# PROTOKÓŁ z XXXI posiedzenia Rady do Spraw Cyfryzacji, które odbyło się 9 maja 2025 roku, o godzinie 12:00 w siedzibie Ministerstwa Cyfryzacji.

## Otwarcie Posiedzenia – p. Agnieszka Jankowska, Przewodnicząca Rady ds. Cyfryzacji.

Pani Przewodnicząca powitała członków Rady ds. Cyfryzacji oraz zaproszonych na posiedzenie gości.

## Stan prac i uwagi organizacji społecznych do projektu ustawy o ochronie małoletnich przed dostępem do treści szkodliwych w Internecie – Pani Dorota Głowacka, Specjalistka ds. rzecznictwa i litygacji w Fundacji Panoptykon.

Przedstawicielka Fundacji Panoptykon podzieliła się z Radą wątpliwościami w zakresie projektu ustawy o ochronie małoletnich przed dostępem do treści szkodliwych w internecie z perspektywy organizacji, która stara się bardziej kompleksowo patrzeć na problem ochrony praw cyfrowych w sieci i dla której jednym z priorytetów jest m.in. przeciwdziałanie negatywnym skutkom funkcjonowania największych platform internetowych. Główny mechanizm, który przewiduje ustawa dot. wprowadzenia obowiązku weryfikacji wieku dla usługodawców internetowych „oferujących dostęp do treści pornograficznych”. Podmioty, które zostaną zobowiązane do wprowadzenia tej weryfikacji, a tego nie zrobią będą narażone na sankcje w postaci m.in. zablokowania dostępu do ich witryny. Analizy wskazują, że nie ma takiego mechanizmu weryfikacji wieku, który nie generowałby pewnych wyzwań/zagrożeń z punktu widzenia prywatności czy danych osobowych, a jednocześnie był skuteczny. Ponadto, każda możliwość blokowania dostępu do stron internetowych zawsze generuje ryzyko nadmiarowej ingerencji w wolność słowa. Nie jest to także środek, który rozwiąże problem dostępu dzieci do szkodliwych treści w sieci. Rozwiązanie problemu wymaga kompleksowych działań przede wszystkim nakierowanych na wymuszanie wprowadzenia systemowych zmian w funkcjonowaniu niektórych usług internetowych przede wszystkim największych platform. Pani D. Głowacka jako wątpliwość wskazała brak jasno określonego kręgu usługodawców zobowiązanych do wprowadzenia mechanizmu weryfikacji wieku. W ocenie Fundacji krąg adresatów ww. obowiązku powinien zostać ograniczony do głównych kanałów dostępu dzieci do pornografii. Ewentualnie ograniczony powinien zostać zakres podmiotowy ustawy w taki sposób, aby wykluczyć z ww. kręgu tych usługodawców, którzy intencjonalnie, co do zasady, nie zamieszczają czy nie dopuszczają publikacji tego rodzaju treści oraz podejmują adekwatne działania mające na celu chronić małoletnich na wypadek, gdyby zostały one jednak rozpowszechnione za pośrednictwem ich serwisów przez osoby trzecie.

Kolejna uwaga to brak definicji w projekcie ustawy pojęcia „treści pornograficzne”, które wzbudza duże emocje oraz jest definiowane w bardzo różnorodny sposób zarówno w doktrynie prawa, ale także w społeczeństwie. Brak zdefiniowania w ustawie „treści pornograficznych” sprzyja ryzyku nadużywania tego pojęcia, które może prowadzić do

nieuzasadnionej ingerencji w prawa podstawowe. Fundacja dostrzega zatem, przeważające nad ryzykami, korzyści z wprowadzenia takiej definicji. Ewentualnie można również rozważyć wprowadzenie do ustawy wyłączeń precyzujących, że pojęcie to nie odnosi się do treści rozpowszechnianych w ramach działalności artystycznej, naukowej i edukacyjnej.

Obecna na posiedzeniu Pani Dyrektor Marzena Sawicka wskazała, że odbyła się długa wewnętrzna dyskusja czy definiować pojęcie pornografii – podjęto decyzję, aby nie definiować tego pojęcia, ponieważ nasz kraj byłby pierwszy, który we wszystkich gałęziach prawa próbuje definiować przedmiotowe pojęcie, a kodeks karny świetnie poradził sobie bez definicji. Wszystkie definicje, które funkcjonują zagranicą były w jakimś stopniu ułomne i umożliwiałyby ich wykorzystanie w złym kierunku. Zasięgnięto także opinii pracowników naukowych – karnistów w tym zakresie. Ponadto, każdy dostawca treści powinien przeprowadzić analizę ryzyka, by ocenić szansę pojawienia się treści pornograficznej. Pani Dyrektor poinformowała, że w maju br. będą przeprowadzane konsultacje/uzgodnienia projektu przedmiotowej ustawy.

Pani D. Głowacka przedstawiła drugi filar ustawy, tj. obowiązek „przeprowadzenia i udokumentowania analizy ryzyka związanego z umożliwieniem małoletniemu dostępu do treści szkodliwych" co 24 miesiące, który ma dot. wszystkich usługodawców internetowych poza usługodawcami oferującymi dostęp do treści pornograficznych. Wątpliwości to brak definicji „treści szkodliwych", niejasne korzyści wynikające z obowiązku przeprowadzenia analizy ryzyka w zaproponowanym kształcie oraz na ile rozwiązanie zawarte w ustawie o ochronie małoletnich powiela podobne i lepsze rozwiązania zawarte w DSA: m.in. obowiązek przeprowadzenia analizy ryzyka także pod kątem możliwych zagrożeń dla ochrony zdrowia publicznego i małoletnich dla największych platform i największych wyszukiwarek – to ryzyka, z którym wiąże się konieczność wprowadzenia środków mitygujących to ryzyko. Ta procedura poddawana jest niezależnemu audytowi, a ostatecznie kontroli Komisji Europejskiej. Ponadto, zgodnie z DSA, wszystkie platformy dostępne dla małoletnich mają obowiązek wprowadzić „odpowiednie i proporcjonalne środki, aby zapewnić wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich w ramach świadczonych przez siebie usług" (art. 28 ust. 1 DSA[1]), co wydaje się dalej idącym wymogiem, niż ten wynikający z aktualnego brzmienia art. 3 projektu ustawy o ochronie małoletnich, przewidującego sam obowiązek identyfikacji tego rodzaju ryzyk. Przede wszystkim jednak art. 28 ust. 1 DSA może być również podstawą działań Koordynatora Usług Cyfrowych podjętych w reakcji na stwierdzone nadużycia w tym obszarze. Uznano, że w praktyce art. 3 nie wniesie w zasadzie niczego nowego w odniesieniu do działalności podmiotów, będących głównym źródłem ekspozycji małoletnich na tzw. szkodliwe treści, natomiast nałoży dodatkowy obowiązek na bardzo szeroką grupę podmiotów, która w zdecydowanej większości tego rodzaju zagrożeń w ogóle nie generuje, przy jednocześnie niejasnych korzyściach, na które miałaby się

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych) (Dz.U.UE.L.2022.277.1).

przełożyć realizacja tego wymogu (ponieważ samo dokonanie oceny ryzyka nie zwiększa poziomu ochrony).

W dalszej części wypowiedzi Pani D. Głowacka wymieniła pozytywne aspekty omawianego projektu ustawy:

- wykluczenie metod biometrycznych;
- zakaz wykorzystania danych przetwarzanych na potrzeby weryfikacji wieku w innym celu, obowiązek konsultowania z PUODO wytycznych dotyczących mechanizmów weryfikacji wieku;
- obowiązek zawiadomienia PUODO w sytuacji, gdy Prezes UKE poweźmie wątpliwości co do zgodności danego mechanizmu weryfikacji wieku wykorzystywanego przez usługodawcę z zasadami ochrony danych;
- możliwość włączenia NASK w procedurę oceny zasadności kwalifikacji treści;
- standardy z zakresu sprawiedliwości proceduralnej w postępowaniu przed Prezesem UKE. Należałoby rozważyć możliwość wprowadzenia tzw. modelu hybrydowego, w którym odwołania od decyzji Prezesa UKE będą rozpatrywane przez sąd powszechny, a nie sąd administracyjny, który ma ograniczone możliwości merytorycznego badania takich spraw.

Pani Dyrektor Marzena Sawicka podziękowała za rekomendacje i za prace na etapie przygotowawczym projektu ustawy i wskazała, że wiele z rekomendacji zostanie uwzględnionych. Poinformowała, że definicja treści szkodliwych pojawi się w przedmiotowym projekcie ustawy. Przekazała także, że na forum UE rozstrzygnął się przetarg Komisji nakierowany na wyłonienie wykonawcy mechanizmu weryfikacji wieku.

W toku dyskusji zaproponowano, aby sugerowane rozwiązania zmierzały w kierunku rozwiązań systemowych, a także wprowadzenia dobrych praktyk dla wszystkich usługodawców i podstawy prawnej do działania resortów takich jak Ministerstwo Edukacji Narodowej czy Ministerstwo Zdrowia w zakresie zadań miękkich.

## Dostęp do Informacji Publicznej – wyzwania w kontekście cyberbezpieczeństwa – Pan Sławomir Wojciechowski, Członek Rady ds. Cyfryzacji.

Pan Sławomir Wojciechowski wskazał, że temat dot. głównie zagadnienia dostępu do informacji publicznej regulowanego przez ustawę o dostępie do informacji publicznej, ale także innych rozwiązań prawnych i działań oddolnych w przypadku np. samorządów - od dłuższego czasu jest to ustawa – Prawo zamówień publicznych. Wielość przepisów i działań podmiotów publicznych wymaga transparentności tych podmiotów, która odbywa się na podstawie zapytań w ramach dostępu do informacji publicznej, publikowania na BIP dokumentów/informacji, w social mediach, w mediach lokalnych czy jawność zamówień publicznych.

W kontekście gmin zakres przetwarzanych danych jest bardzo duży, a udostępnienie

informacji może generować zagrożenia dla bezpieczeństwa informacji i ujawnienie danych chronionych (nieumyślne ujawnienie danych osobowych, tajemnic przedsiębiorstw, informacji o infrastrukturze IT). Ryzykiem jest naruszenie przepisów RODO, odpowiedzialność karna, utrata zaufania społecznego. Przykład stanowi udostępnienie umowy z danymi dot. usług i systemów IT wykorzystywanych do zabezpieczeń sieci informatycznej.

Pan S. Wojciechowski wskazał, że w gminach często zdarza się sytuacja, że firmy handlowe (przy czym w ramach ustawy o dostępie do informacji publicznej nie ma możliwości zweryfikowania kto wnioskuje o te informacje) proszą o zanonimizowane skany umów na systemy informatyczne, poszczególne oprogramowania czy urządzenia stosowane w infrastrukturze urzędów, co może stanowić ryzyko dostępu do wiedzy o podatnościach danego oprogramowania i wykorzystania informacji w celu ataku.

Pan S. Wojciechowski zwrócił także uwagę na aspekt zagrożenia błędnej kwalifikacji informacji – pracownicy mogą uznać, że informacja jest publiczna, mimo że powinna podlegać wyłączeniu, co stanowi ryzyko ujawnienia danych strategicznych lub poufnych. Ponadto, uzyskane informacje mogą być wykorzystane do celów konkurencyjnych lub nieetycznych, co jest zagrożeniem dla interesu gminy i jej mieszkańców. Pan S. Wojciechowski wspomniał także o braku kontroli wersji i logów. Często, budowa infrastruktury czy inne oddolne działania włodarzy samorządowych, potencjalnie stwarzają takie zagrożenie wynikające z braku świadomości.

Członek Rady zauważył, że jednym z ograniczeń udostępniania wrażliwych informacji jest ochrona informacji niejawnych – zastrzeżonych przez każdy organ władzy publicznej, także administracji publicznej, jeżeli takie informacje mają istotne znaczenie dla bezpieczeństwa i porządku wykonywania tych zadań. Być może jest to pewne rozwiązanie, aby instytucje/organizacje, które mają z tym problem nauczyły się wprowadzać klauzulę zastrzeżone, wówczas w kontekście dostępu do informacji publicznej takie materiały nie mogą być udostępnione. Pan S. Wojciechowski zauważył, że te instrumenty można stosować, jednak nie są to łatwe rozwiązania, ponieważ wymagają posiadania odpowiedniej wiedzy i świadomości podmiotów. Normy Krajowych Ram Interoperacyjności wskazują od wielu lat, że chociażby wprowadzenie w podmiotach publicznych systemu zarządzania bezpieczeństwem informacji w pewien sposób podniesie poziom bezpieczeństwa. Pan S. Wojciechowski wskazując przykłady ujawniania informacji zwrócił uwagę, że bezpieczeństwo informacji to nie tylko zabezpieczenie sieciowe czy sprzętowe, lecz najistotniejsze jest budowanie świadomości przedstawicieli szeroko rozumianych podmiotów publicznych w zakresie ujawniania newralgicznych informacji, które mogą być gromadzone i niebezpiecznie wykorzystane.

W toku dyskusji uznano, że rozwiązaniem problemu jest stworzenie dobrych praktyk/standardów/zaleceń dla organów w obszarze udostępniania informacji publicznych i uświadomienia potencjalnych zagrożeń. Pani Przewodnicząca poinformowała, że być może Rada wskaże rekomendacje w przedmiotowym temacie pod kątem projektu Cyberbezpieczny Samorząd. Potrzebne są także zalecenia, które przy każdym postępowaniu z

zakresu zamówień publicznych w przedmiocie teleinformatyki powinny uwzględniać cyberbezpieczeństwo. Pani Przewodnicząca zaproponowała zwrócenie się do Departamentu Cyberbezpieczeństwa MC w celu zasięgnięcia informacji dot. rozwiązań i ewentualnych możliwych działań do podjęcia w omawianych kwestiach.

## Informacja w sprawie prac prowadzonych w Ministerstwie Finansów w kontekście cyberbezpieczeństwa – Pani Agnieszka Gryszczyńska, Członkini Rady ds. Cyfryzacji.

Podniesiono temat związany z cyberzagrożeniami, atakami ukierunkowanymi na monetyzację i działaniami jakie może w tym zakresie podjąć Rada - zarekomendowania lub wesparcia innych podmiotów. Pani A. Gryszczyńska zwróciła uwagę na gigantyczną liczbę oszustw inwestycyjnych. Wskazała schemat przestępczego działania - przekonywanie, że najlepszą inwestycją jest *Baltic Pipe* i wykorzystywanie wizerunku polityków oraz sztucznej inteligencji w akcjach reklamowo - promocyjnych. Osoby, które uwierzą w takie działania zadłużają się, by zainwestować licząc na duży zysk. Inny mechanizm działania sprawców to telefony podszywające się pod pracownika banku (podszywający się informuje o konieczności wypłacenia pieniędzy z powodu zagrożenia rachunku, a następnie wpłacenia środków na bezpieczny rachunek techniczny), policjanta czy prokuratora.

Pani A. Gryszczyńska omówiła proces odnalezienia sprawców przestępstwa. Najistotniejsze znaczenie ma czas oraz szybkość uzyskania niezbędnych informacji. Z uwagi na to, że oszustwa inwestycyjne są w bardzo mocnym zainteresowaniu również Komisji Nadzoru Finansowego, podejmowane są działania wraz z Ministerstwem Finansów dot. zmiany procedury prowadzenia tego typu postępowań w sposób skupiający się na tym, co jest blokerem takich postępowań. Być może pojawią się propozycje związane ze zmianą tajemnicy bankowej w kontekście dynamiki pozyskiwania danych na potrzeby postępowań. Uznano, że jest to istotny element zapewnienia instrumentów zwalczania cyberprzestępczości w tym zakresie. W związku z tym pojawiła się propozycja stworzenia przez Radę stanowiska dot. podjęcia działań mających na celu zapewnienie narzędzi zwalczania przestępczości nakierowanej na monetyzację.

## Zamknięcie posiedzenia.

## Uczestnicy posiedzenia:

### Członkowie Rady:

1. Izabela Albrycht
2. Katarzyna Chałubińska-Jentkiewicz
3. Andrzej Dulka
4. Agnieszka Gryszczyńska
5. Agnieszka Jankowska – Przewodnicząca
6. Jolanta Jaworska
7. Janusz Kosiński
8. Anna Beata Kwiatkowska
9. Krzysztof Silicki
10. Bianka Siwińska
11. Katarzyna Szymielewicz
12. Sławomir Wojciechowski
13. Małgorzata Zakrzewska

### Zaproszeni goście:

14. Dorota Głowacka, Specjalistka ds. rzecznictwa i litygacji w Fundacji Panoptykon
15. Marzena Sawicka, Dyrektor Departamentu Telekomunikacji w MC
16. Katarzyna Sienkiewicz, Specjalista w Departamencie Cyberbezpieczeństwa w MC

### Sekretariat Rady i pracownicy Ministerstwa Cyfryzacji:

17. Karolina Taczalska, Biuro Ministra w MC
18. Joanna Gójska, Biuro Ministra w MC