przypadku rozproszonej architektury współczesnych systemów IT/OT, oznacza to groźbę użycia zdezaktualizowanych danych i odrzucenia prawidłowych informacji. To determinuje nowy rodzaj zagrożenia i definiuje dwa rodzaje cyberataków destabilizacji, przed którymi chroni firma ELPROMA (www.elpromaelectronics.com) :

- **Time Synchronization Attack** (atak na czas)
- **Time Delay Attack** (atak na opóźnienia w sieci)

Obserwowane na przestrzeni ostatniej dekady awarie zawsze w jakimś stopniu wskazywały na udział desynchronizacji. Wśród wielu możliwości zagrożeń na szczególną uwagę zasługują te dotyczące odbiorników satelitarnych GNSS.

**Istnieją dwie metody zakłócania GPS: zagłuszanie oryginalnego sygnału *jamming* i fałszowanie wskazań odbiorników poprzez podawanie nieprawdziwych danych w depeszach, tzw. *spoofing*. W samej kategorii *jammingu* możemy rozróżnić podgrupy *jammingu PRN, chirp jammingu, coded jammingu* itp. Podobnie w *spoofingu* istnieją podgrupy synchronicznego *spoofingu*, a ostatnio Niemcy opublikowali informację o identyfikacji nowego rodzaju *spoofingu*, który nazwali okrężnym (*circle spoofing*). Rozpoznanie nowych rodzajów zagrożeń atakami RF jest istotne dla stworzenia antidotum i wytworzenia odporności układów odbiorczych GNSS na zagrożenie. Tym właśnie zajmują się eksperci z polskiej firmy ELPROMA.**

## Rosyjska aktywność

Prowadzone od 2016 r. przez niezależne zespoły USNO[1] i C4ADS[2] obserwacje wskazały miejsce źródła zagłuszającego GPS w rejonie Morza Czarnego. Do badań wykorzystano dopplerowskie pomiary sensorem STP-H5[3] zainstalowanym na stacji kosmicznej ISS orbitującej 400 km nad powierzchnią Ziemi. Na co dzień służył on do badań jonosfery, ale „w wolnych chwilach" wykonywał dodatkowe pomiary. Za pomocą wbudowanego w pełni programowalnego odbiornika satelitarnego SDR (Software Defined Radio) rejestrowano sygnały GPS wiązek L1 i L2 z częstotliwością próbkowania 6 Mbps. Niezinterpretowane surowe dane, przekazane na Ziemię specjalnym 60-sekundowym slotem transmisyjnym, zostały poddane rozszerzonej analizie sygnałowej DSP. W analizie wykorzystano sztuczną inteligencję i uczenie maszynowe. Badania skoncentrowano na rejonie Morza Czarnego, gdzie odnotowywane były w połowie poprzedniej dekady interferencje sygnałów GPS, a szczególnie dawał się we znaki *spoofing*. Wiele wcześniejszych raportów żeglujących tam statków handlowych opisywało anomalia pracy odbiorników GPS. Niektórzy kapitanowie twierdzili, że ich statki nawigacja przenosiła o kilkaset kilometrów dalej – do Moskwy.

Kiedy ISS przelatywała nad obszarem Morza Czarnego podejrzanym o *spoofing* GPS, wartość depeszy LNAV była odczytywana jako zero na wszystkich dostępnych kanałach odbiornika GPS. Zera znikały po opuszczeniu obszaru zakłóceń. Nie było wątpliwości co do celowego zakłócania GPS, jednak nie pasowało to do klasycznego *jammingu*, ponieważ dekodowana informacja nie była zakłócona losowym szumem częstotliwości nośnej L1. Nie był to też typowy *spoofing* GPS, bo nie wykazano fałszowania telemetrii nawigacyjnej depeszy LNAV, a jedynie jej wyzerowanie. Analiza spektralna w widmie częstotliwości L1 1575,42 MHz potwierdziła obecność sztucznego sygnału zakłócenia. Amerykanie nazwali ten rodzaj zakłócenia *coded jamming*. Dzisiaj uważa się, że jest to forma cyberataku DoS, blokująca funkcjonalność PNT odbiornika GPS z chwilą, gdy musi on wykonać zimny start lub reakwizycję satelitów GPS. Kodowany *jamming* stanowi więc potencjalną i niewidoczną dla odbiornika GPS pułapkę.

W 2018 r. Amerykanie pokusili się o określenie lokalizacji źródła *jammingu*. Pomiar był skomplikowany, zależał od parametrów ruchu stacji ISS po orbicie. Wynik obliczeń wszystkich zaskoczył: źródło *jammingu* GPS „znad Morza Czarnego" znajdowało się o kilkaset kilometrów dalej, w basenie Morza Śródziemnego. Okazało się, że nadajnik zagłuszający umiejscowiony był na terenie rosyjskiej bazy wojskowej w Syrii[4]. Wygląda na to, że zakłócenia GPS na terenie Polski są prawdopodobnie spowodowane podobnym *jammingiem* GPS wywoływanym przez Rosję z jej terytorium.

## PNT w ryzach

Często błędnie zakładamy, że czas i pozycja odbiornika GNSS są przesyłane z kosmosu, a odbiornik satelitarny działa jak karta sieciowa LAN. W rzeczywistości parametry PNT wyznaczane są w odbiornikach GPS na Ziemi i każdy robi to nieco inaczej. W konsekwencji nie ma dwóch bliźniaczych odbiorników wyznaczających jednocześnie te same parametry PNT. Różnica wskazań PNT jest miarą oczekiwanej dokładności i błędu odbiornika. Dzieje się tak, ponieważ odbiornik GPS musi sporo policzyć, a jego przetwarzanie – mimo zgodności sprzętu i *firmware* – jest asynchroniczne.

Problem utrzymania zgodności PNT odbiorników rozproszonych na dużym obszarze kraju czy kontynentu rozwiązuje się za pomocą sztucznej inteligencji (SI), która używając metod statystycznych potrafi zminimalizować niepewność pomiaru (szum) *jitter*. Wbudowana w firmware odbiorników SI dla DSP pozwala rozpoznawać zakłócenia, takie jak odbicia, opóźnienia, zagłuszanie i fałszowanie sygnałów GNSS. W celu zwiększenia cyberodporności na ataki DoS, odbiorniki GPS mogą korzystać z naziemnych poprawek A-GPS (GSM), RTK drogą radiową, a te wyposażone w łączność mobilną 4G/5G mogą otrzymywać wsparcie synchronizacji z wykorzystaniem NTP i PTP IEEE1588. Coraz więcej odbiorników korzysta z telemetrii satelitów LEO i geostacjonarnych stellitów SBAS (EGNOS).

Rozumiejąc niepewność GPS, Amerykanie jako pierwsi zalecili w 2020 r. dywersyfikację ryzyka PNT i używanie naziemnych struktur dystrybucji czasu z NIST (dyrektywa EO13905[5]). W styczniu 2023 r., Komisja Europejska opublikowała zaktualizowaną dyrektywę NIS2, która w ślad za doktryną USA zaleca krajom członkowskim UE tworzenie alternatywnych naziemnych systemów A-PNT (*ang. Assured Piositiong Navigation and Timing*).

## Czas pod kontrolą

Uznanie synchronizacji za obszar cyberbezpieczeństwa wymaga aktualizacji procedur operacyjnych, zarówno na

1 https://navi.ion.org/content/68/4/673, https://radionavlab.ae.utexas.edu/images/stories/files/papers/leo_int_mon.pdf
2 https://c4ads.org/wp-content/uploads/2022/05/AboveUsOnlyStars-Report.pdf
3 https://space.skyrocket.de/doc_sdat/stp-h5.htm
4 https://radionavlab.ae.utexas.edu/images/stories/files/papers/leo_int_mon.pdf
5 https://www.govinfo.gov/app/details/DCPD-202000071

szczeblu państwowym, jak i w lokalnych środowiskach pracy. Kluczowym elementem jest edukacja, która podnosi świadomość znaczenia utrzymania stabilnej domeny czasu UTC (uniwersalnego czasu skoordynowanego) dla nowoczesnych technologii informatycznych (IT) i systemów sterowania (OT) zarówno w czasie pokoju, jak i w przypadku konfliktu.

Odbiorniki GNSS (korzystające z GPS) wyprodukowane przed 2022 r. nie są odporne na zakłócenia typu *jamming* i *spoofing*. W Polsce, podobnie jak w innych krajach, funkcjonuje bliżej nieznana duża liczba urządzeń wykorzystujących odbiorniki satelitarne, które pomimo deklaracji producenta, zamiast korzystać z systemów GPS+GALILEO, synchronizują się do rosyjskiego GLONASS i chińskiego BEIDOU.

> *Krajowi posiadacze starszych serwerów NTP, niezależnie od marki, powinni rozważyć wymianę urządzeń.*

Dobrym kandydatem w miejsce starszych urządzeń są krajowe serwery NTP/PTP firmy ELPROMA. Posiadają kodyfikację NATO i certyfikację metrologiczną Głównego Urzędu Miar RP.

Polskie serwery czasu używane w NATO.

## eCzasPL

Polska wcześniej niż USA i Wielka Brytania zauważyła konieczność wyodrębnienia czasu urzędowego i zaczęła go chronić prawnie. Polscy użytkownicy powinni wziąć pod uwagę dołączenie swoich infrastruktur IT/OT do krajowego systemu bezpiecznej synchronizacji eCzasPL[6] Głównego Urzędu Miar RP, który niezależnie od GPS dostarcza uwierzytelniony kryptograficznie polski czas urzędowy UTC(PL) za pomocą sieci Internet i dedykowanych łączy Ethernet. System został oddany do użytku na dwa tygodnie przed pierwszymi zakłóceniami sygnałów GPS nad Polską. Technologia eCzasPL została opracowana w latach 2015–2016 przez inżynierów polskiej firmy ELPROMA[7], którzy uczestniczyli w europejskim projekcie Horizon 2020 o nazwie DEMETRA[8]. Obecnie technologia eCzasPL jest kompletnym rozwiązaniem oferowanym na eksport przez polskie konsorcjum firm ELPROMA i PIK Time[9]. Rozwiązanie to obejmuje również projekt i wyposażenie laboratorium w zegary atomowe.

Polski serwer czasu firmy ELPROMA model NTS-5000 z anty-jammingiem i anty-spoofingiem GPS (LEVEL-1). Takich serwerów dołączonych bezpośrednio do zegarów atomowych używa projekt eCzasPL

Możliwe jest włączenie odizolowanych od Internetu systemów korporacyjnych ICT i sieci infrastrukturalnych OT do eCzasPL. Takie połączenie jest realizowane na poziomie trzecim oznaczonym etykietą LEVEL-3 za pomocą urządzenia GNSS-firewall. Urządzenie to symuluje sygnał satelitarny GNSS na podstawie wzorca UTC(PL) czasu urzędowego określonego w ustawie o czasie urzędowym.

Symulator LEVEL-3 pobiera czasu urzędowy z systemu eCzasPL i konwertuje na sygnał antenowy serwerów ELPROMA NTS-5000, NTS-4000, NTS-3000. W ten sposób tworzy się źródło czasu UTC niezależne od jammingu/spoofingu GPS nad Polską.

Tak długo, jak rozproszone systemy informatyczne mają dostęp do Internetu, zasoby te mogą korzystać z systemu eCzasPL. Należy się jednak liczyć z zagrożeniem, że zcentralizowana struktura informatyczna GUM RP może ulec ograniczeniom funkcjonalności wywołanym hybrydowym atakiem DoS/DDoS na krajową metrologię. Dlatego tak ważne jest posiadanie systemu monitorowania sygnałów GNSS, który wysyłając alarmy, pozwoli na czas uruchomić awaryj-

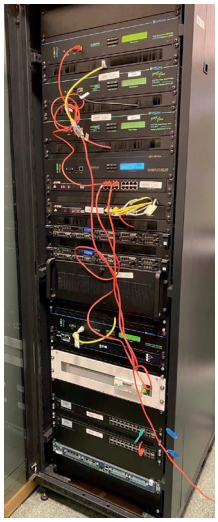
6 https://www.gum.gov.pl/pl/projekty-eu/e-czaspl/3632,e-CzasPL.html.

7 www.elpromaelectronics.com

8 https://www.ion.org/publications/abstract.cfm?articleID=14982

9 https://www.piktime.com

ne procedury postępowania, a w szczególności – w razie konfliktu zbrojnego – mobilne wzorce UTC, tzw. defibrylatory UTC (urządzenia klasy TIME LOADER).



Polski „defibrylator UTC" firmy ELPROMA.

Węzeł autonomicznej synchronizacji UTC w Polskiej Agencji Żeglugi Powietrznej.

Wyposazony jest w zegary atomowe podtrzymujące czas przy braku GPS.

## Czas na wojnie

Wojsko musi zapewnić zgodną domenę czasu dla systemów i składowych OT nie tylko podczas pokoju, ale również podczas konfliktu zbrojnego. Z pomocą przychodzą przenośne systemy podtrzymania czasu UTC z wbudowanym akumulatorem i z wysokiej klasy oscylatorami kwarcowymi lub rubidowymi o dobrej stabilności długoterminowej. Urządzenia takie są już na wyposażeniu taktycznego działania armii w Izraelu. Wspierają pracę systemów autonomicznych UAV, radarów/EO, systemów obrony przeciwrakietowej i dowolnych innych systemów naziemnych, morskich i powietrzno-desantowych, wymagających zewnętrznej synchronizacji ToD/1PPS w czasie rzeczywistym w zabronionych środowiskach dostępności GPS (GNSS).

Innym alternatywnym źródłem UTC dla wojska może być sieć publicznych serwerów NTP dostępnych w Internecie, NTPPOOL[10]. Niestety, korzystanie z tych serwerów wiąże się z ryzykiem, ponieważ nie zawsze wiadomo, kto nimi zarządza i skąd pochodzi źródło czasu UTC. Od czasu wybuchu wojny na Ukrainie liczba publicznych serwerów NTPPOOL w Rosji[11] wzrosła o około 20 proc. – do 200 szt. Istnieje techniczna możliwość utrzymywania przez Rosję serwerów NTP również poza granicami kraju[12].

Dla porównania, od czasu wybuchu wojny w Ukrainie w 2022 r. aspirująca do wejścia do NATO Szwecja zwiększyła liczbę swoich publicznych serwerów NTP aż dwukrotnie. Dwa lata wcześniej wzrost odnotowała Finlandia. Niemcy zwiększyły liczbę publicznych serwerów NTP skokowo w roku aneksji Krymu (2014). Obecnie łączna liczba publicznych serwerów w Niemczech wynosi aż 900.

Przy budowie wewnętrznego korporacyjnego systemu zarządzania czasem trzeba mieć na uwadze, że bezpieczna synchronizacja nie może się bazować na pojedynczym serwerze NTP/PTP. Jako niezbędne minimum uważa się użycie w pojedynczym węźle co najmniej kilku serwerów czasu skonfigurowanych do pracy w układzie redundancji i zapewniających również agregację (bezwładność pracy bez GPS) swoich zegarów. **Firma ELPROMA wspiera w tym zakresie krajowy przemysł i biznes. Prowadzi doradztwo i nieodpłatne konsultacje, jak włączyć wewnętrzne sieci informatyczne do państwowego systemu wiarygodnej synchronizacji czasem urzędowym UTC(PL) – eCzasPL Głównego Urzędu Miar RP.** Używanie eCzasPL jest bezpłatne dla użytkowników krajowych i podmiotów zarejestrowanych w Polsce.



10 https://www.ntppool.org/en/

11 https://www.ntppool.org/zone/ru

12 https://gist.github.com/mutin-sa/eea1c396b1e610a2da1e5550d94b0453

# Czy na pewno jesteśmy bezpieczni?

**Katarzyna Żółkiewska-Malicka**

dyrektor ds. bezpieczeństwa informacji w ZETO sp. z o.o. w Lublinie. Audytor wewnętrzny, specjalista ds. bezpieczeństwa informacji z 20-letnim stażem pracy w zakresie przeprowadzania audytów cyberbezpieczeństwa, bezpieczeństwa informacji, ochrony danych osobowych oraz audytów śledczych. Auditor Wiodący systemu zarządzania bezpieczeństwem informacji wg ISO/IEC 27001. Członek Stowarzyszenia Praktyków Ochrony Danych Osobowych oraz Stowarzyszenia Inspektorów Ochrony Danych SABI. Ekspert w Cyber Women Community. Lider ISSA Polska Lublin. Członek CSO Council Społeczności Dyrektorów Bezpieczeństwa Informacji.

**„Cyberbezpieczny Samorząd" to po „Cyfrowej Gminie" kolejny program, którego celem jest wzmocnienie krajowego systemu cyberbezpieczeństwa. Wnioski można składać do połowy grudnia 2024 r.**

Projekt realizowany jest w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 „Cyberbezpieczny Samorząd" na podstawie ustawy z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021–2027. Początkowo nabór wniosków trwać miał od 19.07.2023 r. do 30.09.2023 r., jednak z uwagi na to, że termin obejmował okres wakacyjny, wiele podmiotów publicznych obawiało się o jego dotrzymanie. Ostatecznie, po kilku jeszcze zmianach, termin składania wniosków został przesunięty na 14.12.2024 r.

**Koszty niekwalifikowane w projekcie to wszelkie wydatki na zakup, dostawę lub usługi, które nie służą bezpośrednio wsparciu cyberbezpieczeństwa w JST. W szczególności są to:**

**a. komputery stacjonarne i przenośne;**

**b. urządzenia mobilne – smartfony lub tablety;**

**c. akcesoria i urządzenia peryferyjne, np. drukarki, skanery, urządzenia wielofunkcyjne, kserokopiarki, klawiatury, myszy;**

**d. materiały eksploatacyjne;**

**e. oprogramowanie biurowe, z wyłączeniem systemów operacyjnych niezbędnych do instalacji i utrzymania systemów bezpieczeństwa;**

**f. szkolenia informatyczne niezwiązane z cyberbezpieczeństwem, np. szkolenia z obsługi oprogramowania biurowego;**

**g. usługi dostępu do internetu, abonamenty telefoniczne.**

Zakup przynajmniej części z tych urządzeń był możliwy w ramach „Cyfrowej Gminy". Osoby odpowiadające za IT w gminach podnosiły kwestię, że gdyby wiedziały o kolejnym projekcie skierowanym na SZBI (System Zarządzania Bezpieczeństwem Informacji), oprogramowanie np. typu EDR (*Endpoint Detection and Response*), XDR (*Extended Detection and Response*) czy oprogramowanie do wykonywania kopii zapasowych, to środki z „Cyfrowej Gminy" zostałyby przeznaczone na zakup sprzętu. Dałoby to możliwość dosprzętowienia urzędów i następnie zakupu dedykowanego oprogramowania.

## Teoria sobie, praktyka …

Regulamin projektu kładzie duży nacisk na podnoszenie świadomości pracowników w zakresie cyberbezpieczeństwa. I jak to zwykle bywa, w teorii wszystko prezentuje się bardzo dobrze, a w praktyce wygląda zupełnie inaczej.

Ankieta dojrzałości cyberbezpieczeństwa już na starcie nastręczyła wielu problemów, gdyż niezbędne było określenie i opisanie stanu obecnego, stanu planowanego oraz opis planowanego zakresu zmian. Do tego doszła presja czasu z uwagi na okres wakacyjny, brak wcześniejszej zapowiedzi projektu oraz kilkukrotną zmianę terminu składania wniosków.

> *Informatyk w urzędzie musiał określić, co ma, co chce zakupić oraz jak wydatkowanie środków wpłynie na podniesienie poziomu cyberbezpieczeństwa w gminach.*

Nie wszystkie osoby odpowiadające w gminach za kwestie IT mają stosowną wiedzę w zakresie *cybersecurity* oraz rozwiązań dostępnych na rynku. Zainteresowani wskazują również, że z uwagi na nadal istniejące niedobory sprzętowe czy niewspierane systemy operacyjne, sam zakup oprogramowania nie zmieni istotnie sytuacji. Łatwo więc zidentyfikować pierwszą przeszkodę w osiągnięciu celu projektu – to niewystarczająca wiedza osób odpowiadających za kwestię IT w gminach w obszarze *security* oraz braki sprzętowe.

Podnoszenie poziomu świadomości pracowników jest kosztem kwalifikowanym i w ramach projektu można przeprowadzać szkolenia zarówno dla pracowników, jak i osób z IT. Najsłabszym ogniwem jest człowiek, na co również wskazują raporty powłamaniowe, bo atak najczęściej zaczyna się od pracownika. Wydawać by się więc mogło, że podmioty publiczne chętnie będą finansować szkolenia w ramach projektu.

Dla mnie ogromnym zaskoczeniem był opór osób z IT przed organizowaniem szkoleń dla pracowników. Najczęściej padał argument, że nie ma po co robić szkolenia, bo i tak nie będą wiedzieli, o co chodzi. Kilkakrotnie słyszałam szokujące dla mnie stwierdzenie, że szkolenie jest niepotrzebne, bo „my jesteśmy bezpieczni". W dzisiejszych czasach, gdy nie ma dnia bez informacji o kolejnej firmie, podmiocie publicznym czy koncernie, które padły ofiarą cyberprzestępców, takie stwierdzenie jest ryzykowne.

Panaceum jest banalnie wręcz proste. Wystarczy, żeby użytkownicy nie mieli możliwości instalowania oprogramowania na swoich stacjach roboczych, bo nie zainstalują przecież wtedy oprogramowania „złośliwego". Jeżeli takich argumentów używa osoba odpowiadająca za kwestie cyberbezpieczeństwa w dużym – jak na województwo lubelskie – urzędzie miasta, to jak podnosić ten poziom w podmiotach publicznych?

## Praca u podstaw

Powinno się zacząć od podnoszenia wiedzy i kompetencji osób odpowiadających za kwestię IT, a dopiero później rozpoczynać realizację programów typu „Cyberbezpieczny Samorząd". Oczywiście, nie można wszystkich informatyków wrzucać do jednego worka, ale w mojej ocenie niewystarczający poziom wiedzy osób z IT ma negatywny wpływ na sposób realizacji projektu.

> *Może właściwym rozwiązaniem byłoby powołanie do życia podmiotu na wzór CUW (Centrum Usług Wspólnych), który z poziomu całego kraju badałby rzeczywisty stan bezpieczeństwa administracji publicznej, wypracowywałby minimalne standardy, jakie powinien w zakresie cyberbezpieczeństwa spełniać podmiot publiczny i byłby wsparciem przy realizacji projektów typu „Cyberbezpieczny Samorząd".*

Bardzo dużym problemem dla podmiotów publicznych jest finansowanie utrzymania – z własnych środków – oprogramowania np. typu NDR (*Network Detection and Response*) po zakończeniu projektu. Okres realizacji projektu grantowego wynosi maksymalnie 24 miesiące od dnia wejścia w życie Umowy o powierzenie Grantu, jednak nie później niż do 30.06.2026 r.

Oprogramowanie typu NDR zapewnia zespołom ds. bezpieczeństwa (w podmiotach publicznych będą to niekiedy pojedyncze osoby) wykrywanie i prognozowanie anomalii w ruchu sieciowym w czasie rzeczywistym. Pozwala na de-

tekcję zagrożeń, obsługę zdarzeń, monitorowanie sieci itp. Używanie tego typu oprogramowania to jednak luksus, bo oznacza koszt ok. 10 tys. zł. miesięcznie (to uśredniona wartość oferty przygotowanej dla średniej wielkości podmiotu zatrudniającego do 40 pracowników; są też oferty zdecydowanie wyższe). W trakcie trwania projektu urząd płaci za oprogramowanie z własnych środków. Pytanie, czy po 30.06.2026 r. jakiekolwiek urząd będzie stać na ponoszenie takich kosztów.

Są dwie strategie radzenia sobie z tym problemem. Jedna grupa podmiotów nie wpisywała we wnioskach tego typu rozwiązań, skupiając się na SZBI oraz szkoleniach. W zakresie sprzętowym decydowała się na zakup macierzy oraz dysków do macierzy, czyli elementów do wykonywania kopii zapasowych.

Druga grupa zdecydowała się na wpisanie we wniosku oprogramowania pozwalającego na wykrycie działań niepożądanych i ataków z pełną świadomością, że po zakończeniu trwałości projektu nie będą go utrzymywać z uwagi na koszty.

Problem w tym, że różnie wyglądają oceny wniosków pod kątem kwalifikowalności kosztów. Raz wyjmowane dyski do macierzy (do wykonania kopii bezpieczeństwa offline, deponowane w innej lokalizacji) są kwalifikowane jako koszt kwalifikowany, a raz nie. Opisywany przypadek dotyczy dwóch urzędów obsługiwanych przez tego samego informatyka, dlatego też opisy w obu wnioskach były identyczne.

W numerze 3/2023 „Domeny" podnosiłam kwestię nieprawidłowości czy wręcz anomalii w zakresie wykonywania audytów w ramach programu „Cyfrowa Gmina". Obawiam się, że i w tym projekcie będzie podobnie, bo wymagania co do podmiotów oraz osób wykonujących audyt się nie zmieniły.

Na pewno przeznaczanie środków na podnoszenie poziomu cyberbezpieczeństwa w podmiotach publicznych jest kierunkiem właściwym. Cieniem na realizacji tego projektu kładą się wskazane przeze mnie problemy: niewystarczająca wiedza w zakresie *cybersecurity* osób odpowiadających za IT w podmiotach publicznych, brak świadomości na temat zagrożeń, konieczność szkolenia pracowników oraz kwestie finansowe po zakończeniu trwania projektu. W celu uniknięcia takich problemów w przyszłości niezbędne jest przeprowadzanie przy takich projektach konsultacji z ekspertami, praktykami. Dobrym krokiem, który jako środowisko odbieramy pozytywnie, jest grudniowe zaproszenie nowego ministra cyfryzacji do udziału w branżowym spotkaniu. Trzymamy za słowo Pana Ministra, że będzie zasięgał opinii naszego środowiska przy planowaniu kolejnych projektów mających na celu zwiększenie cyfryzacji jednostek samorządu terytorialnego w obsarze zwiększenia poziomu cyberbezpieczeństwa.

# RODO do poprawki

**Niedługo minie 6 lat stosowania RODO, a kilka tygodni temu wybrano nowego Prezesa Urzędu Ochrony Danych Osobowych. Jest to zatem znakomity moment, by wrócić do jednego z kluczowych problemów RODO wciąż wymagających działania, czyli do wyjaśnienia błędów w tłumaczeniu Rozporządzenia, o czym wspomniałam w numerze 1/2023 Domeny.**

**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.

Problem jest znany od dnia opublikowania RODO. Wiele osób, mając wątpliwości, wolało w swojej pracy bazować na wersji oryginalnej, czyli angielskiej. Ambitni zestawiali dla porównania kilka wersji językowych.

Znając biegle języki angielski i francuski, też tak zrobiłam, dorzucając wersję hiszpańską. Najbardziej zaintrygowało mnie przetłumaczenie *documented instructions* na „udokumentowane polecenie" w artykule 28 Podmiot przetwarzający. Przypomnę zapis z ust. 3: „... podmiot przetwarzający: a) przetwarza dane osobowe **wyłącznie na udokumentowane polecenie administratora ...**" (w oryginale the processor: (a) processes the personal data **only on documented instructions from the controller**).

Pracując wiele lat w informatyce, zrozumiałam jednoznacznie, że wszelkie wymagania nazwane instrukcjami, dotyczące przetwarzania danych osobowych, administrator ma przekazywać procesorowi / podmiotowi przetwarzającemu tylko i wyłącznie na piśmie. Wymagania mogą dotyczyć chociażby częstotliwości wykonywania kopii zapasowych i miejsc ich przechowywania. Zajrzałam do *Słownika języka polskiego PWN* (https://sjp.pwn.pl) i dowiedziałam się, że instrukcja to „zbiór przepisów ustalających sposób postępowania w jakiejś dziedzinie"; także „dokładne pouczenie, wskazówka", zaś polecenie to „wypowiedź nakazująca komuś wykonanie jakiejś czynności". Zwracam uwagę na słowo „wypowiedź".

## Europa precyzuje

Dla potwierdzenia mojej interpretacji sięgnęłam do wytycznych organów nadzorczych państw UE. Znakomite wyjaśnienie znalazłam w poradniku „Smernice Informacijskega pooblaščenca o (pogodbeni) obdelavi osebnih podatkov" (https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_o_pogodbeni_obdelavi_web.pdf), wydanym przez słoweński organ Informacijski Pooblaščenec. Czytamy „ […] instrukcje mogą obejmować dopuszczalne i niedopuszczalne przetwarzanie danych osobowych, bardziej szczegółowe procedury, metody ochrony danych itp.". Zapoznałam się także z Wytycznymi 07/2020 dotyczącymi pojęć administratora i podmiotu przetwarzającego zawartych w RODO, wydanymi przez Europejską Radę Ochrony Danych (https://edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_pl.pdf). Stosowny zapis dotyczący art. 28 ust. 3 lit. a) brzmi: „116. Konieczność określenia tego obowiązku wynika z faktu, że podmiot przetwarzający przetwarza dane w imieniu administratora. Administratorzy muszą przekazywać podmiotom przetwarzającym instrukcje dotyczące każdej czynności przetwarzania. Takie instrukcje mogą obejmować dopuszczalne i niedopuszczalne sposoby przetwarzania danych osobowych, bardziej szczegółowe procedury, sposoby zabezpieczania danych itd. Podmiot przetwarzający nie może wykraczać poza instrukcje przekazane przez administratora. Podmiot przetwarzający może jednak sugerować elementy, które – jeśli zostaną zaakceptowane przez administratora – staną się częścią wydanych instrukcji".

## Problem zbagatelizowany

W maju 2018 r., po opublikowaniu corrigendum do RODO, zgłosiłam kolejne niezbędne poprawki tłumaczenia Rozporządzenia do wskazanego Wydziału Jakości Regulacji Służby Prawnej Sekretariatu Generalnego Rady UE. Zaproponowałam m.in. zmianę na: a) przetwarza dane osobowe wyłącznie według udokumentowanych instrukcji administratora. Zwróciłam uwagę, że słowa „instrukcje" użyto w Rozporządzeniu (We) Nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych.

> *W 2021 r., czyli po trzech latach analizy, otrzymałam następującą odpowiedź: please be informed that after examination of your request and* ***consultations with competent Polish authorities*** *we came to a conclusion that the Polish version of the Regulation (EU) 2016/679 needs to be corrected as far as Article 82(2) is concerned and that other points raised in your message didn't warrant a corrigendum.*

## Problem ukarany

Prawnicy przyjęli literalną interpretację art. 28 ust 3. lit. a) bez żadnego dodatkowego wyjaśnienia i powtarzają ją jak mantrę. Najlepszym przykładem ich podejścia jest kara administracyjna w wysokości 100 tys. zł nałożona w 2021 r. przez Prezesa UODO (https://www.uodo.gov.pl/decyzje/DKN.5130.2024.2020) na Krajową Szkołę Sądownictwa i Prokuratury (KSSIP).

Dla przypomnienia: incydent polegał na uzyskaniu nieupoważnionego dostępu do kopii bazy danych witryny szkoleniowej KSSIP powstałej w trakcie testowej migracji do nowej platformy szkoleniowej. Naruszenie dotyczyło ponad 50 tys. osób, użytkowników podlegających szkoleniu ustawicznemu, w tym aplikantów sędziowskich i prokuratorskich, sędziów, prokuratorów, asesorów, referendarzy, asystentów oraz pracowników sądów, a także osób prowadzących zajęcia w KSSiP, których dane osobowe zgromadzono na platformie szkoleniowej Szkoły. Kara została nałożona m.in. za powierzenie przetwarzania danych osobowych **bez zawarcia w umowie zobowiązania podmiotu przetwarzającego do przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora**.

Jak wynika z uzasadnienia, umowa główna wprawdzie zawierała zapis *„[…] zgłoszenia usterek związanych z usługami hostingowymi, w tym ich niedostępność, dokonywane będą pisemnie, faksem lub pocztą elektroniczną"*, jednak w ocenie Prezesa UODO wskazane postanowienie umowy było niewystarczające. Umowa powierzenia zawarta z podmiotem przetwarzającym powinna zawierać przynajmniej ogólne sformułowanie zobowiązujące podmiot przetwarzający do działania wyłącznie na udokumentowane polecenie administratora. Pracownicy KSSiP nie mieli pełnej świadomości,

jak kształtują się prawa i obowiązki pomiędzy administratorem a podmiotem przetwarzającym, wynikające z umowy, zaś administrator kilkukrotnie oczekiwał wykonywania zadań wykraczających poza jej zakres. Jedynie na udokumentowane polecenie administratora podmiot przetwarzający może dokonywać ingerencji w zakresie wynikającym z charakteru świadczonych usług i zawartej umowy.

Sprawa była bardzo głośna. Media rozpisywały się o niej, a w jej wyjaśnienie zaangażowano wiele ważnych instytucji. Zastanawia, dlaczego szkoła edukująca prawników sama nie znała prawa. A może go nie rozumiała, bo zabrakło dodatkowych właściwych praktycznych wytycznych i objaśnień zapisów RODO, także dotyczących pojęcia „udokumentowane polecenie".

## Problem powielany

Skoro konsekwencje braku formułki wymaganej przez Prezesa UODO w umowie powierzenia mogą być bolesne dla administratora, postanowiłam sprawdzić, jakie zapisy zawierają przyjęte i proponowane kodeksy postępowania, które mają pomagać we właściwym stosowaniu RODO.

## Problem wyjaśniony?

Pod koniec 2023 r. Prezes Urzędu Ochrony Danych Osobowych nałożył 100 tys. zł kary na Ministra Zdrowia za ujawnienie w jednym z serwisów społecznościowych danych o stanie zdrowia lekarza pozyskanych z e-recepty wystawionej pro auctore. Sprawa była wyjątkowo głośna.

Wiele ciekawych informacji o naruszeniu i jego skutkach zawarto w uzasadnieniu nałożonej kary (https://www.uodo.gov.pl/decyzje/DKN.5131.32.2023).

Okazuje się, że po incydencie Minister zlecił przeprowadzenie audytu w Centrum e-Zdrowia, które odpowiada za organizację i prawidłowe funkcjonowanie Elektronicznej Platformy Gromadzenia, Analizy i Udostępniania zasobów cyfrowych o Zdarzeniach Medycznych (P1) obejmującej usługę e-recepta. W raporcie z audytu znalazły się m.in. następujące cytowane ustalenia:

- polityka bezpieczeństwa danych osobowych obowiązująca w instytucji odwołuje się do nieaktualnych przepisów i stosowane jest stare podejście do ochrony danych osobowych;

**W Kodeksie dla małych placówek medycznych, przyjętym w grudniu 2022 r., jedynie powielono treść art. 28.**

**W Kodeksie dla szpitali, przyjętym w grudniu 2023 r., w ogóle nie pojawia się „udokumentowane polecenie". Z kolei w projektach kodeksów złożonych do zatwierdzenia (https://uodo.gov.pl/pl/426/1109):**

- **dla doradców podatkowych „udokumentowane polecenie" pojawia się dwa razy: w punkcie 6.19.1. jako cytat art. 28 ust. 3 lit. a) oraz we wzorze umowy powierzenia przetwarzania jako zapis: „Podmiot przetwarzający będzie przetwarzał dane osobowe wyłącznie na udokumentowane polecenie Podmiotu powierzającego. Udokumentowane polecenie może stanowić w szczególności niniejsza Umowa. Inne polecenia będą mogły być kierowane do Podmiotu przetwarzającego wyłącznie w formie …….";**
- **dla firm badania opinii i rynku formułki nie ma ani w projekcie kodeksu, ani w załączniku nr 5 (umowa powierzenia przetwarzania danych osobowych);**
- **dla centrów handlowych – nie ma żadnego zapisu (w wersji z dnia 29.06.2020 r.)**
- **dla biobanków – nie ma żadnego zapisu;**
- **dla branży hotelarskiej – zawarto tylko zapis „Powierzenie przetwarzania danych osobowych to sytuacja, w której inny podmiot przetwarza dane osobowe w imieniu administratora wypełniając jego polecenia. Podmiot przetwarzający przetwarza dane osobowe w określonym przez administratora celu".**

Przypomnę, że według Cambridge Dictionary: *code of conduct to set of rules that members of an organisation or people with a particular job or position* ***must follow***. Zatem kodeksy postępowania znakomicie nadają się do wyjaśnienia, co w praktyce oznacza „udokumentowane polecenie" administratora dla podmiotu przetwarzającego. Na razie nie precyzują.

- wymagana jest zmiana Porozumienia przez Centrum wraz z Ministerstwem Zdrowia w części dotyczącej **wydawania poleceń** przez Ministra Zdrowia w taki sposób, aby ewentualne polecenia wydawane były w trybie oficjalnym i zawierały sformułowanie „polecenie" (zamiast za pomocą poczty elektronicznej) oraz wprowadzenie zakazu stosowania innych kanałów komunikacji nieokreślonych w Porozumieniu.

Czy w sformułowaniu „wydawanie poleceń" chodzi o udokumentowane polecenie z art. 28 ust. 3 lit. a)? Tylko dostęp do samego raportu z audytu by to wyjaśnił.

## Problem upoważniony

Ciąg dalszy zamieszania jest związany z artykułem 29 RODO, który dla jasności przytoczę w wersji oryginalnej: *The processor and any person acting under the **authority** of the controller or of the processor, who has access to personal data, shall not process those data **except on instructions from the controller**, unless required to do so by Union or Member State law* i w wersji polskiej: „Podmiot przetwarzający oraz każda osoba działająca z **upoważnienia** administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je **wyłącznie na polecenie administratora**, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego".

> *Otóż według prawników specjalizujących się w RODO owo upoważnienie i owo polecenie są tożsame.*

W poradniku wydanym w 2021 r. autor napisał m.in. „uprawnienie do przetwarzania danych tworzone jest dwuetapowo, przez upoważnienie i polecenie" oraz „przez nieuprawniony dostęp do danych przechowywanych należy rozumieć dostęp bez upoważnienia i bez polecenia administratora lub za upoważnieniem, ale bez polecenia administratora, lub bez upoważnienia podmiotu przetwarzającego i bez polecenia administratora, lub bez upoważnienia administratora, lub bez polecenia podmiotu przetwarzającego". Z kolei w innym poradniku wydanym pod koniec 2023 r. jego kolega po fachu stwierdził, że „*upoważnienie do przetwarzania danych osobowych to obecnie nie wymóg czysto biurokratyczny, lecz element systemu zabezpieczenia danych osobowych, którego istotę można sprowadzić do jednego: każdy, kto przetwarza dane, może to robić wyłącznie na polecenie administratora lub przetwarzającego, a wdrożenie systemu upoważnień ma to zapewnić*". Świadomie pomijam nazwiska, by nie narażać panów na różne komentarze i zalecam im refleksję. Oraz rozmowę z fachowcami od bezpieczeństwa informacji.

## Problem z rzetelnością

W czasie posiedzenia Komisji Sprawiedliwości i Praw Człowieka 23 maja 2023 r. poprzedni Prezes UODO, Jan Nowak, zwrócił uwagę na inną – jego zdaniem – wątpliwość dotyczącą tłumaczenia RODO. Jego wywód dotyczył zapisu artykułu 5 Zasady dotyczące przetwarzania danych osobowych, który brzmi:

1. *Dane osobowe muszą być: a) przetwarzane zgodnie z prawem, **rzetelnie** i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, **rzetelność** i przejrzystość")*, zaś w wersji angielskiej: 1. *Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, **fairness** and transparency')*.

Jak stwierdził Prezes: „Wydawałoby się, że ten zapis jest bardzo czytelny i wszyscy go rozumieją. Nic bardziej mylącego. Chodzi o to słowo **rzetelnie**. Dlaczego? To jest tłumaczenie RODO na język polski, ale szanowni państwo, RODO obowiązuje w 27 państwach europejskich, które mają różne języki i w związku z tym musiało być przetłumaczone na te języki. Tak się składa, że nasze tłumaczenie słowa **rzetelnie** jest absolutnie niewłaściwe, ale jest i u nas funkcjonuje. Co nie znaczy, że sądy mają sądzić tak, jak wskazuje tłumaczenie. W całej Europie, w każdym kraju europejskim należy sądzić i interpretować RODO identycznie. Tu nie ma odstępstw. Posłużę się przykładem niemieckim. To jest **rzetelny** wzór. Gdyby u Niemców było rzetelnie, to by było: *ehrlich*. Niemcy mają takie słowo, odpowiednik polskiego sformułowania rzetelnie. Ale w tłumaczeniu niemieckim jest: *nach treu und glauben*, co znaczy: w dobrej wierze". I dodał: „... po angielsku będziemy mieli słowo: ***fairly***, czyli bardziej idzie w kierunku – uczciwie, po francusku: ***loyal***. My mamy „**rzetelnie**". Jak coś się uda popsuć, to chociaż tłumaczenie".

Nie znam języka niemieckiego, znam angielski. Nie rozumiejąc, na czym polega „popsucie" w tym przypadku, dla pewności sięgnęłam do *Wielkiego Słownika Angielsko-Polskiego*. Według profesora Jana Stanisławskiego słowo „fairly" jako przysłówek oznacza:

1. sprawiedliwie; słusznie; bezstronnie
2. uczciwie; rzetelnie

Zatem użycie słowa „rzetelnie" jest uzasadnione i bardziej właściwe niż „w dobrej wierze".

Z wypowiedzi Prezesa UODO wynika, że nigdy nie zgłosił zmiany do wspomnianego dyrektoriatu Rady Unii Europejskiej. O swoim zastrzeżeniu nigdy nie napisał w biuletynie czy newsletterze wydawanym przez Urząd dla Inspektorów Ochrony Danych (przejrzałam wszystkie numery). Natomiast przyznał publicznie, że tłumaczenie RODO zostało popsute. Cieszę się, że nie tylko ja widzę problem.

Temat polecenia czy poleceń administratora dla podmiotu przetwarzającego i jego/ich dokumentowania wraca jak bumerang. Zatem czas najwyższy na corrigendum polskiej wersji RODO oraz na jasne i konkretne polskie wytyczne wyjaśniające, co w praktyce pomysłodawcy RODO mieli na myśli i jakie jest stanowisko Prezesa UODO.

# Informatycy mają się dobrze

**Raport z Badania Społeczności IT 2024 to już szósta edycja badań firmy rekrutacyjnej Bulldogjob, daje więc pewną perspektywę rozwoju rynku pracy informatyków.**

W 2019 r. Bulldogjob zaczął na swoim portalu publikować wyniki własnych badań polskiej społeczności IT. W raporcie z 2019 r. zebrano rezultaty przeprowadzonego w sierpniu i wrześniu 2018 r. badania 1466 specjalistów IT, którzy udzielili pełnych odpowiedzi (spośród ponad 4 tysięcy osób, które odpowiedziały na pierwsze, „kontaktowe" pytanie). Od tego czasu zespół Bulldogjob co roku udostępnia raporty ze swoich badań, prowadzonych w latach 2020–2024 na próbach od ponad 4 tys. do ponad 7 tys. ankiet.

Raport z 2020 r. podsumował badanie przeprowadzone na przełomie roku 2019 i 2020, od edycji 2021 badania prowadzone są w pierwszych miesiącach danego roku – np. badanie dla edycji 2024 przeprowadzono między 5 stycznia a 4 lutego bieżącego roku. Od 2020 r. publikowany jest raport ogólny prezentujący wyniki badania demografii respondentów, ich wynagrodzeń, charakteru zatrudnienia, wykształcenia, gotowości do ewentualnej zmiany miejsca pracy oraz raporty szczegółowe z badania poszczególnych stanowisk/ról zawodowych specjalistów (od 6 do 8 raportów szczegółowych, w zależności od przyjętego zestawu stanowisk/ról – w każdym badaniu występują kategorie programista oraz architekt IT). Badane są także osoby dopiero przygotowujące się do pracy w branży.

W pytaniach ankietowych w poszczególnych latach występują różnice – pojawiają się pytania odnoszące się do sytuacji, np. pracy zdalnej w czasie pandemii i po niej – co jednak powoduje nieciągłości w niektórych kategoriach (np. wykształcenie czy klasyfikacja stanowisk/ról zawodowych respondentów oraz języków programowania, które znają). Z drugiej strony sam fakt pojawienia się lub znikania w zadawanych pytaniach (a w ślad za nimi – w odpowiedziach) różnych elementów czy aspektów także niesie ze sobą informację o preferencjach ankietujących, a niekoniecznie ankietowanych.

## Demografia respondentów

W grupach wiekowych największy jest udział przedziału wiekowego 25-34 lat, wynoszący od 57 do 60%, od 14 do 16% waha się udział grupy najmłodszej (18-24).

W zasadzie niezmienny jest udział kobiet, oscylujący od 13 do 18%. Najwyższy jest udział kobiet wśród projektantów UX/UI (w 2024 r. 37,4%) oraz menedżerów (30,8%), najniższy wśród administratorów i devopsów (2,8%) i architektów IT (3,1%).

Pandemia nie zmieniła rozkładu terytorialnego zamieszkania oraz miejsc pracy: ok. 25% respondentów mieszka w Warszawie – mniej więcej tyle samo, co razem w dwóch następnych miastach: Krakowie (ok. 14%) i Wrocławiu (ok. 12%). Istotna zmiana pojawiła się dopiero w edycji 2024: udział jako miejsca zamieszkania Warszawy spadł do 21,3%, udziały Krakowa (12,9%) i Wrocławia (11,4%) pozostały niemal niezmienne, ale na drugim miejscu znalazło się ponad 16% odpowiedzi „w żadnym z wymienionych" (na liście edycji 2024 jest 12 miast i aglomeracja śląska). Natomiast niezmiennie Warszawa to siedziba ok. 30% firm.

## Wykształcenie

Najwyższy udział ukończonych studiów II stopnia (41%) występował wśród respondentów edycji 2020 – od tego czasu oscyluje wokół 38%. Od 2022 r. pytano także o studia podyplomowe. W odpowiedziach przewija się udział respondentów, którzy nie mają wykształcenia średniego, ale wynosi on poniżej 1% (w edycji 2024: 0,3%).

tów, w przypadku programistów kolejność bywa trochę inna: w edycji 2024 prowadzi JavaScript (49,4%), dalej kolejno HTML/CSS (40,8%), TypeScript (39%), SQL (37,2%). Jednak ogólnie układ pierwszej 10 jest zbliżony we wszystkich edycjach. W edycji 2022 ok. 8% ogółu respondentów odpowiedziało, że nie zna żadnej technologii programowania. Oczywiście w raportach szczegółowych dotyczących menedżerów, analityków, architektów, projektantów

*Tabela 1. Wykształcenie respondentów*

| wykształcenie | 2024 | 2023 | 2022 | 2021* | 2020 | 2019 |
|---|---|---|---|---|---|---|
| doktorat | 1,4% | 1,6% | 1,5% | 1,3%* | 0,8% | bd |
| studia podyplomowe | 6,4% | 7% | 7% | bd | bd | bd |
| II stopień | 37,4% | 39% | 38% | 59%* | 41% | 37% |
| I stopień | 28,4% | 27% | 27% | 40%* | 32% | 29% |
| w trakcie studiów | 11,4% | 9,3% | 11% | 12% | 12% | 20% |
| studiowało ale nie uzyskało dyplomu | 7,6% | 8,4% | 7,5% | bd | bd | bd |
| średnie | 7,1% | 7,1% | 6,8% | 75%** | 14% | 13% |

**) spośród tych, którzy ukończyli studia*

***) najwyższy stopień osiągnięty spośród tych, którzy nie uzyskali dyplomów*

Ponad 50% respondentów ukończyło studia informatyczne (w edycjach 2020 i 2021 pytano o studia techniczne i inne kierunki ścisłe, bez wyróżnienia informatyki).

*Tabela 2. Typ ukończonych studiów*

| typ studiów | 2024 | 2023 | 2022 | 2021* | 2020 |
|---|---|---|---|---|---|
| informatyczne | 55,6% | 54% | 55% | 87% | 88% |
| inne techniczne/ścisłe | 33,5% | 34% | 30% | | |
| nietechniczne | 19,7% | 21% | 15% | 13% | 12% |

W edycjach 2022–2024 są dane dotyczące kierunku studiów obranego przez aktualnie studiujących: w 2022 r. informatykę wybrało 85% studiujących, w 2023: 82%, w 2024: 87,5%.

## Języki programowania i nie tylko

Najpopularniejszymi znanymi i wykorzystywanymi technologiami programowania są SQL (w 2024 r. 41,7%) i JavaScript (40%), od r. 2020 zamieniające się pierwszymi dwoma miejscami w rankingu 10 najpopularniejszych. Dane te pochodzą z odpowiedzi wszystkich respondentów, w przypadku programistów kolejność bywa trochę inna: w edycji 2024 prowadzi JavaScript (49,4%), dalej kolejno HTML/CSS (40,8%), TypeScript (39%), SQL (37,2%). Jednak ogólnie układ pierwszej 10 jest zbliżony we wszystkich edycjach. W edycji 2022 ok. 8% ogółu respondentów odpowiedziało, że nie zna żadnej technologii programowania. Oczywiście w raportach szczegółowych dotyczących menedżerów, analityków, architektów, projektantów UX/UI pytano o narzędzie, a nie o języki programowania, zaś w programistów – także o inne języki czy środowiska używane obok głównego. Ciekawostka: w edycji 2021 (tylko wtedy zadano to pytanie) najwięcej respondentów (20% ) umieściło JavaScript na pierwszym miejscu wśród najbardziej nielubianych języków programowania.

## Obszar pracy

Zdecydowana większość respondentów to programiści (Tabela 3.), na drugim miejscu od 2020 r. są testerzy.

*Tabela 3.* *Obszar pracy*

| Obszar | 2024 | 2023 | 2022 | 2021* | 2020 | 2019 |
|---|---|---|---|---|---|---|
| programowanie | 50,4% | 53% | 57% | 57% | 57% | 82% |
| Architekt + analityk | 6,8% | 6,7% | | 2,9% + 5,0% | 8,2% | 20% |
| testowanie/QA | 14,7% | 14% | 15% | 18% | 10% | 13% |
| Zarządzanie projektem/Product Owner | 6,1% | 6% | 6% | 6,9% | 6,6% | 10% |
| DevOps/Admin (infrastruktura) | 9,6% | 10% | 11% | 9,9% | 13% | 10% |
| Administrowanie bazami | | | | 4,6% | | 8% |
| UX/UI | 2% | 2,1% | | | 1,5% | 7% |

O znajomość języków obcych pytano w dwóch edycjach: 2019 i 2021. Praktycznie wszyscy respondenci deklarowali znajomość języka angielskiego, w edycji 2019 większość podawała, że na poziomie dobrym lub bardzo dobrym. W edycji 2021 nie było pytania o poziom znajomości języka, 70% respondentów uważało, że pomocna byłaby w pracy jeszcze lepsza znajomość. Na drugim miejscu był niemiecki (w 2019: 26%, w 2021: 16%).

## Współpraca z firmą macierzystą

Najwięcej respondentów (po ok. 20%) pracuje w firmach zatrudniających od 51 do 200 osób oraz w firmach bardzo dużych – korporacjach zatrudniających ponad 10 tys. pracowników. Ogólnie trochę ponad 50% zatrudnionych jest w firmach polskich, ponad 40% w polskich filiach firm zagranicznych, ok. 5% – dla firm zagranicznych nie mających polskiego oddziału.

O dziwo, większość repondentów pracuje na umowach o pracę – w poszczególnych edycjach badania od 51 do 61% (umowy B2B to odpowiednio od 37% do 27% , reszta to np. umowy o dzieło) – przy czym umowy o pracę są częściej wybierane przez młodszych stażem pracowników. Wysokie „oskładkowanie" umów o pracę powoduje dużą różnicę między zarobkami „na rękę" w umowach o pracę a kwotami faktur netto w umowach B2B – na najwyżej opłacanych stanowiskach kwota na fakturze jest ponad dwukrotnie wyższa niż płaca netto. Ok. połowy działających na B2B ma płatny urlop, ale kosztem przychodów niższych o ok. 4 tys. zł.

W firmach małych (do 50 pracowników) średnie płace/przychody B2B netto to odpowiednio 7,7/18,7 tys. zł, w firmach bardzo dużych (powyżej 5 tys. zatrudnionych) to 10,1/23,3 tys. zł.

> *„Rynek pracownika" widoczny jest w tempie podwyżek: w latach 2022–2024 średnia płaca netto wzrosła z ok. 7,8 tys. do 9,2 tys. zł, kwoty netto w B2B z 17,4 tys. do 22 tys. zł, przewyższając średnie wzrosty płac w gospodarce.*

Ogólnie specjaliści IT są zadowoleni ze swojej pracy (w edycji 2024 ponad 59% wskazało wysoki lub bardzo wysoki poziom zadowolenia, dla ponad 62% praca jest ich pasją) i uważają, że w firmie liczą się efekty ich pracy. Nie są jednak bezkrytyczni: w edycjach 2022 i 2023 w odpowiedzi na pytanie o największe przeszkody w efektywnej pracy w 2022 r. 38% respondentów wskazało wadliwe procedury w firmie (w 2023 r. 35%), a 29% – problemy z komunikacją wewnętrzną. W wielkich korporacjach w 2022 było to nawet odpowiednio 43% i 30%, w 2023 r. nie pytano o firmy większe niż 500 zatrudnionych.

Warto przeglądać raporty Bulldogjob. Polskie Towarzystwo Informatyczne od kilku lat sprawuje patronat honorowy nad badaniem.

*Tomasz Kulisiewicz*

# Regulacja CSAM bardziej niebezpieczna niż Pegasus

**Ostatnio dużo się mówi o niebezpieczeństwach czyhających na dzieci w internecie i zapewnieniu im odpowiedniej kontroli treści. Projektowana regulacja dotycząca CSAM (Children Sexual Abuse Material) jest jednak oprotestowywana przez część środowiska i część organów europejskich. O co chodzi?**

**Mirosław Kutyłowski**

kierownik Zakładu Kryptologii w NASK – Państwowym Instytucie Badawczym. Przez ponad 20 lat był związany z Politechniką Wrocławską, założyciel Katedry Podstaw Informatyki i badań z zakresu kryptografii na tej uczelni. Dwukrotnie członek Centralnej Komisji ds. Stopni i Tytułów, członek Komitetu Informatyki PAN. W latach 1980–2000 pracował na Uniwersytecie Wrocławskim (gdzie otrzymał wszystkie stopnie naukowe). Był stypendystą Humboldta na Uniwersytecie Technicznym w Darmstadt oraz docentem w Instytucie Heinza Nixdorfa na Uniwersytecie Paderborn. Profesor wizytujący na Uniwersytecie Xidian.

Zajmuje się głównie tematyką wrogiej kryptografii, obroną przed słabymi punktami technologii kryptograficznych oraz z rozwiązaniami implementowanymi na elektronicznych dokumentach tożsamości.

**Mirosław Kutyłowski:** Projektowane przepisy mają zapobiegać „niegodziwemu traktowaniu dzieci w celach seksualnych" i umożliwiać zwalczanie tego zjawiska. To rzecz niezwykle istotna, tym bardziej że prawdopodobnie nie zdajemy sobie sprawy z zasięgu i konsekwencji tego zjawiska. Wiele problemów wynika z postępu nowoczesnych technologii. Dla przykładu, słyszałem od specjalistów o istnieniu wyspecjalizowanych gangów, które trudnią się pozyskiwaniem zaufania dzieci i wmanewrowują je w sytuacje, w których stają się ofiarami szantażu. Czasami ofiary nie wytrzymują ciśnienia psychicznego i szukają ucieczki w samobójstwie.

Niestety, tego typu działalność może być prowadzona z kraju, gdzie nie sięgają europejskie organy ścigania a lokalne władze co najmniej nie współpracują z naszymi. Bariera językowa przestała stanowić jakąkolwiek barierę dla takiej przestępczej działalności. Technologie AI dają możliwość takiego wytrenowania danych w języku ofiary, że nie ma ona najmniejszych szans zorientować się w sytuacji. Ataki mogą być zautomatyzowane, masowe i autonomiczne i skuteczne. Co prawda, giganci technologiczni są wrażliwi na tego typu działania i starają się zablokować możliwości wytrenowania modeli w dyskutowanym tu kierunku, ale … to może okazać się jedynie ograniczeniem skali szkód.

Projektowana regulacja zmierza w kierunku automatycznej analizy treści przesyłanych pomiędzy użytkownikami w kierunku ochrony dzieci i adekwatnego reagowania, tak aby nie mogło dojść do niepożądanych zdarzeń.

**Co w tym złego? Dlaczego na przykład Europejski Inspektor Ochrony Danych Osobowych ma tak negatywne stanowisko wobec wielu zapisów projektowanej regulacji?**

Tak jak zawsze, diabeł tkwi w szczegółach. Po pierwsze, autorzy regulacji nieco optymistycznie podchodzą do możliwości technologii. Takie życzeniowe myślenie w stosunku do informatyki jest dosyć powszechne. Podobne myślenie w przypadku medycyny skutkowałoby dyrektywami czy

ustawami zobowiązującymi NFZ do opracowania skutecznego leku na nowotwory, z datą wdrożenia np. 1.01.2025 r. O ile w przypadku medycyny takich zapędów legislatorzy raczej nie mają, o tyle w branży IT i owszem.

Problem polega na tym, że z całkiem innych względów (w tym bezpieczeństwa dzieci!), komunikacja elektroniczna powinna być szyfrowana, najlepiej w trybie end-to-end, gdzie tylko odbiorca ma techniczną możliwość odzyskania zaszyfrowanej treści.

> *Postulowana regulacja zmierza więc de facto do zakazania szyfrowania w trybie end-to-end. Jej zwolennicy mówią co prawda o analizie zaszyfrowanej treści pod kątem wykrycia treści nielegalnych, ale dziś to kwestia technicznego science fiction. Science dlatego, że istnieją tzw. w pełni homomorficzne schematy szyfrowania, a fiction dlatego, że w praktyce są zupełnie nierealizowalne ze względu na koszty i nieefektywność.*

**Co złego w objęciu kontrolą komunikacji i efektywnym zakazie szyfrowania end-to-end?**

Wiele złego. Pegasus w porównaniu do projektowanej regulacji CSAM to problem marginalny. CSAM miałaby objąć nadzorem wszystkich mieszkańców UE. Co prawda agencje trudniące się zwalczaniem przestępczości wymierzonej w dzieci miałyby skanować dane tylko pod tym kątem, ale... bezpieczeństwo danych w UE nie powinno zależeć od bezwarunkowego zaufania do określonej instytucji czy grupy ludzi. Ponadto, jeśli zbudujemy tego typu system powszechnej inwigilacji, to tylko czekać, kiedy zostanie on wykorzystany do celów kryminalnych. Pokusa będzie zbyt wielka, a zysk znacznie większy niż ze zbudowania komputera kwantowego. Dodajmy, że włamanie się do systemu informatycznego zbudowanego przez instytucję publiczną w wyniku przetargu prowadzonego na podstawie prawa zamówień publicznych jest dużo łatwiejsze niż zbudowanie komputera kwantowego. I relatywnie wymaga minimalnego zaangażowania środków.

Autorzy propozycji CSAM nie biorą też pod uwagę innej kwestii. O ile cenzura bardzo skutecznie mogłaby gromadzić dane o zwykłych obywatelach, o tyle byłaby bezradna wobec obrotu nielegalnymi treściami przez środowiska przestępcze. Dane takie mogą być skutecznie ukryte jako kryptogramy udające losowy szum zawarty na przykład w danych graficznych. Przekazanie klucza do deszyfrowania również byłoby łatwe, tanie i niewykrywalne dla organów ścigania. Na ostatniej konferencji CRYPTO w Santa Barbara pokazywaliśmy, że wszelkie próby opanowania sytuacji przez cenzora są skazane na niepowodzenie. Tak więc obrotu nielegalnymi danymi w darknecie nie jesteśmy w stanie powstrzymać!

Wdrożenie projektowanej regulacji prowadziłoby do powstania – z pieniędzy podatnika – systemu całkowicie nieefektywnego w stosunku do docelowego zastosowania i gromadzącego bezcenne dla naszych wrogów dane. Na warsztatach w Brukseli prelegentka wykazywała skutki uboczne regulacji dla zdrowia psychicznego dzieci i prawdopodobne nadużycia wobec dzieci, co mnie, jako laika, też zastanowiło.

**To co mamy robić w tej sytuacji?**

Definitywnie należy zwalczać chorobę, ale nie tak, by zabiła pacjenta. Jeśli w populacji mamy do czynienia z nowotworami, to reakcją nie może być obligatoryjne usuwanie węzłów chłonnych u każdego mieszkańca UE, mimo że taką operację niekiedy onkolodzy wykonują. W medycynie nauczyliśmy się stosować procedury koncentrujące się na efektywnym leczeniu większości przypadków, przy zminimalizowanych skutkach ubocznych i w ramach realistycznych kosztów realizacji. Stosujemy te procedury, mimo że to optymalizacja w sensie globalnym, a nie w jednostkowym przypadku pacjenta. To samo musimy zrobić w przypadku problematyki związanej z CSAM.

**Co konkretnie?**

Osobiście jestem zwolennikiem kilku kierunków działania. Pierwszym jest zapewnienie powszechnej elektronicznej, ale zanonimizowanej weryfikacji wieku. Eliminuje to wiele zagrożeń – np. 14-latka korespondująca z osobą dorosłą lub automatem udającym osobę fizyczną od razu miałaby możliwość zorientowania się w rzeczywistej sytuacji. To nie jest panaceum na wszystkie sytuacje, ale na pewno na wiele z nich. Funkcjonalność taka przydałaby się też w innych sytuacjach: cyfryzacja obrotu wymaga znalezienia rozwiązania w zakresie weryfikacji zdolności do podejmowania czynności prawnych zgodnie np. z regułami kodeksu cywilnego. Są też przypadki zupełnie trywialne, takie jak weryfikacja wieku osób osoby kupującej piwo w kasie samoobsługowej. Nie jestem w stanie zrozumieć, dlaczego takiej funkcjonalności nie ma jeszcze np. w mObywatelu.

**Jakiś inny pomysł czy technika?**

Na pewno dużym problemem w świecie mediów społecznościowych (i nie tylko) jest zjawisko *Sybil attack*. Polega ono na występowaniu jednej osoby fizycznej pod wieloma pseudonimami udającymi różne osoby. W świecie niewirtualnym trudno o taki atak – bez względu na to, jak się prze-

bierzemy i ucharakteryzujemy, nie jesteśmy w stanie występować jednocześnie w kilku rolach. A świat cyfrowy to umożliwia. Czasami wymaga to pewnego wysiłku, np. kilku kart SIM, osobno dla każdej tożsamości, ale jest możliwe.

Technologie kryptograficzne mogą tu dostarczyć skutecznego rozwiązania. W skrócie chodzi o to, by za pomocą jednego klucza (np. zawartego w ulepszonym mObywatelu) móc generować odrębny pseudonim (login) dla każdego serwisu. Co więcej, tym jednym kluczem można by uwierzytelniać się wobec serwisu i nawet podpisywać dokumenty. Co istotne, za każdym razem wskazywana byłaby pseudonimowa tożsamość dla danego serwisu, a nie tożsamość rzeczywista.

**A dlaczego miałoby to chronić przed tworzeniem wielu fikcyjnych tożsamości w jednym serwisie?**

Przyczyna jest prosta – schemat pozwala na wygenerowanie dokładnie jednego pseudonimu dla danego serwisu. Gwarancja jest kryptograficzna, nie jest to na przykład jakiś licznik programowy.

Jest jeszcze jedna zaleta: pseudonimy są nielinkowalne. Tak więc dziecko szukające pomocy u psychiatry czy choćby u pedagoga szkolnego mogłoby automatycznie wygenerować sobie taką tożsamość do kontaktów bez obaw, że tożsamość ta zostanie skojarzona z tożsamością z elektronicznego dziennika w szkole. Dobrze zabezpieczony pseudonim również ułatwiłby ofierze nawiązanie kontaktu z organami ścigania, pokonując – dzięki anonimowości – barierę wstydu.

**Brzmi to zachęcająco, ale czy taka funkcjonalność nie jest zbyt droga i trudna do wprowadzenia?**

Na pewno tańsza od systemu powszechnej inwigilacji! Ale na serio, jest kilka istotnych powodów, dla których potrzebujemy takich rozwiązań. Z jednej strony chodzi o takie sprawy, jak: realne wdrożenie dyrektywy o sygnalistach, ochronę świadków w postępowaniach sądowych przy zachowaniu prawa do obrony, zeznania w sprawach trudnych dla ofiar przestępstw (w tym zwłaszcza ofiar będących dziećmi). Z drugiej strony chodzić może o uwolnienie nas od wymyślania setek loginów i haseł do różnorodnych serwisów, do których musimy się rejestrować.

To narzędzie to coś w rodzaju silnego menedżera haseł, gdzie trudno byłoby coś źle zrobić!

**A jak w tym kontekście widzi Pan oprogramowanie opensource z szyfrowaniem end-to-end, np. sieć Matrix.org?**

Każde rozwiązanie typu open source ma tę zaletę, że dużo więcej można sprawdzić. Produkty typu *black box*, gdzie nie mamy dostępu do „wnętrza produktu", są wymarzonym miejscem dla zaimplementowania wrogiej kryptografii. W takiej sytuacji żaden zewnętrzny audyt nie pokaże niezgodności ze specyfikacją (silne gwarancje mają źródło w zastosowanej silnej kryptografii!). Zaimplementowana zapadka daje jednocześnie możliwość deszyfrowania kryptogramów generowanych nawet wtedy, gdy klucze do szyfrowania są bezpiecznie wygenerowane przez użytkownika.

Oczywiście, oprogramowanie otwartoźródłowe też ma swoje wady. Jednym z nich mogą być rozproszone prawa autorskie i brak odpowiedzialności za całość produktu. Prawo do modyfikacji programu to nie tylko prawo do ulepszania oprogramowania, to też prawo i możliwość jego psucia!

**Mamy tyle znakomitych nowych technologii i produktów kryptograficznych, jak choćby blockchain, elektroniczne dokumenty tożsamości, dobrze zabezpieczone paszporty, silne szyfrowanie komunikacji. Czy możemy czuć się w sieci bezpieczniej?**

Z bezpieczeństwem w internecie jest tak, jak ze zdrowiem… „Ile cię trzeba cenić, ten tylko się dowie, kto cię stracił." Niestety, słowa Jana Kochanowskiego doskonale opisują powszechne, dosyć lekkomyślne podejście do kwestii bezpieczeństwa. O ile trudno mieć tu pretensje do „szarego internauty" (bo niby dlaczego konsument ma być specjalistą), o tyle jako społeczeństwo mamy wiele do zrobienia w skali makro.

Od zawsze uwierzytelnianie dokumentów (papierowych czy cyfrowych) bazowało na kontekście. Jeśli co miesiąc otrzymujemy rachunki za wodę, to kolejną fakturę, mającą prawidłowe dane (numer licznika i adres odbiorcy, wykazane zużycie, dane deklarowanego nadawcy), uznajemy za autentyczną i dokonujemy płatności. Podobnie reagujemy, odbierając telefon z urzędu. Dawniej prawdopodobieństwo, że przestępca włamie się do pomieszczeń biurowych i odszuka nasze dane w papierowym segregatorze, by wykorzystać je do sfabrykowania fałszywej faktury na kilkadziesiąt złotych, było znikome. Redagowanie listów wymagało dużo pracy i znajomości lokalnych realiów.

Od tamtej pory wiele się zmieniło. Przestępcy mogą wykorzystywać narzędzia sztucznej inteligencji do preparowania wiadomości, które doskonale naśladują styl językowy danej osoby, a co więcej odwołują się do właściwego kontekstu. Wystarczy, że narzędzie AI otrzyma do „trenowania" skrzynkę mailową określonej osoby, by mogło pisać w imieniu zaatakowanej osoby wiadomości. Ich adresaci nie będą w stanie zauważyć, że w istocie korespondują z automatem.

Dawniej chroniliśmy skrzynkę mailową głównie dla zachowania poufności korespondencji. Często użytkownicy robili to w sposób dosyć niedbały, tłumacząc sobie, że „przecież nie mają nic do ukrycia". Dziś każdy musi

pamiętać, że oprócz samej zawartości informacyjnej korespondencji powinniśmy chronić się przez podszyciem się pod nas przez wrogie narzędzia AI. Co więcej, chroniąc własną skrzynkę, chronimy nie tylko siebie, lecz także swoich rozmówców.

**Jak się więc chronić?**

„Szary internauta" ma niewielki wpływ na stosowane zabezpieczenia i może co najwyżej dołożyć własne niedbalstwo do ewentualnego niedbalstwa usługodawcy. Należy przynajmniej jednak wykorzystać wszystkie możliwości dawane przez wdrożony system tam, gdzie jest to uzasadnione ryzykiem.

Dobrym przykładem są usługi bankowe. Reagując na rosnącą skalę fraudów, Unia Europejska wprowadziła kilka lat temu obowiązek uwierzytelniania dwuskładnikowego do serwisów bankowych. Spowodowało to pewną irytację klientów zmuszanych do bardziej skomplikowanego systemu logowania i potwierdzania transakcji (nie mniejsza zapewne była frustracja dotychczasowych ofiar kradzieży tożsamości, dla których wymagania te są niewystarczające!). I jaka była reakcja? Równanie w dół wymagań uwierzytelniania, tak aby nie stracić klientów. Przykładem jest oferowanie dróg na skróty, np. możliwość określenia „zaufanych urządzeń" itp.

**A co z systemami szyfrowania poczty? Może warto wskazywać na takie rozwiązania?**

Warto. Każda poufna korespondencja powinna być chroniona przed dostaniem się w niepowołane ręce. Nawet gdy ufamy, że dostawca usług pocztowych nie wykorzysta dostępu do niezaszyfrowanej poczty, to co możemy wiedzieć o możliwościach adwersarza atakującego naszego dostawcę usług. Na koniec może się zdarzyć, że dostawca jest zobligowany do ujawnienia naszej korespondencji agencjom rządowym na podstawie przepisów obowiązujących w jego kraju. Szyfrując ułatwiamy więc życie naszemu dostawcy – bezpiecznie będzie mógł przekazać kryptogramy emaili, nie narażając się na kroki odwetowe ze strony Komisji Europejskiej za złamanie zasad ochrony danych osobowych. Powinniśmy wskazywać i popularyzować takie rozwiązania! Nie jest to rzecz łatwa, bo człowiek ceni sobie przede wszystkim wygodę.

**Czy edukacja użytkownika wystarczy?**

Oczywiście nie. Prędzej czy później zostaniemy zmuszeni do strategicznych decyzji i radykalnej zmiany podejścia w wielu obszarach. Nie będą one łatwe. Bezpieczeństwo to coś, czego nie widać i trudno za pomocą sukcesów w tej dziedzinie wygrywać wybory. Nie jest to zresztą tylko polska specyfika. W branży *security* panuje przekonanie, że łatwiej dziś zarobić na mniej lub bardziej bezwartościowych modnych produktach, niż na czymś, od czego zależy bezpieczeństwo nasze i naszych danych. Postęp dokonuje się głównie wtedy, gdy wymagania zostaną narzucone drogą prawną.

**Tak, ale niekoniecznie prowadzi do postępu… Czy wprowadzenie RODO w jakikolwiek sposób poprawiło naszą sytuację? Może lepiej byłoby powstrzymać się od mnożenia przepisów?**

W przypadku RODO mamy zdecydowanie do czynienia z „papierowym tygrysem", który dużo ryczy, generuje wiele kosztów, zaś w praktyce niewiele daje w zakresie ochrony danych. Z jednej strony przechodzimy przez mordęgę akceptowania *cookies* przy każdej okazji, a z drugiej – widzimy rażące praktyki łamania ochrony danych osobowych przez instytucje publiczne. Odkładając na bok problemy o charakterze w istocie kryminalnym, mamy do czynienia z błędami o charakterze strategicznym.

Każda centralizacja przetwarzania danych to w dłuższej perspektywie stworzenie problemu, dla którego nie ma dobrego rozwiązania. Każdy zbiór danych, choćby najlepiej chroniony, jest łakomym kąskiem dla naszych przeciwników czy po prostu dla świata przestępczego. Nasze możliwości i umiejętności niekoniecznie odpowiadają poziomowi i możliwościom naszych adwersarzy. Już dawno temu profesor Ross Anderson, osoba o wielkim autorytecie w branży informatycznej w Wielkiej Brytanii, wskazywał na różnicę zasobów finansowych i ludzkich między sektorem publicznym a światem przestępczym i miażdżącej przewadze tego ostatniego.

Na szczęście, w Komisji Europejskiej i w Parlamencie chyba zdano sobie sprawę z sytuacji. Regulacja eIDAS 2 idzie w kierunku rozproszenia danych związanych z identyfikacją i uwierzytelnieniem, tak aby to „podmiot danych" gromadził je i sprawował nad nimi kontrolę. W istocie jest to jedyna droga do faktycznego zapewnienia ochrony danych osobowych. Takie podejście to dla nas rewolucja, bo w Polsce informatyzacja szła w dokładnie przeciwną stronę.

Jak widać, potrzebny jest cały ekosystem narzędzi i ich kontroli. Najlepiej byłoby to zrobić razem, wspólnie w Europie, wykorzystując cały dostępny potencjał.

*Rozmawiał Adam Jurkiewicz*

PTI member: https://www.linkedin.com/in/adam-jurkiewicz-python--linux/
Sekcja Informatyki Szkolnej (PTI) – Member of Board: https://sis.pti.org.pl/profile/adam_jurkiewicz/
Python support for teachers: https://python.szkola.pl
Teacher · Linux · Python 3: https://github.com/abixadamj
Private Chat: @adam.jurkiewicz:matrix.org

# Kto głosuje, a kto liczy głosy...

**Wyborczy rok 2024 będzie rekordowy – głosować będzie ponad połowa ludności świata, w tym mieszkańcy 8 z 10 krajów o największej liczbie ludności. Listę wyborów w 76 krajach liczących razem ponad 4 miliardy mieszkańców otworzyły w styczniu Bangladesz i Tajwan, zamknie w grudniu Sudan Południowy. Na liście tej jest też Polska z kwietniowymi wyborami do samorządów i kraje członkowskie UE wybierające w czerwcu europosłów. Głosowanie i liczenie głosów odbywać się przy użyciu różnych metod i narzędzi – od tradycyjnych papierowych kart przez urządzenia elektroniczne po platformy internetowe.**

Nie ma rozwiązań idealnych: i tradycyjne głosowania przy użyciu kart, i różne rozwiązania wspierane maszynowo mają swoje zalety i wady, zaś problemy związane z nimi miewają zarówno wyborcy, jak i liczący głosy. Zakres i waga tych problemów zależy od wielu czynników – od liczby wyborców i kandydatów, od systemów parlamentarnych i reguł ordynacji wyborczych, a także od poziomu edukacji wyborców.

Pamiętamy nasze krajowe kłopoty z wyborami samorządowymi w 2014 r., kiedy zamiast niewygodnej karty-płachty zastosowano karty spięte w broszurę. Niestety sprawdziło się stare powiedzenie o tym, że dobrymi chęciami piekło jest wybrukowane. W tych wyborach było ponad 2,52 mln

**dr Tomasz Kulisiewicz**
wykładowca i analityk rynku ICT

głosów nieważnych na 14,42 mln biorących udział. Wśród głosów nieważnych powodem unieważnienia ponad 46% z nich było postawienie krzyżyka na więcej niż jednej stronie broszury. Udział takich błędów był ponad 2 razy wyższy niż np. w poprzednich wyborach w 2010 r., w których listy były na zwyczajowo stosowanej „płachcie". Według autorów analizy[1] do dużego wzrostu liczby nieważnych głosów przyczyniło się właśnie zbroszurowanie list (mylące nie tylko wyborców, ale i komisje), pogłębione nieprecyzyjnym czy wręcz mylącym wyjaśnieniem wyborcom zasad postępowania z tą broszurą. W przypadku komisji sporo było też błędów „w drugą stronę": głosy uznane zostały za prawidłowe, choć powinny być unieważnione. Kiedy bowiem niektóre komisje zliczające głosy docierały do pierwszej ze stron, na której był krzyżyk, uznawały głos za ważny i nie sprawdzały, czy przypadkiem nie było jeszcze krzyżyka na którejś z następnych stron broszury – a więc głos powinien być unieważniony.

A są przecież kraje, w których mimo niełatwej (delikatnie mówiąc) sytuacji politycznej czy złożonego składu etnicznego ludności udaje się tak zaprojektować karty wyborcze, by zminimalizować liczbę głosów nieważnych. Bardzo ważny jest sposób prezentowania kandydatów, w tym język i symbole, a także zdjęcia kandydatów na kartach. Jako przykład radzenia sobie z takimi problemami w głosowaniu tradycyjnym podawany jest Liban, w którym w wyborach w 2022 r. o 128 miejsc w parlamencie ubiegało się 1043 kandydatów należących do 11 społeczności wyznaniowych i zgrupowanych na 103 listach. Warto też zwrócić uwagę, że w wielu krajach tzw. Trzeciego Świata nadal istotny jest procent wyborców nie umiejących czytać – nie tylko w języku urzędowym, ale w jakimkolwiek.

Z przyczyn politycznych – przede wszystkim społecznej wiarygodności wyniku wyborów – istotny jest czas, jaki upływa między zamknięciem lokali wyborczych a ogłoszeniem wyników. Im czas liczenia głosów jest dłuższy, tym częściej podważany jest wynik wyborów. Słynną sentencję „nieważne kto jak głosuje, ważne kto liczy głosy" miał wypowiedzieć Józef Stalin na jednym z posiedzeń politbiura WKP(B) w latach trzydziestych XX w. Cytowana jest też wypowiedź Anastasio Somozy, dyktatora Nikaragui rządzącego w latach 1936–1956: „wy wygraliście wybory, ale ja – liczenie głosów". Po kłopotach z liczeniem głosów na Florydzie w wyborczym pojedynku między Bushem a Gorem w 2000 r. pojawiło się ironiczne sformułowanie „liczą się nie głosy ludzi wybierających, ale ludzie liczący głosy" („*It's not the people who vote that count. It's the people who count the votes*"). Niestety, w ostatnich latach wiarygodność wyników przestaje zależeć od przejrzystości czy sprawności systemu wyborczego: po wyborach prezydenckich w USA w 2020 r. i w Brazylii w 2022 r. gwałtownie wzrosła liczba zwolenników przegranych kandydatów (Donalda Trumpa w USA i Jaira Bolsonaro w Brazylii) uważających wbrew dowodom (a raczej wobec całkowitego braku dowodów na jakiekolwiek machinacje), że wybory „zostały im skradzione".

## Maszyny pomagają

Najpierw głosowano przy użyciu kul, skorup lub kamieni, ale już w starożytnym Rzymie prawo wyborcze w 139 r. p.n.e. wprowadziło „karty wyborcze" – drewniane tabliczki z obu stron pokryte woskiem, na których rylcem zaznaczano oddany głos. Zestandaryzowanych i drukowanych na koszt rządu kart wyborczych po raz pierwszy użyto w wyborach w australijskim stanie Victoria w 1856 r.[2], a potem w pozostałych stanach Australii (karty te nazywano *Australian Secret Ballot*) i w standardowej formie zaczęły się upowszechniać na świecie.

W 1869 r., sławny wynalazca Thomas A. Edison opatentował (US Patent nr 90,646) *Electric-Voice Recorder*, który miał zliczać głosy w Kongresie. Pomysł nie został zrealizowany, bo uznano, że głosy liczone byłyby za szybko (!).

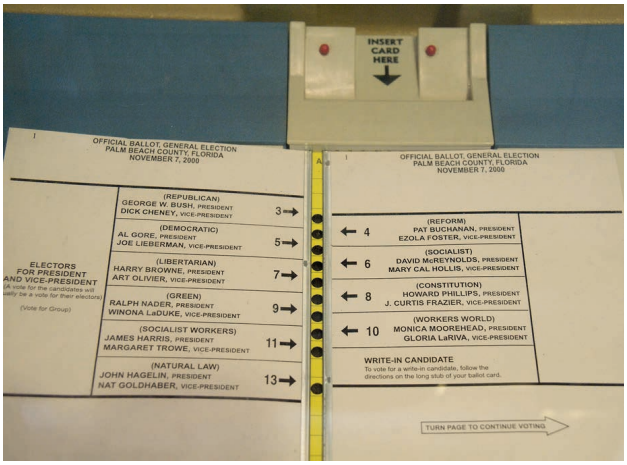
Pomysł maszynowego zbierania i zliczania głosów pojawił się już w 1848 r. (angielski wynalazca William Chamberlain, Jr.), rozwinął go w 1881 r. Amerykanin Anthony C. Beranek. Pierwszą maszynę do zastosowania w wyborach powszechnych opatentował w 1889 r. wynalazca różnych urządzeń rolniczych i sejfów Jacob H. Myers (urządzenie *The Myers Automatic Booth*), rozwinął urządzenie w 1890 r. Alfred J. Gillespie z nowojorskiej fabryki Standard Voting Machine Company of Rochester. W 1892 r. Myers namówił władze wyborcze do zastosowania maszyny w wyborach w Lockport w stanie Nowy Jork.

Ważące początkowo pół tony urządzenia nazywane maszynami dźwigniowymi (*Gear and Lever Voting Machines*) stosowane były szeroko i w zasadzie bez większych zmian konstrukcyjnych w USA przez dekady. Głosy były w nich

1 W ramach projektu Fundacji im. Stefana Batorego i Naczelnej Dyrekcji Archiwów Państwowych przebadano karty do głosowania oraz inne badane materiały z wybranych losowo 100 obwodów głosowania (a w rzeczywistości – z powodu toczących się postępowań protestowych oraz braków w dokumentacji otrzymanej z urzędów gmin i miast – z 93 obwodów) w wyborach do sejmików województw z 2014 r. Raport „Nieważne głosy, ważny problem" (Fundacja im. Stefana Batorego, Warszawa 2016 – https://www.batory.org.pl/upload/files/Programy%20operacyjne/Masz%20Glos/Niewazne%20glosy%20wazny%20problem_Internet2.pdf – dostęp: 15.02.2024)

2 https://theinventors.org/library/weekly/aa111300b.htm (dostęp: 18.02.2024)

„przechowywane" i zliczane czysto mechanicznie (ustawieniami dźwigni i kół), trochę podobnie do mechanicznych arytmometrów do liczenia[3].




Słynne karty do głosowania - Floryda 2000 r.

*Źródło: https://www.washington.edu/news/2016/03/14/documents-that-changed-the-world-hanging-chads-and-butterfly-ballots-florida-2000/*

Od lat 60. zaczęto też coraz szerzej stosować maszyny dziurkujące różne rodzaje kart. Były one używane aż do 1990 r., choć z racji stopniowego zużycia, a potem zatrzymania produkcji maszyn w latach 80. oraz ich części zamiennych (produkcję części zakończono w 1987 r.) było z nimi coraz więcej kłopotów. Maszyny z kartami perforowanymi „dobił" ostatecznie blamaż w wyborach prezydenckich w USA w 2000 r.[4], o czym (a także ogólnie o bardzo dziwnym systemie wyborczym w USA – a ściślej o ponad 50 różnych systemach w 50 stanach USA, a także oddzielnych systemach dla stołecznego Dystryktu Columbii oraz dla terytoriów zależnych, m.in. Portoryko) można przeczytać w pracy doktorskiej Pawła Jankowskiego[5].

## Elektronika z odsieczą

Problem głosowania i liczenia głosów w krajach o bardzo dużej liczbie wyborców, a także o wysokiej różnorodności językowej i/lub wysokim udziale wyborców niepiśmiennych rozwiązywany jest od niemal 50 lat przez wykorzystanie elektronicznych maszyn do głosowania. Ogólnie maszyny do głosowania elektronicznego (nazywane skrótem EVM – *Electronic Voting Machine*) mechanizują zbieranie i liczenie głosów, co stanowi dużą pomoc zwłaszcza w krajach o skomplikowanej strukturze administracyjnej i parlamentarnej oraz towarzyszącej jej zazwyczaj równie skomplikowanej ordynacji wyborczej.

**Rozróżniane są urządzenia do zbierania i liczenia głosów oddanych na nośnikach papierowych (kartach wyborczych) oraz maszyny zbierające głosy bezpośrednio w urządzeniu (DRE – *Direct -Recording Electronic*). W systemach z maszynami DRE stosowana jest najczęściej procedura „hybrydowa" – wyborca głosuje przez wybranie kandydata na ekranie dotykowym lub na specjalnej konsoli maszyny, a po zatwierdzeniu maszyna drukuje potwierdzenie, będące w zasadzie wypełnioną kartą wyborczą. Wyborca sprawdza, czy jest wydruk jest zgodny z jego preferencjami, a następnie wczytuje „paragon z głosowania" do skanera – i dopiero w tym momencie głos zostaje zaliczony. W kilkukrajach maszynom EVM obowiązkowo towarzyszą oddzielne urządzenia VVPAT (*Voter Verified Paper Audit Trail* – weryfikowany przez wyborcę ślad papierowy) drukujące „paragony" służące wyborcom do weryifkacji i wprowadzenia do systemu ich głosów.**

Specyficzna odmiana systemu hybrydowego występuje w amerykańskim stanie Waszyngton: wyborca może głosować przez Internet, ale musi następnie ściągnąć ze strony WWW potwierdzenie, wydrukować je i fizycznie dostarczyć do punktu wyborczego – dopiero wtedy oddany głos jest zaliczany.

Specjalizowane skanery optyczne do skanowania ręcznie wypełnianych kart, na których wyborcy zaznaczali swój wybór w odpowiednich miejscach (okienkach) zaczęto stosować w połowie lat 60. W 1959 r. dział Norden Division lotniczego producenta United Aircrafts[6] opracował stosowany m.in. w uczelnianych testach egzaminacyjnych Norden Electronic

3 Arytmometry mechaniczne nazywane są też arytmometrami Odhnera (od nazwiska ich wynalazcy, Willgodta Odhnera), znane były też pod żartobliwą nazwą „kręciołki"

4 Przed błędami i usterkami maszyn korzystających z kart dziurkowanych ostrzegał już w 1988 r. Roy Saltman w raporcie *Accuracy, Integrity, and Security in Computerized Vote-Tallying* (NBS Special Publication 500-158, Aug. 1988)

5 P. Jankowski, Elektroniczne głosowanie we współczesnych systemach politycznych, Kraków 2023 https://rep.up.krakow.pl/xmlui/bitstream/handle/11716/12654/PJankowski_praca_doktorska.pdf?sequence=1&isAllowed=y

6 Po kolejnych fuzjach i przekształceniach działa do dziś jako RTX, w jej skład wchodzą Collins Aerospace, Pratt&Whitney oraz Raytheon.

Vote Tallying System, który wymagał jednak użycia specjalnego pisaka. W połowie lat 60. skanujący zaznaczenia zwykłym ołówkiem system Votronic (1965) zaczął w USA konkurować ze stosowanymi wtedy już od kilkudziesięciu lat systemami korzystającymi ze specjalnych kart dziurkowanych w urządzeniach dźwigniowych (m.in. IBM Votomatic). Stosowanie maszyn dźwigniowych oraz na karty perforowane zostało zakazane przez Help America Vote Act (HAVA) uchwalony w 2002 r. po wspomnianych problemach z niedokładnie przedziurkowanymi kartami w wyborach na Florydzie w 2000 r.

W 1974 r. pojawił się w USA pierwszy system wyborczy bez papierowego nośnika głosu – rejestrujący głosy elektronicznie bezpośrednio w urządzeniach DRE. W 1982 r. w wyborach uzupełniających do parlamentu stanowego w indyjskim stanie Kerala po raz pierwszy użyto maszyn EVM w 50 komisjach wyborczych.

Maszyny EVM, głównie w wersji DRE, są lub były stosowane w kilkunastu krajach świata – m. in. w Albanii, Armenii, Belgii, Bułgarii, Filipinach, Hiszpanii, Kanadzie, Kenii, Nigerii, Namibii, Ugandzie, Zambii, Sigapurze, Szwajcarii, USA. Dość wcześnie i dość szeroko wprowadzano maszyny EVM/DRE w Ameryce Południowej i Środkowej: w Argentynie, Brazylii, Ekwadorze, Meksyku, Panamie, Paragwaju, Peru i Wenezueli, przy czym w Ekwadorze tylko pilotażowo w 2014 r. w wyborach lokalnych w wybranych okręgach, zaś w Paragwaju tylko w trzech wyborach parlamentarnych w latach 2001–2006, gdzie po krytyce zastosowanych rozwiązań w 2007 r. powrócono do metod tradycyjnych.

W Brazylii głosowanie z wykorzystaniem EVM/DRE zostało przeprowadzone po raz pierwszy w 1996 r., od 2000 r. wszystkie wybory w Brazylii są w pełni zelektronizowane. W Wenezueli maszyny własnego projektu i produkcji zastosowano w 1998 r. i od tego czasu stosowane są we wszystkich wyborach.

W Indiach – największym państwie świata pod względem liczby ludności (1,411 mld w 2022 r.) – głównym problemem wyborów jest nie tylko liczba wyborców, ale także złożona struktura polityczno-administracyjna tego ogromnego kraju i równie złożona ordynacja wyborcza. Indie są republiką federacyjną, na którą składa się 28 stanów, 7 terytoriów związkowych oraz Narodowe Terytorium Stołeczne (Delhi i okolice – ponad 16 mln mieszkańców). W wyborach bezpośrednich wybieranych jest na pięcioletnią kadencję 530 z 552 członków izby niższej (Lok Sabha – Izba Ludowa) dwuizbowego parlamentu. Izba wyższa (Rajya Sabha – Izba Stanowa) wybierana jest przez parlamenty stanowe. Parlamenty stanowe w 5 stanach są dwuizbowe, w pozostałych jednoizbowe, liczą od 60 do 500 członków. Wybierani są oni w wyborach bezpośrednich, co 2 lata wymieniana jest 1/3 składu.

Powszechne wybory do Izby Ludowej są „rolowane" po wielkim terytorium Indii – odbywają się kolejno w 7 jednodniowych fazach na poszczególnych obszarach liczących od 7 do 20 stanów (granice obszarów nie pokrywają się z granicami stanów i terytoriów), w których wybiera się proporcjonalną do liczby ludności liczbę deputowanych określoną dla każdego obszaru przez Indyjską Komisję Wyborczą. Od 2014 r. EVM/DRE wraz urządzeniami/drukarkami VVPAT stosowane są we wszystkich wyborach powszechnych oraz stanowych Indii i obecnie nigdzie nie jest stosowany tradycyjny system głosowania na kartach papierowych.

Głosowanie w Indiach

*Źródło: https://images.app.goo.gl/YLZD16PfgMDFhxuT6*

**Indie – skala problemu**

**W wyborach w Indiach w 2019 r. niemal 2,5 tys. partii politycznych zgłosiło 8 039 kandydatów do Izby Ludowej. Łącznie uprawnionych do głosowania było ponad 912 mln wyborców. Głosy oddało 613 146 768 wyborców (frekwencja wyniosła 67,4%). Głosowali oni w 1,04 mln lokali wyborczych, w których działało 3,96 mln maszyn EVM i 1,74 mln urządzeń VVPAT. Ponieważ zgodnie z indyjską ordynacją wyborczą żaden wyborca nie może mieć dalej niż 2 km do komisji wyborczej, więc niezwykle ważnym elementem logistyki wyborów było dostarczanie na czas przenośnych, zasilanych bateryjnie zestawów EVM/DRE i VVPAT do wszystkich komisji wyborczych na terytorium Indii liczącym 3 287 263 km$^2$.**

Indie 2019 – zestawy EVM/VVPAT przygotowane do wysyłki

*Źródło: https://images.app.goo.gl/NfKws4wmisqUEjQ49*

Od ponad 30 lat EVM/DRE są stosowane w Belgii, obecnie we wszystkich typach wyborów – od lokalnych wyborów samorządowych przez wybory do dwuizbowego parlamentu federalnego po wybory do Europarlamentu. Królestwo Belgii jest krajem federalnym o złożonej strukturze administracyjnej. Ordynacja wyborcza dla obu izb (Izby Reprezentantów i Senatu) jest dość skomplikowana, np. tylko część spośród 71 senatorów jest wybierana bezpośrednio, a wśród senatorów desygnowanych na mocy konstytucji są dzieci króla Belgii (jeśli mają ukończone 18 lat, pełne prawo głosu w Senacie mają od 21 roku życia). W wyborach do Senatu kraj jest podzielony na 3 okręgi wyborcze: flamandzki, waloński i Bruksela-Hal-Vilvorde. W wyborach do Izby Reprezentantów jest 11 okręgów wyborczych, w każdym z nich wybiera się od 4 do 24 przedstawicieli (izba liczy 150 reprezentantów). Od 1893 r. głosowanie jest obowiązkowe (w wyborach do obu izb parlamentu, obecnie także do Parlamentu Europejskiego, od bieżącego roku nie jest obowiązkowe w wyborach lokalnych)[7], za nieuczestniczenie są kary finansowe (od 5 do 25 euro, ale mogą być podwyższone dziesięciokrotnie), czterokrotne nieuczestniczenie może zostać ukarane nawet skreśleniem z list wyborców na 10 lat wraz z zakazem pełnienia funkcji publicznych[8]. Deklarowanym celem wprowadzania od 1991 r. EVM było zmniejszenie liczby głosów nieważnych oraz skrócenie czasu zliczania oddanych głosów. W pierwszym użytym systemie maszyny miały ekrany dotykowe, w drugim (równolegle stosowanym do 2010 r.) używano piór świetlnych i kart magnetycznych udostępnianych wyborcom w lokalu, służących do zapisu oddanego głosu. Obecnie stosowane są nowoczesne maszyny DRE, zaś ordynacja wyborcza umożliwia głosowanie zarówno w maszynach, jak i tradycyjne, na papierowych kartach.

Niepokoje polityczne, protesty i rozruchy wpłynęły negatywnie na wybory w Kenii w 2022 r. i w Nigerii w 2023 r. – choć użycie EVM/DRE od lat ułatwiało tam identyfikację wyborców oraz oddawanie i zbieranie głosów. W Kenii (22,12 mln zarejestrowanych wyborców) w komisjach wyborczych użyto ponad 46 tys. przenośnych zestawów wyposażonych w czytniki biometryczne do trwającej średnio 9 sekund autentykacji wyborców, 99% rezultatów zostało przetransmitowanych do centralnej komisji w dniu wyborów – ale frekwencja wyborcza, choć w porównaniu np. z naszym regionem Europy dość wysoka (65%) była najniższa od 15 lat. W Nigerii (93,5 mln zarejestrowanych wyborców, EVM wprowadzono głównie w celu identyfikacji wyborców) frekwencja w wyborach w lutym 2023 r. wyniosła zaledwie 26,7% (co i tak oznaczało 24,9 mln głosujących) – i była najniższa od 1999 r. Najwyższa, ponad 69% była w 2003 r., natomiast w roku 2011, kiedy wprowadzono EVM, wynosiła 53,7%.

## Co przemawia za elektroniką

Systemy DRE przede wszystkim istotnie skracają krytyczny czas liczenia głosów. Dostawca jednego z takich systemów chwali się, że w wyborach parlamentarnych i prezydenckich w Argentynie w 2019 r. już w 3 godziny po zamknięciu o godz. 18:00 lokali wyborczych oficjalnie podliczone zostało niemal 70,5% głosów, zaś do północy – ponad 96% spośród 27,5 mln oddanych głosów (frekwencja ponad 80,4%). Nawet szybciej dostępne były pełne wyniki wyborów prezydenckich w Argentynie w 2023 r. (22 października – pierwsza tura, 19 listopada – druga tura). Na Filipinach, gdzie maszyny zastosowano po raz pierwszy w 2010 r., a w wyborach w 2022 r. głosowało ok. 67 mln wyborców, wyniki były dostępne 2 godziny po zamknięciu lokali wyborczych.


Terminal wyborczy w Brazylii

*Źródło: https://www.wilsoncenter.org/person/anya-prusa*

W wyborach powszechnych w Brazylii w 2022 r. maszyny zliczały 123 682 372 głosów[9] (frekwencja 79,05%). Oficjalne wyniki były znane już po kilku godzinach, a z mniejszych miejscowości – po kilku minutach po zakończeniu głosowania na gubernatorów i wicegubernatorów sta-

7 W krajach UE udział w wyborach jest obowiązkowy w Belgii, Bułgarii, Grecji i Luksemburgu.

8 Ciekawą różnicę w zachowaniach wyborców przytoczono w literaturze przedmiotu: średnio w latach 1995-2014 frekwencja w prowincji Liège w gminach, które pozostały przy tradycyjnym głosowaniu na kartach papierowych przekraczała 90,35%, zaś w gminach głosujących elektronicznie wynosiła 87,56%. W Limburgii frekwencja wynosiła odpowiednio 94,07% i 92,61% (R. Dandoy, DOI: 10.4324/9781003104643-5),

9 W Brazylii czynne prawo wyborcze mają wyborcy od 16 roku życia, udział w wyborach jest obowiązkowych dla wyborców między 18 a 70 rokiem życia.

nów, deputowanych i senatorów dwuizbowego Kongresu oraz parlamentów stanowych (w wyborach prezydenta potrzebna była druga tura). W Indiach w 2019 r. kolejne jednodniowe fazy wyborów rozpoczęły się 11 kwietnia i zakończyły 19 maja. Obliczanie głosów rozpoczęto rano 23 maja i tego samego dnia Indyjska Komisja Wyborcza ogłosiła oficjalne wyniki ponad 613 mln oddanych głosów.

Obok skrócenia czasu zbierania głosów i obliczania wyników systemy e- oraz i-votingu[10] zasadniczo obniżają udział głosów nieważnych z powodów błędów – zarówno wyborców, jak i liczących głosy. Oprogramowanie maszyn EVM/DRE przeważnie zawiera mechanizmy kontroli poprawności oddanego głosu, np. uniemożliwiając oddanie głosu na więcej kandydatów, niż określają to przepisy dotyczące konkretnych wyborów, ostrzegając o niewybraniu żadnego kandydata (w niektórych krajach jest możliwość zaznaczenia oddzielnej opcji „nie wybieram żadnego z kandydatów). Na ekranach można zaprezentować zdjęcia kandydatów i/lub logotypy partii politycznych, co razem z ekranami dotykowymi umożliwia uczestnictwo w wyborach nawet wyborcom niepiśmiennym. W krajach wieloetnicznych istotne jest łatwość udostępnienia wielu wersji językowych interfejsów maszyn i systemów. Dodatkową korzyścią jest dużo łatwiejsze stosowanie narzędzi lub rozwiązań wspierających głosowanie przez wyborców z różnymi niepełnosprawnościami. W kilku krajach systemy elektroniczne – choć nie są stosowane „na miejscu" – umożliwiają zdalne głosowanie uprawnionym wyborcom mieszkającym na stałe czy znajdującym się czasowo zagranicą (jest to niejako unowocześnienie głosowania pocztowego z zagranicy). Mimo sporych nakładów inwestycyjnych, a także kosztu utrzymania i ewentualnej aktualizacji systemów używanych przeważnie tylko co kilka lat, jednostkowe koszty głosowania elektronicznego są dużo niższe niż głosowania tradycyjnego.

Według oceny Głównego Inspektora Wyborczego Delhi zastosowanie EVM zaoszczędziło ok. 10 tys. ton papieru używanych na karty i inne dokumenty wyborcze w tradycyjnych wyborach parlamentarnych. Zastosowanie systemu bazującego na EVM położyło też kres licznym aktom przestępczym dokonywanym w czasie i wokół wyborów (wymuszanie głosów, handel głosami, manipulacje z kartami itp.). Zjawiska te narastały w latach 90. tak bardzo, że w 1998 r., kiedy po raz pierwszy zaprezentowano urządzenie EVM (rodzimej produkcji) ani Indyjska Komisja Wyborcza, ani sądy nie miały wątpliwości co do konieczności „mechanizacji" wyborów, choć do dziś podnoszone są zastrzeżenia dotyczące zarówno samych maszyn, jak i transmisji danych do komisji centralnej.

EVM/DRE są elementem całych platform elektronicznej obsługi głosowania – tym najbardziej widocznym dla wyborców. Bardzo ważnym elementem systemów wyborczych są narzędzia weryfikacji wyborcy, np. na podstawie odcisku palca czy dowodu osobistego z warstwą elektroniczną[11].

Pięć miesięcy przed wyborami w Brazylii w 2022 r. prezydent Jair Bolsonaro zarządził dodatkowy szczegółowy audyt systemu i maszyn (co opozycja uznała za szukanie pretekstu do nieuznania wyniku wyborów w razie ewentualnej przegranej), zaś po przegranej musiał się tłumaczyć przed komisją parlamentarną z wynajęcia za 8 tys. dolarów programisty, który miał zdyskredytować wyniki wyborów, włamując się do maszyny DRE – co mu się jednak nie udało, urządzenie okazało się odporne na ingerencję.

## Nie ma systemu bez wad

Jest wiele opracowań na temat zastrzeżeń do systemów wspierających wybory – i to zarówno systemów wykorzystujących maszyny EVM/DRE, jak w głosowaniu internetowym.

W kilku krajach rzeczywiste błędy i usterki urządzeń oraz systemów doprowadziły do wycofania się z e- oraz i-wyborów (Holandia, Irlandia, Niemcy, Norwegia). W Nigerii, gdzie wyborom w 2023 r. towarzyszyły nie tylko masowe protesty, ale nawet fizyczne walki oponentów, „oliwy do ognia" dolały opóźnienia przesyłania wyników oraz gubienie ich części z powodu błędów transmisji wynikających z niewydolnej infrastruktury transmisyjnej.

W Holandii pierwsze maszyny dźwigniowe zastosowano w 1966 r. W 1968 r. rozpoczęto projektowanie własnych maszyn EVM. Do ich produkcji wybrano krajową firmę Nederlandse Apparaten Fabriek NV (NEDAP), która zaczęła modyfikować oryginalny projekt. W końcu lat 80. w wyborach krajowych stosowano już ok. 1200 maszyn NEDAP. Dopiero w 1990 r. centralny organ wyborczy oraz ministerstwo spraw wewnętrznych stwierdziły, że obowiązujące przepisy w zasadzie nie formułują wymagań odnoszących się do tych urządzeń. Rozpoczęła się dyskusja nad wymaganiami i przepisami, ale weszły one w życie dopie-

10 Choć często e-votingiem nazywane jest ogólnie głosowanie wspierane elektronicznie, w ślad za zwyczajem przeważającym w literaturze przedmiotu -e-votingiem nazywamy w tekście głosowanie z użyciem maszyn, zaś i-votingiem – głosowanie on-line przez Internet.

11 Warto nadmienić, że w USA nie ma jednolitego systemu weryfikacji wyborców (choćby z racji braku wspólnego, federalnego dokumentu tożsamości – nawet używane często w tej roli prawa jazdy różnią się w zależności od stanu, w którym je wydano) a nawet jednolitego systemu rejestracji wyborców.

ro w 1997 r. i nadal nie wymagały udostępniania wyborcy jakiegokolwiek potwierdzenia oddanego głosu. Mimo tego braku, a także nieudostępnieniu przez NEDAP kodu źródłowego oprogramowania, pod koniec lat 90. ok. 95% wyborców holenderskich głosowało z użyciem EVM/DRE produkcji NEDAP i drugiego dostawcy VUGA/SDU (jego udział w dostawach wynosił tylko 5%). Choć pojawiało się coraz więcej wątpliwości dotyczących prawidłowego działania urządzeń, zgłaszanych centralnej Komisji Wyborczej i w interpelacjach parlamentarnych, to jednak nawet opisana poniżej rezygnacja z użycia tych maszyn w Irlandii w 2004 r. nie wywołała reakcji holenderskiego rządu.

Użycie maszyn NEDAP i SDU zakwestionowała dopiero społeczna inicjatywa pod hasłem „Nie ufamy wyborczym komputerom" rozpoczęta przez Ropa Gonggrijpa, założyciela jednego z pierwszych holenderskich dostawców Internetu. Inicjatywa domagała się w trybie informacji publicznej od Komisji Wyborczej i od ministerstwa dokumentów certyfikacyjnych i potwierdzeń bezpieczeństwa zamkniętego kodu oprogramowania NEDAP. W październiku 2006 r. inicjatywa opublikowała raport z badania dwóch maszyn NEDAP ESB3 odkupionych od urzędu miasta Amsterdamu po wyborach lokalnych. Konkluzje raportu były miażdżące, zarówno w odniesieniu do oprogramowania, jak i możliwości przeprogramowania (w ciągu 5 minut) zupełnie niezabezpieczonego fizycznie układu w maszynie, co umożliwiało manipulację danymi.

Początkowo obaj dostawcy maszyn walczyli z inicjatywą w sądach, ale ostatecznie – także po krytycznych raportach dwóch specjalnych komisji rządowych oraz zapoznaniu się z raportami z Irlandii – w październiku 2007 r. zarówno certyfikaty dla maszyn, jak i przepisy umożliwiające ich stosowanie zostały wycofane i Holandia wróciła do tradycyjnego głosowania kartami papierowymi[12].

Jak wcześniej wspomniano, holenderskie maszyny nie sprawdziły się też w Irlandii. Po testach z 6 maszynami NEDAP w 2001 r. (wtedy wprowadzono odpowiednie zmiany do ordynacji) zakupiono najpierw 600, a potem jeszcze 400 maszyn i przeprowadzono pilotażowe głosowania w trzech regionach w 2002 r. W marcu 2003 r. zamówiono kolejne 6 tys. maszyn NEDAP (kosztowały 51 mln EUR), które miały być użyte w wyborach lokalnych oraz eurowyborach w czerwcu 2004 r. Nacisk polityczny ze strony rządu był tak duży, że zupełnie zignorowano raporty z pilotaży o błędach i nieprawidłowym działaniu maszyn oraz sygnały z Holandii. W marcu 2004 r. rząd powołał specjalną komisję ds. głosowania elektronicznego, która przez dwa miesiące miała przygotować ostateczny raport potwierdzający gotowość systemu. Pierwszego maja komisja opublikowała raport z główną konkluzją: komisja nie zaleca przeprowadzenia głosowania z wykorzystaniem zakupionych EVM. Zastrzeżenia komisji oraz licznych krytyków projektu dotyczyły braku drukowanego potwierdzenia dla wyborcy (i jakiegokolwiek rozwiązania VVPAT) – co zdaniem komisji oraz ekspertów nie budowało zaufania wyborców, tak potrzebnego przy wprowadzaniu nowego systemu. Komisja podniosła też problem nieudostępnienia przez dostawcę kodu źródłowego oprogramowania, zaś jej eksperci wskazywali na podatności oprogramowania, umożliwiające manipulowanie danymi. W rezultacie na 5 tygodni przed ustalonym terminem wyborów rząd wycofał się z projektu EVM i wybory przeprowadzono w tradycyjny sposób. Koszty zarówno polityczne, jak i finansowe były wysokie: ówczesna partia rządząca w wyborach uzyskała najgorszy wynik od lat 20. Do 51 mln euro „utopionych" w samych maszynach (łącznie z testowymi było ich 7,5 tysiąca) doszły koszty ich składowania przez następne 8 lat (3 mln euro), dodatkowo kilkadziesiąt tysięcy zapłacono za doradztwo na temat tego, co zrobić z tym fantem. W końcu w 2012 r. maszyny udało się sprzedać na złom. Firma recyklingowa kupiła je wszystkie za łączną kwotę 70 tys. euro (czyli po 9,30 za sztukę). Za chichot historii można uznać fakt, że nabywca, właściciel firmy recyklingowej, uczestniczył jako testowy wyborca w pilotażowym głosowaniu w 2002 r.[13]

Tekst o głosowaniu internetowym on-line, nazywanym i-votingiem, pojawi się w kolejnym wydaniu „Domany".

12 https://www.ndi.org/sites/default/files/5_Netherlands.pdf (dostęp: 15.02.2024)

13 https://www.independent.ie/irish-news/54m-voting-machines-scrapped-for-9-each/26870212.html (dostęp: 14.02.2024)

Wiesław Paluszyński
prezes PTI


Fot. Beata Sołtys

# Gadał dziad do obrazu...

Wielokrotnie uczestniczyłem w posiedzeniach sejmowych komisji, a nawet jako ekspert odnosiłem małe sukcesy w naprawianiu wpływających do Sejmu propozycji. Ostatnie lata przekonały mnie jednak, że zapraszających nie interesuje opinia gości, więc zacząłem bardziej cenić swój czas, a także możliwość działania na własnych warunkach i przestałem uczestniczyć w tych gremiach.

Złamałem się jednak, gdy dostałem zaproszenie na posiedzenie połączonych Komisji Cyfryzacji i Edukacji poświęcone programowi „Laptop dla ucznia". Jest on mi szczególnie bliski, bo rok temu po mojej krótkiej wypowiedzi na jego temat zostałem zaszczycony „Listem otwartym" ówczesnego ministra cyfryzacji Janusza Cieszyńskiego, w którym zmieszał mnie z błotem i skłonił do szczegółowej odpowiedzi, co sadzę o przygotowaniu tego programu (korespondencja jest dostępna na naszym portalu).

Wszystkie moje zastrzeżenia potwierdziły się w trakcie realizacji programu, byłem więc ciekaw opinii posłów na ten temat. Spodziewałem się refleksji i prezentacji koncepcji ratowania jakiś fragmentów tej inicjatywy. Stawiłem się więc w Sejmie i cierpliwie odczekałem godzinę spóźnienia. Na spotkanie stawili się posłowie obecnej opozycji z posłem Januszem Cieszyńskim na czele, przedstawiciele MC, MEN i posłowie obecnej koalicji oraz liczne grono gości. Poziom kultury dyskusji i wymiany poglądów był porażający.

Ocena realizacji tego programu przez przedstawicieli ministerstw niewiele różniła się od mojej prognozy sprzed roku. Były minister cyfryzacji dokonywał ekwilibrystycznych sztuk, aby wykazać, że rozdanie komputerów dzieciom (a właściwe ich rodzicom) było pełnym sukcesem. Natomiast uzupełnienie braku oprogramowania bezpieczeństwa i narzędziowego to, jego zdaniem, zadanie dla samorządów. Zapomniał tylko o tym, że komputery są teraz prywatną własnością, a samorząd nie może obdarowywać ze swoich pieniędzy osób fizycznych. Niektórzy posłowie rzewnie opowiadali o płaczu rodziców, gdy dostawali laptopy, taki to był dla nich skok cywilizacyjny. Nieco to dziwne, bo nie mówimy o programie socjalnym, tylko o wspierającym cyfrową edukację.

Nikt nie zadał sobie trudu odpowiedzi na pytanie, jak dzieci mają nosić te ciężkie laptopy do szkoły. Zresztą okazało się, że i tak nie mogą, bo do sieci OSE nie można podłączać prywatnego sprzętu. Laptop ma siedzieć w domu. Nikt nie zapytał, jakie wnioski wysnuto ze zdalnego nauczania w czasie pandemii przy okazji tego programu. Poza informacją, że w kolejnym roku komputerów nie będzie – bo nie zapewniono w budżecie na nie pieniędzy i powstanie nowy program po stworzeniu strategii cyfryzacji edukacji – żadne konkrety nie padły.

Czyli mamy stan po burzy, dzieci mają w domach sprzęt, z którym robią, co chcą, a zainteresowanych tym, co robią, odsyłam do mediów społecznościowych, wpisy są pouczające!

Programu ratunkowego nie ma, miliardy wydane, politycy okładają się wypowiedziami jak cepami. Pytanie o propozycję, co z tym pasztetem zrobić, wykraczało, zdaniem przewodniczącej Komisji Edukacji, poza ramy spotkania poświęconego wyłącznie ocenie.

Ja zostałem ze swoim dylematem, czy warto chodzić na takie spotkania. Mam nadzieję, że coś się jednak zmieni i będzie szansa na sensowną dyskusję, bo przed nami Ustawa o Krajowym Systemie Cyberbezpieczenstwa, regulacje o sztucznej inteligencji i implementacja do polskiego porządku całego legislacyjnego tsunami UE. Postaram się dzielić sprawiedliwie te aktywności wśród członków naszych władz, bo jedna osoba może skończyć – jeśli sposób funkcjonowania parlamentu się nie unormuje – u lekarza specjalisty od stresu pourazowego.

**Michał Ogórek**
satyryk i felietonista, od 1989 r. związany z „Gazetą Wyborczą". Obecnie pisuje w „Angorze". Autor wielu książek. Ostatnio wydał „Sto lat! Jak czciliśmy przywódców w ostatnim stuleciu", o kulcie przywódców – od Piłsudskiego przez Bieruta i Gomułkę po braci Kaczyńskich.

# Czy sztuczna inteligencja nas zaora

**Kiedy mamy do czynienia ze zjawiskiem całkiem nowym, aby je jakoś oswoić, robimy sobie porównania do czegoś już znanego, choć na ogół całkiem różnego. Aby zwizualizować sztuczną inteligencję – najnowszą królową tajemnic – dokonywano już wielu nieprawdopodobnych analogii, ale wszystko przebił szacowny „The Economist", który w sztucznej inteligencji zobaczył… traktor.**

Użycie tego niemal obraźliwego porównania miało być może trochę polepszyć samopoczucie ludzi, którzy nic o niej nie wiedzą, jako że o traktorze również, a przecież w ogóle nie wpływa to rujnująco na ich samoocenę i ich wyobrażeń o sobie nie niszczy. Przeciwnie: całkowita nieznajomość traktora może nawet być źródłem poczucia wyższości i ulgi.

## Dzielenie skóry na niedźwiedziu

Taka również mogła być motywacja „Economista", ale nie jest to powód jedyny. Pismo przytacza również inne argumenty. Jak przystało na ten tytuł, skupia się na wymiarze ekonomicznym i wylicza, że upowszechnienie w pierwszej połowie XX w. traktora doprowadziło w skali globu do takiego skoku dochodu PKB, jaki spodziewany jest obecnie za sprawą zastosowania sztucznej inteligencji.

Zauważmy, że nikogo nie zraża, że zupełnie nie wiadomo, do czego ta sztuczna inteligencja zostanie zastosowana i w jakim zakresie, a nawet czy, a szczególnie komu przyniesie jakieś wymierne korzyści, ale już wyliczono dokładnie zyski z niej płynące. Przyniesie wzbogacenie się świata o siedem procent globalnego dochodu w ciągu dziesięciu lat. To, że w ogóle nie wiadomo, co z niej wyrośnie, nie przeszkadza w dzieleniu skóry na niedźwiedziu. Nikt nie bierze pod uwagę, że może to być niedźwiedź polarny, który na roztopionej z powodu ocieplenia klimatu krze Bieguna Północnego może już tego nie doczekać.

## Inne oblicze traktora

Złośliwy zresztą traf sprawił, że ledwo „The Economist" wyciągnął ten nieco już zardzewiały traktor ze swojego redakcyjnego archiwum wynalazków, pojazd ten nabrał wyjątkowej aktualności i opuszczając wiejskie ostępy, triumfalnie wyjechał na ulice miast całej Europy, łącznie z centralą w Brukseli. Okazało się tym samym, że te siedem procent globalnego dochodu brutto może przynosić nam też wymierne straty.

Nie udawajmy zresztą, że traktor zawsze kojarzy się z jakąś korzyścią: wystarczy, że wyjeżdża nam przed maskę na wąskiej drodze. W takich przypadkach nikt nie przekona nas, że nie opóźnia on postępu społecznego i nie zmniejsza tempa przyrostu naszych dochodów.

Teraz jednak okazało się, że brak korzyści z tego epokowego wynalazku przenosi się i na jego głównych – wydawałoby się – beneficjentów, czyli rolników, wykonujących swą robotę jak w klimatyzowanej limuzynie, no może tylko podskakującej jak na pohitlerowskiej autostradzie pod Wrocławiem.

Tym samym wyszło na jaw, że wszelkie kalkulacje zysków z wynalezienia traktora mogą wziąć w łeb. I to z różnych, a nawet przeciwstawnych powodów. Nie tylko może w pole nie będzie już po co nim wyjeżdżać z powodu zmian klimatycznych, lecz także z powodu zapobiegania traktorom, karnie egzekwowanemu przez Komisję Europejską.

Już policzone, a nawet podzielone zyski z traktora zaczynają przynosić straty i to nie dlatego, że ów motor postępu nie spełnia przydzielonych mu zadań, lecz właśnie dlatego, że robi to za gorliwie.

> *Okoliczność, że sztuczna inteligencja pod jakąkolwiek postacią wyjedzie blokować autostrady nie jest brana pod uwagę w planach jej rozwoju, a przecież w ogóle nie wiemy, co siedzi w jej głowie, a nawet gdzie ją ma.*

Nie wiadomo też, jak zareaguje, kiedy dowie się, że ma przynieść światu siedem procent zysku, sama nie będąc brana pod uwagę przy jego podziale. Trudno zakładać, że da się tak robić w konia przez ludzi, jak traktor; jakiś swój własny rozum bowiem ma.

Potwierdzają się wszystkie czarne wizje dotyczące złego i niezgodnego z przeznaczeniem wykorzystywania tych wynalazków. Jeśli traktor, który miał siedzieć w polu, jest w stanie zerwać wszystkie hamulce i wmieszać się w politykę europejską, to co dopiero może zrobić sztuczna inteligencja. Widzieliśmy w telewizji jakiego poświęcenia wymagało od Marie Le Pen w kampanii wyborczej już nie uruchomienie, ale nawet samo wejście na traktor: teraz wyobraźmy sobie, jak będzie ujarzmiać sztuczną inteligencję.

Potwierdza to tylko naszą stałą początkową lekkomyślność przy uwalnianiu z butelki każdego dżina, jakiego chcemy wprząc do pracy na naszą rzecz. W socjalistycznej Polsce w czasach mechanizacji rolnictwa lansowano taki wierszyk: „Tata na traktorze, mama na traktorze, a Hania w przedszkolu w świetnym jest humorze". A okazuje się, że Hania też zaorana.

**15-16 maja'24**

ŚWIATOWY DZIEŃ SPOŁECZEŃSTWA INFORMACYJNEGO

SDSI

# CYFROWE INNOWACJE DLA ZRÓWNOWAŻONEGO ROZWOJU

**Technosfera przemysłu i edukacji przyszłości**

www.sdsi.pl

Organizatorzy

POLSKIE TOWARZYSTWO INFORMATYCZNE

SEP

Partnerzy debat

Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo

Sektorowa Rada ds. Kompetencji Informatyka

Platforma Przemysłu Przyszłości