Ministerstwo Cyfryzacji

# Notatka z trzeciego spotkania konsultacyjnego Strategii Cyfryzacji Państwa

## Temat: Bezpieczna sfera cyfrowa

**Data spotkania:** 3 grudnia 2024 roku

**Miejsce spotkania:** Ministerstwo Cyfryzacji, ul. Królewska 27 w Warszawie

**Dyrektor Ryszard Łuczyn** przywitał uczestników debaty i przekazał głos Ministrowi Dariuszowi Standerskiemu.

**Minister Dariusz Standerski** przywitał wszystkich uczestników na trzecim spotkaniu i zaprosił na 11 grudnia br. na spotkanie finałowe, kończące proces konsultacji społecznych Strategii Cyfryzacji Państwa. Podkreślił, że MC przeprowadza konsultacje, aby wszystkie tematy zostały omówione i zauważone, ponieważ publikując pierwszy projekt Strategii Cyfryzacji Państwa MC wyszło z założenia, że jest to dokument otwarty, który powinien być na bieżąco uzupełniany.

Po pierwszych turach konsultacji pojawiły konkretne wnioski, które będą przedstawione podczas spotkania 11 grudnia 2024. Minister wspomniał o jednym z wniosków z dotychczasowych konsultacji, że wskaźniki strategii powinny być bardziej szczegółowe, wskazywać także na „trajektorię" dojścia do wskaźnika ogólnego na rok 2035. MC dołączy także część dot. finansowania, a także odpowiedzialności poszczególnych ministerstw i urzędów centralnych za części danej strategii. To zostało odnotowane i będzie wdrażane w kolejnej wersji strategii.

Poprzednie spotkania dot. m.in kwestii gospodarczych, a dziś Minister chciał porozmawiać o kwestiach bezpieczeństwa szeroko rozumianego, w zakresie bezpiecznej sfery cyfrowej, przeciwdziałania dezinformacji, sytuacji dzieci i młodzieży w Internecie, w jaki sposób zabezpieczać nasze dane oraz bezpieczny rozwój dyskusji w Internecie w zakresie dostępu do treści, moderacji treści, jak walczyć z *fakenewsami*, jak tworzyć przestrzeń cyfrową, która jest bezpieczna i przyjazna dla wszystkich.

## I RUNDA

**<u>Wypowiedzi uczestników debaty:</u>**

**Piotr Kowalski, Polska Izba Informatyki i Telekomunikacji**

- Uczestnik przekazał zadowolenie, że wnioski z poprzednich debat, w kontekście struktury dokumentu, zostaną uwzględnione.
- Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 – obowiązuje do końca 2024 roku; warto byłoby w Strategii Cyfryzacji Państwa wziąć pod uwagę to, co będzie w nowej Strategii Cyberbezpieczeństwa od roku 2025.
- Bezpieczna sfera cyfrowa – bez większych uwag PIIT, co do tego, co na ten temat zostało wpisane do Strategii – przez PIIT popierane są zapisy zawarte w Strategii; przedstawiciel PIIT poprosił, aby w pracy nad poszczególnymi blokami prowadzony był dialog operacyjny przy wdrożeniu.
- Kwestia cyberbezpieczeństwa – koncepcja powołania centralnej instytucji dot. cyberbezpieczeństwa, w dyskusjach pojawiał się ten temat na przestrzeni lat. Obecnie struktura jest jasna – trzy CSIRTy krajowe, struktura jednak jest rozproszona. Pojawia się pytanie co do powołania nowej instytucji, sposobu jej powołania, jakim dokumentem?
- W zakresie odporności systemów informatycznych – brakuje w Strategii kwestii odporności na poziomie infrastruktury energetycznej i telekomunikacyjnej, które są podstawą do wszystkich działań cyfryzacyjnych.
- Diagnoza w zakresie cyberbezpieczeństwa – w analizie SWOT mocną stroną są kadry w sektorze prywatnym i publicznym – wg PIIT kadry to spory potencjał, ale wg nich nie jest to na razie mocna strona (raporty, opracowania w zakresie NIS2 – braki kadrowe w sferze publicznej i prywatnej są dużymi barierami) – diagnozę należy zweryfikować.
- Kompetencje w zakresie cyberbezpieczeństwa – ważny element.
- W Strategii Cyfryzacji Państwa zabrakło kwestii dot. obciążeń regulacyjnych w zakresie cyberbezpieczeństwa – z perspektywy firm tworzą one skomplikowany łańcuch współzależności i przez to firmy zaczynają więcej wydawać na dokumentację, na kwestie formalne, a nie na realne cyberbezpieczeństwo.
- Analiza SWOT – należy dodać do zagrożeń zasoby ludzkie.

**Tomasz Bukowski, Polska Izba Komunikacji Elektronicznej (PIKE)**

- Przedstawiciel PIKE wskazał, że obserwuje ostatnie działania ministerstwa w zakresie identyfikacji blokowania treści nielegalnych i niepożądanych – jako rynek są pozytywnie zaskoczeni działalnością MC – jest to odejście od idei wdrażania mechanizmów inwigilacji i kontroli treści, narzucanych na przedsiębiorców telekomunikacyjnych. To technicznie było bardzo trudne do wykonania, kosztowne oraz wątpliwie ze względu na kwestie moralne. Minister forsuje koncepcję odpowiedzialności dostawców treści, ew. dostawców usług hostingowych, co jest rozwiązaniem podobnym do tych obecnych w innych

krajach. Przedstawiciel PIKE zapewnił o chęci pomocy z ich strony i sektora w zakresie technicznym. Uczestnik wskazał, że w Sejmie czeka debata na temat hejtu w Internecie (projekty poselskie) – zapewnił o tym, że chcieliby jako organizacja stanowić pomoc dla Państwa.

- W kwestii jednego modelu blokowania treści – to nie powinien być jeden urząd, który procedowałby całość – PIKE rozumie to jako jeden urząd, który by tym procesem zarządzał (przykład Urzędu Ochrony Konkurencji i Konsumentów (UOKiK) – propozycja, aby domeny przez nich blokowane stanowiły część rejestru Ministerstwa Finansów (MF), natomiast nie doszło to do skutku – ustawa nie została w tym zakresie uchwalona – taki system byłby jednak tańszy i bezpieczniejszy). Przedstawione zostały dwa warianty – jeden urząd prowadzący, koordynujący rejestr (urzędy zgłaszają swoje listy, a przedsiębiorcy „podpinają się" do systemu i ściągają te dane); drugi wariant (powstały w konsultacji z Naukową i Akademicką Siecią Komputerową – Państwowym Instytutem Badawczym – dalej: NASK) – każdy urząd ma swój system, ale byłyby one połączone z jednym głównym systemem, który zbiera dane (uniknięcie problemu podwójnego blokowania). Systemy stosowane przez NASK, MF czy od niedawna Komisję Nadzoru Finansowego (KNF) będzie dużo bardziej dogodny technicznie – zarówno dla instytucji państwowych, jak i przedsiębiorców do realizacji.
- W Strategii Cyfryzacji Państwa wspomniany jest mechanizm dostawcy wysokiego ryzyka, który jest w projekcie ustawy nowelizującej krajowy system cyberbezpieczeństwa – na rynku telekomunikacyjnym budzi jednak poważne zaniepokojenie. Przyjęto mechanizm w bardzo szerokim zakresie jego stosowania, w stosunku do wszystkich możliwych systemów telekomunikacyjnych i teleinformatycznych z założeniem, że chodzi o sprzęt dwóch chińskich firm – tu widać dwa problemy. Po pierwsze – mechanizm wysokiego ryzyka będzie mocno niezależny od mechanizmu certyfikacji bezpieczeństwa (ten jest mechanizmem przejrzystym) – mechanizm wysokiego ryzyka budzi zaniepokojenie w kwestii odwołalności (np. w sprawie tempa usuwalności sprzętu proweniencji chińskiej). Dodatkowo będzie on dotyczyć wszystkich przedsiębiorców stosujących technologie cyfrowe, ale także instytucje publiczne. PIKE zwraca także uwagę na niekonsekwencję – mówi się dużo o zagrożeniu, które niesie sprzęt produkcji chińskiej, a z drugiej strony sieć Ogólnopolska Sieć Edukacyjna (OSE) funkcjonuje w oparciu głownie o taki sprzęt, co wynikało z założeń przetargowych na tę sieć. W efekcie za wiedzą NASK sieć OSE składa się z takich komponentów (tzn. firm chińskich), co więcej – NASK nie miał tutaj żadnych zastrzeżeń co do tego, że w OSE jest zbudowana na bazie sprzętu, wg NASK, niebezpiecznego. Drugi problem – polski mechanizm jest odwzorowaniem mechanizmu, który został zastosowany jedynie w jednym kraju – w USA. W 2019 roku USA uchwaliło ustawę o bezpieczeństwie w sieciach telekomunikacyjnych, w której zawarty był także postulat usunięcia sprzętu chińskiego. Polska zaimplementowała część obowiązkową z systemu amerykańskiego, nie zaimplementowano pozostałych regulacji amerykańskich – wsparcia instytucji z

budżetu z racji wycofania niebezpiecznego sprzętu oraz wparcie dla identyfikacji barier i przeszkód w szczególności w zakresie łańcucha dostaw. Federalna komisja komunikacji monitoruje na bieżąco postępy refinansowania usuwania sprzętu, jak i ew. blokad na zasobach kadrowych, a także na dostępności zamienników. Pytanie – czy MC zdaje sobie sprawę czym się skończyły amerykańskie doświadczenia? Program amerykański wycofania chińskiego sprzętu zakończył się porażką. Na wymianę sprzętu chińskiego i refinansowanie władze amerykańskie zakładały wydatek w postaci 1 miliarda dolarów, po roku (od 2019, czyli w 2020) kwotę tę podwojono, przy czym w toku postępowania, w raporcie Federalna Komisja Komunikacji stwierdziła, że tylko w pierwszej grupie podmiotów zakwalifikowanych do refinansowania (przedsiębiorcy telekomunikacyjni do 2 milionów użytkowników) potrzeby finansowe wynoszą ponad 5 miliardów dolarów. Uczestnik konkludując wypowiedź zapytał w jaki sposób ten sam proces może zakończyć się w Polsce, bez wsparcia finansowego.

**Jakub Orlik, Fundacja Internet. Czas działać!**

- Uwaga do wskaźnika – 80% urzędów będzie korzystać z AI – wskaźnik powinien zostać usunięty, bo korzystanie z technologii nie powinno być celem samym w sobie, celem powinno być to, że urzędy będą działać sprawnie. Dodatkowo, można ich sprawność ulepszyć innymi rozwiązaniami cyfrowymi, a także niecyfrowymi. Korzystanie z AI jest związane z zagrożeniami, m.in. *Prompt Injection*, modele językowe są obarczone uprzedzeniami, bo są uczone na danych, które są pełne uprzedzeń (przykład z generowaniem przez AI postaci na stanowisku zarządczym, częściej AI tworzy mężczyznę, niż kobietę). Biorąc pod uwagę brak transparentności przy działaniu modeli językowych, nie powinny brać udziału w procesach obywatelskich. Program komputerowy nie może być rozliczany.
- Pojawił się postulat przekazania środków na sprawnie działający Urząd Ochrony Danych Osobowych (zamiast na własne modele językowe).
- Zużycie energii w kontekście sztucznej inteligencji jest bardzo wysokie – technologia „mało zielona".
- Celem powinna być sprawność urzędów, a nie ich nowoczesność.
- Technologia *blockchain* – w Strategii została zdefiniowana jako ta, dzięki której można sprawdzić wiarygodność danych, prawdziwość danych, a tak nie jest – pozwala jedynie sprawdzić, czy dane były zmieniane. Niezmienność danych w *blockchain* łączy się z dodatkowymi konsekwencjami – jeżeli będzie włamanie i umieści treści nielegalne w *blockchainie*, to wtedy w publicznym *blockchainie* to się pojawi i nie będzie można tego usunąć. W miejscach, które są publicznie dostępne, utrzymywane przez Państwo, usuwalność powinna być. Są inne elementy kryptografii asymetrycznej, której można użyć w celu większej transparentności publikowanych informacji.
- Więcej spraw powinno być możliwe do załatwienia w sposób cyfrowy – powinno to wybrzmiewać mocno w Strategii Cyfryzacji Państwa (np. nadal wiele procesów można rozpocząć cyfrowo, ale należy kontynuować papierowo, np. zawiadomienie

o wykroczeniu). Kompleksowy przegląd procesów pomógłby zwiększyć bezpieczeństwo w tym zakresie.

- mObywatel – jest dostępny jednie dla klientów Google i Apple. Przy np. zablokowaniu konta Google użytkownikowi – nie mam możliwości użytkowania aplikacji. Uczestnik przytoczył także problem przysyłania smsów uwierzytelniających przez Google na numery telefonu obsługiwane przez operatora Orange – klienci nie mogli się logować. Konkluzja – aplikacja powinna być do pobrania ze strony www.gov.pl.
- Państwo jest uzależnione od prywatnych mediów społecznościowych – np. informacja dot. szczepień w trakcie pandemii COViD-19 publikowane były jedynie na prywatnej platformie Twittera (obecnie: X), nie było łatwego dostępu do tych danych na stronie www.gov.pl – to utrudnienie dostępu do informacji, ponieważ obecnie nie ma możliwości przeglądania informacji na tym portalu bez rejestracji w nim. Dla bezpieczeństwa informacji podmioty publiczne powinny informować na swojej stronie internetowej, a na mediach społecznościowych poprzez podawanie linków lub kopiowanie tych treści.
- *Public money – public code* – wszystkie aplikacje finansowane z publicznych pieniędzy powinny mieć publicznie dostępny kod. Byłoby to ułatwienie np. dla samorządów.

**Kinga Pawłowska-Nojszewska, Krajowa Izba Komunikacji Ethernetowej (KIKE)**

- Uczestniczka w pierwszej kolejności podziękowała za debatę i poważne podejście do słuchania, także przedsiębiorców – również w kontekście tematyki dot. ochrony małoletnich w Internecie – głos ten jest zauważony, także w toku prac nad założeniami do nowego projektu ustawy dot. ochrony małoletnich w Internecie. KIKE ocenia te prace pozytywnie – małoletnich należy w Internecie chronić, pytanie kto i w jakim zakresie powinien za to odpowiadać – dostawcy infrastruktury internetowej nie powinni dodatkowo filtrować treści.
- W Strategii Cyfryzacji Państwa jest mowa o głównych założeniach – analiza SWOT – propozycja KIKE, aby w silnych stronach (w zakresie cyberbezpieczeństwa, jak i infrastruktury) dodać polskich przedsiębiorców (30% Internetu przewodowego w Polsce to są polscy przedsiębiorcy). KIKE uważa, że polska infrastruktura, polscy przedsiębiorcy to wartość dodana dla państwa w zakresie cyberbezpieczeństwa.
- Kwestia dostawców wysokiego ryzyka – proporcjonalność, która wyraża się w tym, że z jednej strony dbamy o bezpieczeństwo, z drugiej dbamy o to, aby obowiązki nakładane na przedsiębiorców nie wykraczały ponad to, co jest konieczne, aby to bezpieczeństwo osiągnąć. Obecnie ta zasada w zakresie cyberbezpieczeństwa nie jest zachowana na żadnym etapie (MC unika rozmowy nt. ekonomicznych skutków w zakresie DWR – dostawców wysokiego ryzyka). W przesłankach dotyczących wydawania decyzji DWR nie ma miejsca, aby jakakolwiek analiza ekonomiczna została dokonana – nie to jest przesłanka wydania decyzji DWR, bierze się pod uwagę jedynie czynnik bezpieczeństwa, a nie czynnik ekonomiczny. KIKE pracuje obecnie nad konkretnymi propozycjami nad

zmianami do ustawy o KSC, które uwzględniałyby zasadę proporcjonalności (w tym wdrażanie *5G Toolbox* – to są jedynie niezbędne wykluczenia, które mogą dotyczyć np. redukcji ilości sprzętu w sieci, a nie całkowitej eliminacji dostawcy). Jedna decyzja DWR może oznaczać zaprzepaszczenie kilkunastoletniego dorobku w zakresie budowania konkurencji przedsiębiorców telekomunikacyjnych, także kliku projektów Centrum Projektów Polska Cyfrowa (CPPC) czy OSE. Ponownie padła kwestia przesłanek ekonomicznych DWR, a także kwestia dostawców sprzętu spoza UE i NATO.

**Rafał Rozwadowski, adwokat**

- Uczestnik zadał pytanie – czy MC w ramach zapowiedzi ujętych w dokumencie Strategii, będzie używać legislacji jako „oręża" w walce z *deepfake*, jako zagrożeniem technologicznym w różnych płaszczyznach (przykład regulacji z Hiszpanii czy Singapuru). Zjawisko *deepfake* przyjmuje rożną formę i oddziałuje na różne sfery życia (gospodarcze, prywatne). Definicja *deepfake* z AI Act jest bardzo nieprecyzyjna, nie chroni (ograniczona do funkcjonalności oznaczania, przedmiotowo i zakresowo nie zabezpiecza). Czy MC w ramach działań własnych lub międzyresortowych będzie starało się wypracować regulację, która będzie się kierunkowo odnosić do tego zagrożenia (np. bezpieczeństwo publiczne, kwestia wyborów i procesów demokratycznych, ochrony dzieci przed niewłaściwymi treściami)? Obecne przepisy na siłę mogą być stosowane do walki z *deepfake*, ale one nie są przeznaczone do tego celu. Czy MC zastanawia się także nad kwestią tzw. wirtualnego wizerunku, który mógłby być generowany przez różne technologie. AI Act w zakresie *deepfake* odnosi się jedynie do kwestii audio i wideo – pytanie czy treści tekstowe mogą być uznane za takie zagrożenie?
- Czy jeżeli MC rozważa to zagadnienie – czy jest zwolennikiem definicji neutralnej technologicznie?

**<u>Podsumowanie I rundy wypowiedzi:</u>**

**Minister Dariusz Standerski** podkreślił, że MC widzi korelację pomiędzy Strategią Cyfryzacji Państwa a Strategią Cyberbezpieczeństwa. Wkład do SCP w zakresie cyberbezpieczeństwa został opracowany na podstawie tworzonej Strategii Cyberbezpieczeństwa od 2025 roku – dokumenty mają być w ścisłej relacji, uzupełniać się. Kwestia Agencji Cyberbezpieczeństwa to bardzo ważny i ciekawy temat – to, co udało się dotychczas zrobić to np. utworzenie Centrum Operacji Cyberbezpieczeństwa, wzmocnienie roli Pełnomocnika Rządu ds. Cyberbezpieczeństwa. Widać przestrzeń, która powinna zostać uzupełniona, a która jest polem działalności takich instytucji, jak *National Cybersecurity Center* w Wielkiej Brytanii, czyli pole działalności dotyczące prewencji, szkolenia przedsiębiorców, publikowania regularnych informacji o zagrożeniach w cyberprzestrzeni. Dzisiaj te działania częściowo są wykonywane przez komunikaty Pełnomocnika Rządu ds. Cyberbezpieczeństwa, ale nie jest to systematyzowane. Podobnie jeśli chodzi o cyberodporność w zakresie kompetencji. MC widzi miejsce dla Agencji Cyberbezpieczeństwa, nie należy jednak zmian wprowadzać nagle i jednocześnie. W tej chwili mamy do czynienia z dużą liczbą zmian w tym zakresie – to nie jest kwestia tego roku. Co do braków kadrowych – przyjmujemy uwagę, jednak wskazaną „silną stronę" trzeba inaczej sformułować – nasze kadry są

doświadczone i kompetentne. W kwestii obciążeń regulacyjnych – MC chce podnieść tę kwestię na poziomie unijnym (dziś projekt regulacji w Polsce musi być szczegółowo określony na poziomie oceny skutków regulacji – kwoty są określone); w kontekście rozwiązań unijnych nie ma zawartych kosztów, jest ważne, aby to również na poziomie unijnym było rozwijane.

Minister podziękował także za uwagi doprecyzowujące w zakresie blokowania treści i zwrócił uwagę, że UOKiK w tym zakresie zmienił swoje stanowisko – po tym doprecyzowaniu MC jest zgodne co do kwestii uspójnienia systemowego tym obszarze.

Co do uwag odnoszących się do dostawców wysokiego ryzyka – jednym z celów prowadzenia konsultacji publicznych jest rozgraniczenie miejsca na dialog w zakresie wpływu na regulacje i proces legislacyjny oraz na dialog w zakresie strategicznym – Minister stwierdził, że uwagi z procesu legislacyjnego ustawy o zmianie ustawy o krajowym systemie bezpieczeństwa mogą być rozpatrywane na ścieżce legislacyjnej. Minister podziękował za uwagi dotyczące zastosowania sztucznej inteligencji w urzędach – wskazał, że obecnie w Ministerstwie Cyfryzacji testujemy takie rozwiązania, na podstawie modelu PLLuM. Ciekawym rozwiązaniem byłoby stosowanie AI w zakresie dekretacji dokumentów czy porządkowania dokumentów – jest to perspektywa na rozszerzenie systemu EZD RP. Analizie zostanie poddana sprawa ściągania aplikacji mObywatel z innych źródeł (pod kątem bezpieczeństwa, wydajności, itp.). MC będzie wskazywać rekomendacje ministerstwom, aby umieszczać informacje bezpośrednio na stronie internetowej resortu.

Bardzo ważnym tematem jest kwestia *deepfake* – Minister wskazał, że ma nadzieję szybkiego wdrażania w najbliższym czasie Aktu o usługach cyfrowych – to będzie punkt odniesienia do przyszłych interwencji legislacyjnych w tym zakresie. W opinii Pana Ministra sztuczna inteligencja w zakresie *deepfake* wpływa na poszczególne obszary prawa (np. prawo administracyjne), jednak w ograniczonym zakresie powinna wpływać na prawo cywilne i prawo karne – dziś zagrożenie *deepfake* analizujemy z zastosowaniem konkretnych przepisów prawa karnego, także z perspektywy naruszenia dóbr osobistych czy prawa autorskiego. Minister stwierdził, że unikałby konstruowania specjalnych przepisów dotyczących sztucznej inteligencji w tym zakresie – powinniśmy AI traktować w tym wypadku jak inne dotychczasowe technologie, tzn. podstawowe prawa człowieka pozostają takie same, podstawowe zasady prawa karnego i kategorie przestępstw pozostają bez zmian, różni się sposób dokonywania niektórych przestępstw, różni się sposób przekazywania treści, różni się także skala – powinniśmy dokonywać interwencji w tym zakresie. Dlatego ważny jest Akt o usługach cyfrowych – wdrożenie tego dokumentu zwielokrotni procesy dot. zgłaszania treści nielegalnych lub naruszających prawa autorskie. Równocześnie NASK prowadzi badania w zakresie *deepfake* – te badania będą w przyszłości publikowane.

## II RUNDA

**<u>Wypowiedzi uczestników debaty:</u>**

**Jakub Szymik, CEE Digital Democracy Watch**

- Wytyczne w zakresie AI dla administracji były opracowywane w MC w ramach Grupy Roboczej ds. AI.
- Uczestnik wskazał fragment Strategii Cyfryzacji Państwa dotyczący opisania problemu zarządzania dezinformacją i nadzorem nad dezinformacją – diagnoza jest poprawna – mówi o nieporządku i braku koordynacji; w Strategii nie ma jednak zbyt wiele na temat kwestii unijnej w tym zakresie (nadzór nad dezinformacją na poziomie unijnym funkcjonuje i będzie jeszcze się zwiększał).
- Fundacja apeluje o jak największą niezależność polityczną – aby instytucja nadzorująca sprawę dezinformacji nie wykorzystywała swoich kompetencji do innych celów.
- Szczególnie istotnym obszarem są wybory oraz kampania wyborcza, w zakresie wycofywania publikacji treści, które mogłyby być nielegalne, szkodliwe lub mogłyby być objęte protestem wyborczym, ale także zapewnienia, żeby platformy udostępniały miejsce do komunikacji politycznej i społecznej (propozycja zmian wyborczych do uszczelnienia zadań PKW w zakresie reklamy politycznej, zgodnie z unijną regulacją) – kierunek zaproponowany w Strategii oceniają pozytywnie. Jest wskazany termin, że organ koordynujący ds. dezinformacji powinien się pojawić w 2026 roku – czy już jest w tym zakresie jakiś pomysł?

**Paweł Terpiłowski, Demagog**

- W kontekście dezinformacji i zwalczania treści nielegalnych na mocy Aktu o usługach cyfrowych – to bardzo ważne w kontekście dezinformacji, ponieważ treści, które my uznajemy za dezinformację nie zawsze wchodzą w ten katalog treści nielegalnych, np. na gruncie naszego polskiego prawa: przykład kłamstwa oświęcimskiego, publiczne pochwalanie wojny napastniczej, nawoływanie do nienawiści z racji przynależności kulturowej – są treściami nielegalnymi, a negowanie zmian klimatycznych czy dezinformacja zdrowotna nie są uregulowane prawnie, także dezinformacja w obszarze 5G. Z tego tytułu może grozić niebezpieczeństwo infrastrukturze krytycznej (są przykłady także w Polsce, nakręcające zagrożenie i ataki na infrastrukturę 5G).
- Słuszna w Strategii jest diagnoza niedofinansowania NGOsów zajmujących się dezinformacją, jednak brak w dokumencie rozwiązania tego problemu (kwestia zaufanych podmiotów sygnalizujących – brak mechanizmu finansującego tego typu podmioty).
- Strategia Cyfryzacji Państwa mogłaby bardziej akcentować rolę NGOsów jako pośrednika pomiędzy stroną rządową a przedstawicielami tzw. *Big Techu*.
- Istnieje problem w stosunku do platform egzekwowanie obecnych regulacji w zakresie dezinformacji (zwalczanie fałszywych kont, *deepfake'ów*, zgłaszania *scamów*). Widać, że działania *Big Techu* w tym zakresie są niewystarczające.
- Ważna jest rola w edukacji medialnej w przeciwdziałaniu dezinformacji i budowaniu odporności społecznej – zostało to dostrzeżone w Strategii. Zauważono także rolę budowy kompetencji w zakresie przeciwdziałaniu cyberzagrożeniom, jeśli chodzi o biznes (duża ilość nieprawdziwych treści

odnoszących się do biznesu, *scamów*, nieprawdziwych ofert) – firmy muszą na to mocniej zwracać uwagę.
- W Strategii należy mocniej podkreślić temat mediów publicznych (w tym KRRiT jako krajowego regulatora) i działań w zakresie przeciwdziałaniu dezinformacji w sferze medialnej. Cel wskazania koordynatora ds. dezinformacji został wyznaczony na 2026 rok – wydaje się to być w opinii uczestnika czas dosyć odległy (w przyszłym roku są wybory prezydenckie i czeka Polskę spora kampania dezinformacji z zewnątrz, jak i z wewnątrz – taki koordynator jest potrzebny już teraz).
- Rola Polski w kształtowaniu regulacji na poziomie unijnym powinna być bardziej aktywna, teraz już widać, że Akt o usługach cyfrowych nie jest dokumentem wystarczającym w zakresie działań przeciwko dezinformacji (duże platformy w swojej działalności będą dążyć jedynie do minimalizacji kar).

**Blanka Wawrzyniak, Fundacja Instrat**

- Uczestniczka poruszyła kwestię bezpieczeństwa rynku pracy w obliczu zmian technologicznych.
- W debacie publicznej ostatnio pojawiły się głosy, że rząd planuje stworzyć katalog zawodów potencjalnie zagrożonych i specjalnie chronionych przed wpływem AI. Zamiast zamkniętego katalogu jednak bardziej zasadne wydaje się położenie nacisku na budowanie kultury uczenia się przez całe życie, w tym budowania odporności obywateli i ich zdolności do przekwalifikowania się oraz kształtowania kompetencji przyszłości w kontekście rynku pracy.
- Nie powinny to być wyłącznie kompetencje cyfrowe. W Strategii zabrakło szerszego uwzględnienia tzw. kompetencji miękkich, jak np. kompetencji krytycznego myślenia, aktywnego uczenia się, rozwiązywania problemów itp.
- Liczba specjalistek/ów w sektorze ICT powinna odpowiadać na zapotrzebowania polskiej gospodarki, co wynika również z założeń *Cyfrowej Dekady*. Tu też przydałoby się bardziej elastyczne podejście i rozwiązania, które faktycznie pozwolą odpowiedzieć na realne potrzeby bieżącej sytuacji na rynku pracy.
- Jako przykład można podać zawody lingwisty czy filozofa, które uznawane są zawody wymierające, podczas gdy w dobie rozwoju sztucznej inteligencji i dużych modeli językowych, widzimy, że zyskały one na znaczeniu. Biorąc pod uwagę dynamiczne zmiany na rynku pracy i długi horyzont czasowy Strategii, Fundacja Instrat sugeruje znalezienie bardziej elastycznych narzędzi i rozwiązań.
- Została zwrócona również uwaga na kwestię prawa do odłączenia się. Fundacja Instrat docenia, że ten element pojawił się w Strategii. Jednocześnie, ważne jest podkreślenie jego egzekwowania poprzez wdrożenie go do polskiego kodeksu pracy w połączeniu z działaniami edukacyjnymi, skierowanymi zarówno do pracodawców, jaki i pracowników. Te działania na rzecz respektowania „prawa do odłączenia się", powinny zastąpić kulturę ciągłej dostępności w pracy.

**Joanna Karczewska, ASKOT**

- Uczestniczka zgłosiła postulat spojrzenia na kwestię bezpiecznej przestrzeni cyfrowej z perspektywy “szarego obywatela”. Powinna zostać stworzona możliwość zgłaszania gdzieś swoich wątpliwości, uwag, naruszeń, problemów itp. Przy dalszej cyfryzacji, Strategia powinna też zostać uzupełniona o pojęcie “krzywdy” oraz system oceny wymiaru etycznego z możliwością zgłaszania nieprawidłowości do MC (np. w postaci specjalnej skrzynki zgłoszeń).
- Cyfryzacja jest obecnie wymuszana – przykład wymuszania zakładania kont w mediach społecznościowych i publikowania ważnych komunikatów politycznych na Twitterze (Platformie X).
- Poruszony został również problem dezinformacji, która może być różnie interpretowana – na przykładzie CERT, którego konto zostało zablokowane przez Facebooka. Instytucje publiczne powinny przede wszystkim utrzymywać dobrej jakości i zabezpieczone strony internetowe oraz rzetelnie publikować informacje w BIP. Potrzebne są przede wszystkim unowocześnienia i usprawnienia w dostępności treści oraz publikacji publicznych danych.
- W kontekście ochrony dzieci w przestrzeni cyfrowej – po wprowadzeniu „ustawy Kamilka” (nowelizacja Kodeksu rodzinnego i opiekuńczego, weszła w życie 15 lutego 2024 r.) wiele organizacji zaangażowało się w opracowywanie nowych pomysłów w zakresie ochrony dzieci, natomiast zapomniano o tym, że już wcześniej były opracowywane różne rozwiązania przez NGO-sy oraz odpowiedzialne instytucje.
- Istotna jest również komunikacja z urzędami - urzędy powinny mieć obowiązek udzielania konstruktywnej odpowiedzi na zapytania, uwagi i zgłoszenia obywateli.

**Dorota Głowacka, Fundacja Panoptykon**

- Kluczowe dla zapewnienia ochrony praw obywateli w sieci jest zbudowanie silnego nadzoru instytucjonalnego nad tą sferą oraz kwestia regulacji w kontekście funkcjonowania platform społecznościowych, w szczególności tych o globalnym zasięgu.
- Fundacja popiera trzy główne punkty wymienione w Strategii w tym obszarze:
    - wspieranie silnego wsparcia instytucjonalnego wokół regulacji, które mają zapewnić bezpieczeństwo i poszanowanie praw jednostek w sieci;
    - zapowiedź prowadzenia badań wpływu technologii na zdrowie psychiczne;
    - zapowiedź prowadzenia kampanii informacyjnych dotyczących ochrony praw obywateli w sieci.
- Ze strony uczestniczki padło pytanie czy wymienione punkty wiążą się z deklaracją powołania silnego i wyposażonego w odpowiednie zasoby Koordynatora ds. usług cyfrowych lub szerzej instytucji, która będzie miała odpowiednie kompetencje, także w zakresie rozpoznawania indywidualnych sporów dotyczących moderacji treści między platformami społecznościowymi a użytkownikami.
- Pytania odnosiły się również do bardziej szczegółowych planów MC w zakresie przeprowadzania kampanii edukacyjnych m.in. dotyczących praw obywateli zawartych w DSA (Digital Services Act, Akt o Usługach Cyfrowych) i czy badania

wokół problemu wpływu nowych technologii na zdrowie psychiczne, będą prowadzone także w sferze wpływu funkcjonowania platform społecznościowych.

**Podsumowanie II rundy wypowiedzi:**

W podsumowaniu II rundy, Pan Dyrektor Ryszard Łuczyn uporządkował główne wątki poruszane w dyskusji. Minister Dariusz Standerski, podziękował w szczególności za uwagi dotyczące organu koordynującego walkę z dezinformacją.

Minister wskazał na ważny punkt dotyczący kalendarza wyborczego – przepisy wyborcze są przestarzałe i należy je zmienić. Zwrócił też uwagę, że od sierpnia 2023 r. w Polsce trwa praktycznie nieustająca kampania wyborcza. Ze względu na to, że nie zmienia się reguł gry w czasie jej trwania, możliwość zmiany kodeksu wyborczego pojawi się dopiero po wyborach prezydenckich i po zakończeniu maratonu wyborczego.

W kontekście badań rynku pracy, będą rozwijane działania w tym zakresie. Z punktu widzenia Pana Ministra lista zawodów chronionych przed sztuczną inteligencją z definicji jest pusta. Trudno wskazać jakikolwiek zawód, który pośrednio lub bezpośrednio nie byłby pod wpływem rozwoju AI.

Każda zmiana technologiczna powinna być dobrze zarządzona. W rzeczywistości I i II rewolucja przemysłowa nie doprowadziły do tego, że mamy dzisiaj mniej pracy, tylko jest ona inna. Podobnie wykorzystanie narzędzi AI powinno doprowadzić do tego, żeby uświadomić sobie, że relacje w ramach pracy mogą ulegać zmianie i z doświadczenia historycznego wiemy, że ważne jest dostosowanie specjalistek/ów do realnych potrzeb.

Prawo do odłączenia się – planowane są kampanie edukacyjne, tak samo jak w zakresie wykorzystania algorytmów w miejscu pracy. W komisji sejmowej przygotowywany jest projekt w tym zakresie.

W kwestii prowadzenia komunikacji przez instytucje publiczne jedynie przez strony internetowe są różne racje, które trudno ocenić. Z jednej strony trzeba rozważyć preferencje użytkowników, z drugiej administracji publicznej.

W kontekście pojęcia “krzywdy” i obsługi rozpatrywania spraw, wiąże się to m.in. z opartą na usługach cyfrowych i uczestniczenia w tym procesie elementów automatyzacji. Z jednej strony wymagane jest zatrudnienie dużej liczby osób, które mogą obsłużyć różne procesy, z drugiej automatyzacja tych procesów, także w relacjach z obywatelami. Dyskusję na ten temat będzie trzeba podjąć ze względu na to, że zasoby ludzkie w administracji publicznej mogą okazać się niewystarczające, żeby zapewnić odpowiednią obsługę wszystkich procesów.

W kontekście zablokowania konta CERT na jednym z portali społecznościowych – jest ogromna potrzeba wdrożenia aktu o Aktu o Usługach Cyfrowych oraz wejścia w życie ustawy wdrażającej.

Minister Dariusz Standerski, zadeklarował, że jest zwolennikiem nadania jak najszerszych kompetencji dla koordynatora ds. usług cyfrowych. Na koniec zaznaczył, że istnieją już wystarczające regulacje z zakresu prawa cyfrowego i teraz trzeba skupić się na wdrażaniu.

Natomiast w perspektywie następnych 10 lat pojawią się kolejne regulacje cyfrowe i do tych regulacji trzeba być przygotowanym w zakresie struktur organizacyjnych.

## III RUNDA

**<u>Wypowiedzi uczestników debaty:</u>**

**Paweł Hebda, Student informatyki na SGGW**

- uczestnik na początku wypowiedzi poinformował, że prowadzi projekty badawcze oraz założył koło naukowe związane z poruszanymi zagadnieniami. Jest również jednym z organizatorów Sieci Debat Oksfordzkich.
- Uwagi dotyczyły głównie zagadnienia jak z korzyścią dla człowieka można zarządzać sferą cyfrową:
    - Automatyzacja i e-powiadomienia – z jednej strony chodzi o zwiększenie produktywności i ograniczenie zadań nudnych oraz monotonnych. Ważne jest jednak, żeby ludzie byli w stanie utrzymać odpowiednią higienę cyfrową i nauczyli się odpowiednio korzystać z narzędzi cyfrowych, tak żeby umieć przenieść różne procesy do cyfrowej rzeczywistości, podobnie jak to się stało w systemie EZD (tworzenie koszulek, zakładanie i przekazywanie spraw itp.).
    - Wprowadzanie narzędzi AI do urzędów – trzeba uważać, żeby nie uzależnić się od tych narzędzi i traktować je przede wszystkim jako narzędzia do przeszukiwania dużych zbiorów informacji oraz źródła inspiracji. Narzędzia AI można traktować jako ulepszoną wyszukiwarkę, która na złożone zagadnienia jest w stanie odpowiedzieć zrozumiałym językiem (przy zaznaczeniu, że wykorzystanie narzędzi AI wiąże się też z ryzykiem powielania dezinformacji). Najlepiej, gdyby te narzędzia były wykorzystywane do usprawnienia pracy administracji publicznej, a nie jako narzędzie kontroli.
    - Jako przykład dobrego pomysłu został przedstawiony europejski ID (osobisty cyfrowy portfel dla obywateli i mieszkańców UE), podobnie jak Klucz FIDO, który spełnia różne standardy zabezpieczeń i umożliwia bezpieczny dostęp do wielu miejsc.
    - Korzystanie z otwartych danych – zostało przedstawione przez uczestnika jako pozytywny aspekt automatyzacji.
    - Ponieważ sami twórcy nie wiedzą do końca jak działa sztuczna inteligencja, dlatego trzeba wziąć pod uwagę ciągły proces dostosowywania się i aktualizacji regulacji związanych z AI.

**Magdalena Miecielica, rodzic (osoba prywatna)**

- Uczestniczka zgłosiła potrzebę stworzenia mechanizmu/miejsca, gdzie można byłoby zgłaszać szkodliwe treści – obecnie nie ma takiego rozwiązania.

- Uczestniczka postulowała również ograniczenie dostępu do mediów społecznościowych dla dzieci i młodzieży (powinny być dostępne dopiero od 15 roku życia).
- Poruszony został również coraz większy problem z umiejętnością czytania, rozumienia i skupienia się na dłuższych tekstach ze względu na negatywne oddziaływanie korzystania z mediów społecznościowych na mózg człowieka, przypominający uzależnienie od różnych używek.
- Pod kątem usprawnienia procesów i komunikacji z obywatelami w administracji publicznej został zgłoszony postulat prowadzenia bezpośredniej komunikacji, kiedy jest to tylko możliwe – bezpośredni kontakt z człowiekiem może często bardziej usprawnić i przyspieszyć proces niż sztuczna inteligencja.

**Małgorzata Krajewska, Rada Telekomunikacji i Cyfryzacji Lewiatan**

- Uczestniczka poruszyła wątek bezpieczeństwa infrastruktury cyfrowej, w tym bezpieczeństwa fizycznego. Zwróciła szczególną uwagę na istotę utrzymywania sprawności, odporności i bezpieczeństwa infrastruktury teleinformatycznej oraz energetycznej. W kontekście ryzyka o charakterze militarnym, hybrydowym, a także zagrożeń związanych ze zmianami klimatycznymi, potrzebne są długoterminowe inwestycje w zdecentralizowaną infrastrukturę energetyczną i telekomunikacyjną i ten wątek powinien być w Strategii bardziej widoczny.
- Sugerowaną formą byłoby stworzenie specjalnego Funduszu Odporności i Bezpieczeństwa Infrastruktury Cyfrowej. Uczestniczka podkreślała również, że ze względu na powstanie urzędu pełnomocnika ds. insfrastruktury energetycznej ten wątek powinien być bardziej uwidaczniany.
- Został również poruszony wątek dezinformacyjny i teorii spiskowych związanych z 5G – przykład absurdalnych zarzutów, że 5G wywołało powódź, które doprowadziły do tego, że nowa infrastruktura jest często niszczona.
- Problem występuje w różnych krajach, nie tylko w Polsce, dlatego branża teleinformatyczna od dłuższego czasu pracuje nad programami edukacyjnymi związanymi z adopcją technologiczną w oparciu o naukę, jak również rozwiązaniami związanymi z bezpieczeństwem infrastrukturalnym.

**Tomasz Bukowski, Polska Izba Komunikacji Elektronicznej (ponownie)**

- Jako pierwszą poruszył kwestię konieczności nadrobienia zaległości w legislacji w zakresie cyberbezpieczeństwa – w Sejmie trwają dyskusje na temat regulacji związanych z mową nienawiści i dezinformacją, co prowadzi do ingerencji w kodeks prawa cywilnego.
- Wznowienie działalności Komisji Kodyfikacyjnej Prawa Cywilnego w Ministerstwie Sprawiedliwości – środowisko prawnicze wyraziło niezadowolenie ze zmian ad hoc w przepisach cywilnych bez konsultacji ze środowiskiem ekspertów. Są prowadzone prace nad fundamentalnymi zmianami również w kontekście przepisów dotyczących cyfryzacji – niestety nie ujawniono szczegółów, w związku z tym zostało zadane pytanie, czy Ministerstwo wie o tych pracach.

- Ze strony uczestnika padła uwaga dotycząca zainteresowania się działalnością Komisji Kodyfikacyjnych w Ministerstwie Sprawiedliwości oraz skorzystania ze wsparcia prawników oraz ekspertów telekomunikacyjnych, żeby ustalić co fizycznie i technicznie jest możliwe, a co nie.
- Dezinformacja w kontekście mediów społecznościowych – sugestia, żeby nie wycofywać się z działalności w mediach społecznościowych ze względu na powszechne korzystanie z tego środka przekazu i komunikacji przez ogromną część społeczeństwa. Jednocześnie, ponieważ przedsiębiorcy telekomunikacyjni i dostawcy usług internetowych nie są w stanie blokować poszczególnych treści oraz napotykane są różne trudności w porozumiewaniu się z *Big Techami*, być może trzeba rozważyć rozwiązania podobne do tych zastosowanych w Rumunii – zablokowanie niektórych platform w całości.

**Kinga Pawłowka-Najszewska, Krajowa Izba Komunikacji Ethernetowej (ponownie)**

- Przedstawicielka KIKE zwróciła uwagę na wskaźnik nr 10 opisany w Strategii jako "wdrożenie mechanizmu umożliwiającego wykluczanie dostawców wysokiego ryzyka". Według uczestniczki tak określony wskaźnik jest wyrazem nadregulacji, która występuje tylko w Polsce. Wskaźnik ten powinien brzmieć: "wdrożenie mechanizmu ograniczania wykorzystania dostawców wysokiego ryzyka w sieciach 5G".
- Sektor MŚP: w wątkach horyzontalnych, w analizie SWOT w silnych stronach Polski warto ująć sektor małych i średnich przedsiębiorstw (sektor MŚP) jako podmioty które są bardzo innowacyjne, odpowiedzialne w dużej mierze za dużą część PKB oraz zmotywowane do wykorzystania narzędzi AI.
- Postulat do uwzględnienia w Strategii w sposób horyzontalny, to proporcjonalność. W kontekście cyfryzacji trzeba wziąć koniecznie pod uwagę aspekt ekonomiczny i cyberbezpieczeństwa, w innym przypadku cały plan cyfryzacji można będzie pogrzebać. Nakładając obowiązki w jakiekolwiek dziedzinie należy mieć na uwadze proporcjonalność.

**Jakub Orlik, Fundacja Internet. Czas działać! (ponownie)**

- Uczestnik odniósł się do kwestii tego, że społeczeństwo nie korzysta z rządowych stron, których jest wiele i nie ma możliwości codziennego śledzenia wszystkich stron, w celu sprawdzenia czy pojawiły się nowe informacje. Ze stron rządowych systematycznie znika funkcjonalność RSS, która pomaga zbierać obywatelom różne strony w jedno miejsce i dostawać powiadomienia, kiedy nowe wiadomości się pojawią. Prywatne media społecznościowe wypełniły tę lukę i tam tę zdolność sprawdzają.
- Ze strony Fundacji Internet. Czas działać! przy zeszłorocznych konsultacjach zostało przesłane zalecenie, żeby wydać rozporządzenie, żeby wszystkie strony rządowe miały RSS, dzięki czemu osoby zainteresowane mogą subskrybować treści bez uczestnictwa prywatnych firm.

- Dodatkowo rządowe strony powinny pojawić się na Fediwersum (wspólna nazwa wielu połączonych ze sobą serwisów społecznościowych korzystających ze wspólnych protokołów / sfederowana sieć społecznościowa). Jest to alternatywne rozwiązanie, które pokazuje, że państwo może utrzymywać strony na własnej infrastrukturze, a media społecznościowe mogą działać bez algorytmów, bez cenzury i bez polegania na prywatnych firmach, co też może przyczynić się do walki z dezinformacją.

**Podsumowanie III rundy wypowiedzi:**

Minister Dariusz Standerski podziękował za wszystkie uwagi i podkreślił, że Ministerstwo już prowadzi szkolenia dla urzędników z zakresu wykorzystania sztucznej inteligencji w administracji publicznej. Zakres i liczba tych szkoleń będą sukcesywnie zwiększane, co jest niezbędne, żeby wprowadzić odpowiednie zmiany. W ramach Krajowego Planu Odbudowy w przyszłym roku odbędą się również dodatkowe działania szkoleniowe związane z usprawnieniem elektronicznego obiegu dokumentów i systemem EZD.

W odniesieniu do regulacji mediów społecznościowych, uwaga Ministerstwa jest skupiona nie tyle na ograniczaniu wieku użytkowników, co na jego weryfikacji. Samo pytanie o wiek nie rozwiązuje sprawy. We współpracy z instytucjami unijnymi są opracowywane rozwiązania w tym zakresie. Jednocześnie opracowywane są rozwiązania takie jak Europejski Portfel Cyfrowy, nad którym prace są już bardzo zaawansowane (na wzór mObywatela, tylko w obrębie całej UE) i jest to jeden z priorytetów.

Minister zaznaczył jednak, że proces cyfryzacji nie musi koniecznie oznaczać odzwierciedlania w świecie cyfrowym procesów z wykorzystaniem papieru, np. składania tego samego papierowego formularza tylko online w formie elektronicznej. Czasami takie działania są po prostu bezsensowne. Jako Ministerstwo mamy wiele cennych lekcji na temat tego, jak nie powinno cyfryzować się różnych administracyjnych procesów. Każda cyfryzacja powinna polegać na tym, żeby usprawnić proces oraz sprawić, że jest on krótszy. Podobnie jest z różnymi rejestrami państwowymi i to inaczej powinno wyglądać niż w wersji papierowej. Nad tym też trwają prace, w szczególności związane z portalem mObywatel.

Odnośnie komisji kodyfikacyjnych działających przy Ministrze Sprawiedliwości – to szczególne jednostki, a ich prace nie są częścią procesu legislacyjnego. Podobnie jak Ministerstwo Cyfryzacji ma swoją grupę GRAI, w Ministerstwie Sprawiedliwości działają komisje kodyfikacyjne. Nie jest natomiast prowadzony żaden rządowy proces legislacyjny, ani nie ma żadnego wniosku o wpis do Wykazu prac legislacyjnych i programowych Rady Ministrów w tym zakresie.

Jeżeli chodzi o uwagi dotyczące powiązania między dostawcami wysokiego ryzyka a Strategią – Minister przyznał rację osobie zgłaszającej uwagę i zapewnił, że wskaźniki zostaną przeanalizowane, również pod kątem tego, czy wymieniony wskaźnik powinien w ogóle się znaleźć. Ten wskaźnik jest zbyt szczegółowy i trudny do oceny.

Odnośnie małych i średnich przedsiębiorstw oraz kwestii Fediwersum - uwagi zostały odnotowane do rozważenia.