Krytyczne myślenie na serio

Według Wikipedii, krytyczne myślenie to proces analizowania dostępnych faktów, dowodów, obserwacji i argumentów w celu wyciągnięcia wniosków lub dokonania świadomych wyborów (pl.wikipedia.org/wiki/Krytyczne_myślenie). Podobno ma kluczowe znaczenie w erze natłoku informacji i powszechnej dezinformacji. Do krytycznego myślenia szczególnie namawiają instytucje rządowe. Dopóki krytyka nie dotyczy ich własnych działań.

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.

W numerze 3-4/2024 „Domeny" wspomniałam o bezrefleksyjnym przepisaniu do wytycznych ważnego ministerstwa zasad dotyczących bezpiecznego korzystania z internetu i mediów opublikowanych przez znaną fundację. Wzmianka dotyczyła wytycznych do Standardów ochrony dzieci (SOM-ów) wydanych w 2024 r. przez Ministerstwo Sprawiedliwości w części dotyczącej korzystania z internetu i urządzeń mobilnych.

Krytycznie o SOM-ach

Jako inspektor ochrony danych w przedszkolach uważnie zapoznałam się z wytycznymi ochrony dziecka w przedszkolach i w internecie, przygotowanymi przez Zespół do Spraw Ochrony Małoletnich powołany na podstawie ustawy o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich. Czytając dokumenty miałam nieodparte wrażenie, że autorzy wytycznych w ogóle nie znają i w związku z tym nie uwzględnili działań, czynności i prac już podjętych i cały czas prowadzonych w placówkach oświatowych dotyczących bezpieczeństwa online. Tak, jakby nie było KRI od 2012 r., RODO od 2016 r. czy KSC od 2018 r.

Swoje zastrzeżenia wysłałam do resortu, wskazując, że wytyczne zawierają zapisy sprzeczne z obowiązującymi przepisami, standardami i dobrymi praktykami dotyczącymi zapewnienia cyberbezpieczeństwa, bezpieczeństwa informacji i ochrony danych osobowych. Z pisma otrzymanego cztery miesiące później dowiedziałam się, że wytyczne:

- to w założeniu praktyczny, krótki zbiór wskazówek, przyswajalny dla osób o różnym poziomie umiejętności;
- nie zastępują obecnie obowiązujących przepisów ustaw czy rozporządzeń;
- zostały przygotowane przez interdyscyplinarne grono ekspertów m.in. z Ministerstwa Cyfryzacji oraz NASK bazujących na dokumencie opracowanym przez ekspertów z Fundacji Dajemy Dzieciom Siłę, standardach i dobrych praktykach wykorzystywanych w środowisku szkolnym w Wielkiej Brytanii i Australii, materiałach organizacji pozarządowych działających na rzecz bezpieczeństwa dzieci w internecie, publikacjach NASK i Ministerstwa Edukacji Narodowej;

moje zaś uwagi będą na pewno poddane analizie podczas aktualizowania wytycznych. Czyli nie ma tematu.

Temat SOM-ów jednak wrócił 3 czerwca 2025 r. na wspólnym posiedzeniu Komisji Cyfryzacji i Komisji ds. Dzieci i Młodzieży Sejmu RP dotyczącym dzieci i młodzieży w internecie, w którym uczestniczyli przedstawiciele Ministerstwa Cyfryzacji, Ministerstwa Edukacji Narodowej i Ministerstwa Sprawiedliwości. Skorzystałam z okazji i poddałam w wątpliwość profesjonalizm autorów wytycznych do SOM-ów. Koronny argument powinien być zrozumiały dla wszystkich obecnych. Otóż wytyczne zalecają korzystanie przez przedszkola z Ogólnopolskiej Sieci Edukacyjnej (OSE) oraz z zaawansowanych usług bezpieczeństwa OSE plus. Tyle, że zgodnie z art. 2 ustawy o Ogólnopolskiej Sieci Edukacyjnej, OSE jest publiczną siecią telekomunikacyjną, która publicznie świadczy dostępne usługi telekomunikacyjne **szkołom** w rozumieniu art. 2 pkt 2 ustawy Prawo oświatowe. **Szkołom, nie przedszkolom**. Autorzy (zresztą obecni na sali) o tym nie wiedzieli? Zasugerowałam wymianę ekspertów, którzy będą aktualizować wytyczne.

Ponieważ jako jedyna osoba zabierająca głos musiałam skrócić moją wypowiedź, nie mogłam zadać pytań dotyczących innych aspektów bezpieczeństwa dzieci i młodzieży w internecie, które powinny zostać zadane w trakcie trzygodzinnego posiedzenia. Pytania te dotyczą:

- powierzania danych firmom big-tech, zwanym chupadados. Czy wiemy, jak wielkie platformy wykorzystują dane naszych dzieci i o naszych dzieciach przetwarzane w ich systemach? Czy dane zasilają systemy sztucznej inteligencji? Problem poruszyłam w numerze 4/2022 „Domeny", przywołując raport organizacji Human Rights Watch zatytułowany „How Dare They Peep into My Private Life?' Children's Rights Violations by Governments that Endorsed Online Learning during the Covid-19 Pandemic", w którym wezwano rządy do ustanowienia nowych praw ochrony danych dzieci w internecie;
- aplikacji rekomendowanych przez MEN. Kto sprawdza, gdzie trafiają dane? Dobrym przykładem jest polecana na Zintegrowanej Platformie Edukacyjnej gra „Warsaw Rising – Miasto Bohaterów" Instytutu Pamięci Narodowej do pobrania z platformy STEAM amerykańskiej korporacji Valve z siedzibą w Bellevue, WA. Zgodnie z ich Polityką Prywatności to Federalna Komisja Handlu (FTC) sprawuje jurysdykcję nad przestrzeganiem przez „Valve Ram" ochrony danych UE-USA (*Data Protection Framework EU-USA*) i przeprowadza wiążące arbitraże. Czy MEN pomoże uczniom, ich rodzicom i opiekunom, nauczycielom i szkołom w postępowaniu przed FTC w przypadku naruszenia ochrony danych osobowych?
- patronatu ministerstw nad różnymi przedsięwzięciami dotyczącymi dzieci (konkursy, projekty, szkolenia itp.). Czy instytucje pytają organizatorów, jak i gdzie będą przetwarzane dane osobowe dzieci biorących udział w imprezach i uzależniają przyznanie patronatu od spełnienia wszystkich obowiązujących przepisów? Dobrym przykładem jest projekt IT Fitness Test (itfitness.eu/pl), czyli największy bezpłatny test kompetencji cyfrowych uczniów i nauczycieli państw Grupy Wyszehradzkiej i Ukrainy, zapoczątkowany w Słowacji w 2010 r. Według Polityki Prywatności opublikowanej na stronie projektu, organizatorem i administratorem danych osobowych jest Związek Cyfrowa Polska z siedzibą w Warszawie. Według Regulaminu testy odbywają się za pośrednictwem kompleksowej platformy

informatycznej obsługiwanej przez Koalicję Cyfrową, Stowarzyszenie Interesów Osób Prawnych z siedzibą w Bratysławie. Natomiast według informacji na stronie https://digital-skills-jobs.europa.eu/en/inspiration/resources/it-fitness-test-largest-free-online-digital-skills-assessment-v4-countries organizatorem jest IT Association of Slovakia (ITAS). Niezły RODO-wy miszmasz.

Krytycznie o wyborach

Mamy za sobą kolejne wybory powszechne. Media pełne były doniesień o różnych wątpliwościach prawnych. Przyjrzyjmy się wątpliwości RODO-wej.

Na trzy godziny przed ciszą wyborczą drugiej tury wyborów prezydenckich trafiłam w internecie na rozmowę dwóch znanych mediaworkerów (MW) ze znanym politykiem (ZP). Zaskoczyła mnie taka wymiana zdań:

MW1: ***Nie zbiorą, tylko kupią. Umówmy się, przecież te podpisy się kupuje. Ma Pan jakieś wątpliwości? Żyjemy w czasach, w których na klatce schodowej nie może Pan wypisać listy lokatorów, bo RODO. Ludzie są przerażeni. Nie mogą podawać swoich imion i nazwisk, bo RODO. A jednocześnie wierzy Pan, że setki tysięcy na ulicy podają imię, nazwisko, PESEL, opowiadając się za jakimiś kompletnie przypadkowymi kandydatami (nie patrząc na to, czy ktoś sobie weźmie na te dane kredyt czy nie). Jak mówi młodzież – za randomowymi ludźmi?***

ZP: ***A z drugiej strony podają swoje dane całkowicie dobrowolnie.***

MW1: ***Jeżeli są to podawane dane. Wie Pan dobrze – musi Pan to wiedzieć – że przed rozpoczęciem kampanii najbardziej oblegani byli właściciele klinik dentystycznych i w ogóle prywatnych przychodni. Oni mają duże bazy danych, z PESEL-ami, z adresami.***

ZP: ***Rozumiem, tyle że w tej chwili rozmawiamy o popełnieniu przestępstwa. Powiedzmy sobie otwarcie. Bo tam potrzebne są jeszcze podpisy.***

MW2: ***Dokładnie rozmawiamy o popełnieniu przestępstwa.***

ZP: ***Dane to jedno, podpis to drugie, fałszerstwo to trzecie w tym przypadku.***

MW2: ***Dokładnie tak.***

MW1: ***Pan ma jakieś wątpliwości, czy to się nie dzieje? Tak serio teraz.***

Po ogłoszeniu wyników wyborów zwróciłam się do Inspektora Ochrony Danych Krajowego Biura Wyborczego (KBW) z pytaniem o możliwość sprawdzenia, czy moje dane osobowe pojawiły się na listach poparcia kandydatów na urząd Prezydenta RP. Okazało się, że „nie ma możliwości ustalenia, czy wśród doręczonych Państwowej Komisji Wyborczej wykazów podpisów poparcia znajdują się Pani dane osobowe. Przepisy prawa nie upoważniają Państwowej Komisji Wyborczej do prowadzenia elektronicznego zbioru danych osobowych wyborców, który ewentualnie pozwalałby na wyszukiwanie wnioskowanych przez Panią informacji. Ze względu na fakt, iż w formie papierowej dostarczono do Państwowej Komisji Wyborczej kilka milionów podpisów realizacja Pani wniosku jest technicznie niemożliwa".

Postanowiłam eskalować problem i złożyłam protest do Sądu Najwyższego. Przytoczyłam powyższe fakty i powołałam się na art. 304 § 2 Kodeksu wyborczego, zgodnie z którym Państwowa Komisja Wyborcza, sprawdzając prawidłowość zgłoszenia kandydata na Prezydenta Rzeczypospolitej, jest zobowiązana zweryfikować, czy faktycznie zgłoszenie kandydatury poparło podpisami co najmniej 100 000 obywateli. Poparło **świadomie i dobrowolnie**. Zaznaczyłam, że w przypadku nielegalnego wykorzystania moich danych przez któregokolwiek zarejestrowanego kandydata mogło dojść do popełnienia przestępstwa z art. 248 Kodeksu karnego, co mogło mieć wpływ na przebieg wyborów. Sąd Najwyższy w 3-osobowym składzie postanowił pozostawić protest bez dalszego biegu. W uzasadnieniu Sąd nie odniósł się do przedstawionych przeze mnie dokumentów KBW. Wręcz przeciwnie, stwierdził, że moje zarzuty „nie odnosiły się do żadnych konkretnych zdarzeń, w których brała udział osobiście czy których była świadkiem, a stanowiły one jedynie przytoczenie zarzutów pojawiających się w medialnej przestrzeni publicznej oraz osobistych przekonań". Dodał, że nie przedstawiłam dowodów na poparcie moich twierdzeń i nie wskazałam, jak podnoszone okoliczności miałyby wpływać na ogólny wynik wyborów.

Wysoki Sądzie! Pragnę zwrócić uwagę, że w 2024 r. pojawił się – entuzjastycznie zaopiniowany przez Sąd Najwyższy – poselski projekt ustawy o zmianie ustawy – Kodeks wyborczy (druk 556), dostępny na stronie https://www.sejm.gov.pl/Sejm10.nsf/druk.xsp?documentId=6A6336616938A5B-7C1258B620063E0B0.

Projekt zakłada powstanie portalu służącego do udostępniania formularza poparcia kandydatów lub list kandydatów drogą elektroniczną, obsługiwanego przez KBW. Zatem część podpisów z poparciem byłaby w wersji cyfrowej. Pozostają papierowe listy poparcia. Czy można je zdigitalizować? Przy obecnie dostępnych technologiach nie będzie to trudne. Wtedy IOD KBW nie będzie miał wymówki, by nie udzielać informacji na podstawie art. 15 RODO. KBW będzie wręcz mogło wysyłać powiadomienia w mObywatelu, że nasze dane pojawiły się na określonej liście poparcia, a my będziemy mogli od razu zareagować, jeżeli będzie to wbrew naszej woli.

Jest jednak poważne ryzyko dla naszej prywatności związane z tworzeniem bazy danych osób popierających poszczególnych kandydatów, przetwarzającej dane wrażliwe ujawniające preferencje polityczne i światopoglądowe obywateli. Każdą bazę danych można skopiować, każdą można zhakować. Dane wrażliwe mogą się dostać w niepowołane ręce i mogą zostać niecnie wykorzystane nawet po wielu latach. Kto wtedy pomoże obywatelowi? Prezes Urzędu Ochrony Danych Osobowych potrzebował **pięciu lat** na wydanie decyzji i nałożenie kary na firmę McDonald's Polska Sp. z o.o. za doprowadzenie do ujawnienia danych osobowych w publicznie dostępnym katalogu. W sądach powszechnych sprawy toczą się równie długo. Chyba będziemy musieli radzić sobie sami.

À propos przychodni lekarskich, w lipcu 2025 r. w „Gazecie Wyborczej" ukazał się artykuł o lekarzu, który odchodząc z pracy skopiował na prywatną skrzynkę dane ponad 11 tys. pacjentów placówki medycznej, w której dotychczas leczył (https://wyborcza.pl/7,75398,32112949,lekarz-wykradl-dane-ponad-11-tys-pacjentow-nadrzedna-wartosc.html). W tekście podano informację, że placówka zawiadomiła Urząd Ochrony Danych Osobowych o zdarzeniu, a Urząd tylko upomniał lekarza.

Krytycznie o mObywatelu

W numerze 2/2025 „Domeny" analizowałam sytuację po rezygnacji z budowy Centralnej Informacji Emerytalnej (CIE). Dzisiaj już wiadomo, co się stanie. ZUS wystąpił z inicjatywą budowy zbliżonej do CIE funkcjonalności w ramach swoich prac nad modernizacją Platformy Usług Elektronicznych. W związku z tym w ramach działań deregulacyjnych rządu 20 maja 2025 r. do Sejmu wpłynął rządowy projekt ustawy o uchyleniu ustawy o CIE. Po rozpatrzeniu przez komisje sejmowe i Senat ustawa została przekazana Prezydentowi do podpisu w dniu 6 sierpnia 2025 r. Jak wynika z ostatecznej wersji ustawy opublikowanej na stronie Sejmu RP (http://orka.sejm.gov.pl/opinie10.nsf/dok?OpenAgent&1307_u), wygrał pomysł stworzenia ZUS HUB-u i udostępniania ubezpieczonemu przez ZUS, przy użyciu aplikacji mObywatel, informacji o stanie jego konta ubezpieczonego, a także o jego wszystkich produktach emerytalnych.

Zadałam też pytanie: po co Ministrowi Cyfryzacji wiedza o naszych hipotetycznych emeryturach? Już ma listę wszystkich emerytów i rencistów i ich dane zawarte w mLegitymacji. Teraz ma gromadzić dane o ubezpieczeniach emerytalnych wszystkich pracujących Polaków. Wskazówek dotyczących sposobu przetwarzania danych poszukałam w ustawie i jej uzasadnieniu i znalazłam następujące zapisy:

- w ustawie: elementy informacji o stanie konta ZUS **może** udostępniać ubezpieczonemu, który w systemie teleinformatycznym Zakładu utworzył profil informacyjny, będącemu użytkownikiem aplikacji mObywatel;
- w ustawie: ZUS **może** udostępniać ubezpieczonemu, który w systemie teleinformatycznym Zakładu utworzył profil informacyjny, będącemu użytkownikiem aplikacji mObywatel, o stanie jego konta ubezpieczonego i środkach zgromadzonych w programach emerytalnych;
- w uzasadnieniu: zakłada się **przekierowanie z aplikacji mObywatel do aplikacji mZUS**;
- w uzasadnieniu: informacje o zaoszczędzonych środkach w nieobowiązkowych programach emerytalnych będą mogły być zamieszczane za pośrednictwem aplikacji mObywatel na dotychczasowych warunkach, tj. na podstawie **dobrowolnych porozumień** pomiędzy operatorami tych produktów emerytalnych a Ministrem Cyfryzacji.

Nasuwają się kolejne pytania i wątpliwości. Czy ZUS może czy musi udostępniać stan konta i środków? Czy tylko osób, które już są użytkownikami mObywatela czy wszystkich klientów ZUS-u? Czy przekierowanie oznacza, że system mObywatel będzie mógł buszować w bazach ZUS-u? Czy w mObywatelu pojawią się informacje o środkach w programach emerytalnych dopiero po zawarciu umowy Ministerstwa Cyfryzacji ze stosownymi podmiotami czy też Ministerstwo otrzyma je z ZUS-u, który otrzyma je od podmiotów zgodnie z ustawą?

Wraz z kolejnymi dokumentami i usługami mObywatel zamienia się w gigabazę danych o Polakach, idealnie nadającą się do profilowania nas z naruszeniem naszej **prywatności**. Pamiętajmy, że system mObywatel jest zasilany naszymi danymi niezależnie od tego, czy zainstalujemy aplikację na naszym smartfonie. Wystarczy kolejna ustawa i kolejne nasze dane są przekazywane bez naszej wiedzy i zgody.

> *Już dawno temu wielu ekspertów ostrzegało przed tworzeniem megasystemów i megabaz. Wystarczy jedna wielogodzinna awaria, by użytkownicy zaczęli tęsknić za plastikiem. Wystarczy jeden udany atak i wyciek, by miliony obywateli było zagrożonych najprzeróżniejszymi oszustwami. Czy wtedy pomoże nam Minister Cyfryzacji czy też znów będziemy musieli radzić sobie sami?*

Krytycznie o cyberbezpieczeństwie

11 sierpnia 2025 r. wicepremier i minister cyfryzacji Krzysztof Gawkowski oraz wicepremier i minister obrony narodowej Władysław Kosiniak-Kamysz ogłosili, że na budowanie cyberodporności w sferze cywilnej tylko na 2025 r. zaplano-

wano rekordowe wydatki przekraczające 3,1 mld zł. Środki te zostaną przeznaczone m.in. na wsparcie administracji publicznej, samorządów i kluczowych sektorów gospodarki. Zapowiedzieli także zaprezentowanie nowej Strategii Cyberbezpieczeństwa RP. Wszystko w odpowiedzi na rosnącą skalę ataków w sieci.

Zajrzałam do obowiązującej Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 i przejrzałam zapisy dotyczące celu szczegółowego 4.: „Budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa" i jego podpunktów; „Stworzenie warunków do bezpiecznego korzystania z cyberprzestrzeni przez obywateli" oraz „Rozwijanie świadomości społecznej w kierunku bezpiecznego korzystania z cyberprzestrzeni". Wzruszyły mnie zapowiedzi z 2019 r. obejmujące: kampanie społeczne skierowane do różnych grup docelowych, współpracę z organizacjami pozarządowymi, sektorem prywatnym i ośrodkami akademickimi, działania systemowe uwrażliwiające społeczeństwo na zagrożenia płynące z cyberprzestrzeni i działania edukacyjne w zakresie uprawnień osób, które padły ofiarą cyberataku i poniosły szkodę w wyniku naruszeń bezpieczeństwa w sieci. Niestety, kontrola „Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości" przeprowadzona przez Najwyższą Izbę Kontroli za okres 1.01.2019 – 31.12.2021. wykazała brak skutecznych działań zwiększających wiedzę obywateli (użytkowników Internetu) na temat przestępstw internetowych oraz sposobów zapobiegania takim zdarzeniom. Jednym z podstawowych wniosków było zatem wypracowanie i wdrożenie jednolitych założeń modelu edukowania oraz ostrzegania obywateli na temat zagrożeń cyberbezpieczeństwa, w tym **stworzenie jednego, rozpoznawalnego, oficjalnego, państwowego serwisu, zawierającego łatwo dostępne informacje na temat zagrożeń cyberbezpieczeństwa, trwających kampanii, a także zaleceń i dobrych praktyk z zakresu „cyberhigieny"**. Moje zestawienie badań przeprowadzonych przez różne podmioty przez ostatnie cztery lata dotyczące pozyskiwania wiedzy przez Polaków o zagrożeniach w sieci – omówione w numerze 3–4/2024 „Domeny" – potwierdziło, że Polacy nadal sami szukają w internecie wiedzy o cyberbezpieczeństwie bądź pytają rodzinę czy znajomych zamiast korzystać ze źródeł rządowych (NASK czy Ministerstwo Cyfryzacji).

Co zatem mamy? Mamy portal CYBER.GOV.PL, de facto https://www.gov.pl/web/baza-wiedzy/aktualnosci. Czy jest to portal, który mogę rekomendować na moich szkoleniach? Nie. Jako wzorzec pokazuję wszystkim brytyjski portal WWW.NCSC.GOV.UK z oddzielną sekcją dla sektora publicznego bogatą we wskazówki i podpowiedzi przedstawione w przystępny i zrozumiały sposób. Co znajdziemy na polskim portalu w zakładce „Dla samorządów"? Ostatni komunikat dotyczy webinaru „Cyberbezpieczny Samorząd" i jest datowany na 21.11.2023. Jeżeli samorządowcy szukają poradników, muszą pracowicie przewijać sekcję i uważnie wypatrywać w tytułach poszczególnych wpisów. Sekcja „Dla każdego – cyberhigiena" jest niewiele lepsza. Czy nowa strategia i zapowiadane miliardy złotych zmienią sytuację? Nie sądzę. Ministerstwo Cyfryzacji i NASK znają rekomendację NIK-u od 2022 r. I nie zrobili nic oprócz zarejestrowania wspomnianej domeny cyber.gov.pl w lipcu 2023 r. Może brakuje kompetencji?

Krytycznie o kompetencjach cyfrowych

Na koniec kilka słów o przetargu ogłoszonym przez Ministerstwo Cyfryzacji pod koniec lipca 2025 r. na przygotowanie ogólnopolskiej kampanii informacyjno-edukacyjnej poświęconej rozwojowi kompetencji cyfrowych. Jak zaznaczono w SWZ, „głównym celem kampanii jest zachęcenie różnych grup docelowych do rozwoju kompetencji cyfrowych we własnym zakresie – kampania ma budować potrzebę i chęć rozwoju kompetencji cyfrowych, bo to przynosi szereg korzyści i poprawia jakość życia. Kampania musi zatem wzmocnić sprawczość jej odbiorców". Odbiorcami kampanii mają być obywatele, specjaliści ICT, kobiety w ICT, przedsiębiorcy i osoby zarządzające. Nie wchodząc w szczegóły przetargu, polecam organizatorom skecz „Przedszkole" Kabaretu Młodych Panów i Marty Podobas, dostępny pod adresem https://www.youtube.com/watch?v=sLWJ07Ts1gI. Daje do myślenia.

Wszystkie informacje zawarte w artykule są podane według stanu na dzień 15 sierpnia 2025 r.
W opracowaniu analizy autorka nie korzystała z narzędzi AI.