# PROTOKÓŁ z XIV posiedzenia Rady do Spraw Cyfryzacji, które odbyło się 4 października 2019 roku, o godzinie 11:00 w siedzibie Ministerstwa Cyfryzacji.

## Dyskusja wewnętrzna Rady na temat społecznych skutków technologii cyfrowych, prywatności i anonimowości w Internecie.

Na początku dyskusji przytoczono projekt zrealizowany przez Uniwersytet Stanforda, Uniwersytet w Erlangen i Instytut Maxa Plancka, w wyniku którego powstało rozwiązanie pozwalające ingerować w materiały wideo i zmieniać mimikę twarzy widocznych na ekranie postaci w czasie rzeczywistym. Dzięki temu możliwe było np. spreparowanie wystąpień Donalda Trumpa czy Władimira Putina. Pokazuje to, jak przy wykorzystaniu technologii możliwe jest oddziaływanie na zachowania społeczne, a ludzie nie zdają sobie sprawy z tego, że są manipulowani. Zauważono, że technologie używane są jako element projekcji siły, dlatego bardzo ważne jest budowanie świadomości zagrożeń związanych z technologiami uzależniającymi, takimi które wpływają na rozwój społeczny człowieka.

Podkreślono, że żyjemy w okresie bardzo szybkiego rozwoju technologii cyfrowych, w którym rzeczywistość zmienia się niemal co pół roku – za tym idą zmiany zachowania się, sposobów komunikowania itp. Społeczeństwo traci poczucie tego, co jest trwałe, co jest ważne. W toku dyskusji wskazane zostało, że destrukcja systemu wartości odnosi się raczej do pokoleń młodszych. Podkreślono, że sektor prywatny dobrze rozumie profil psychofizyczny tego pokolenia, dysponuje narzędziami, które dają możliwość wywierania wpływu i powodowania określonych zachowań. Sektor publiczny pozbawiony jest takich narzędzi – co widać choćby patrząc na szkołę i przepaść pomiędzy postrzeganiem świata przez nauczycieli i uczniów. Wskazano, że mówiąc o budowaniu jakiegoś systemu wartości (w wychowaniu) należy pamiętać, o że mamy do tego drogę, ale musimy ją realizować profesjonalnie, w takich warunkach, w jakich jest to dzisiaj możliwe. Podkreślone zostało, że być może Rada powinna się zająć nie tylko kwestią informatyzacji edukacji, ale i samego systemu edukacji.

Zwrócono uwagę, że od kilku lat z różnych źródeł wydawane są bardzo duże środki na rozmaite projekty edukacyjne – nauczycieli, rodziców, osób starszych, dzieci w zajęciach pozalekcyjnych – które dotyczą tego, w jaki sposób powinno się korzystać z narzędzi cyfrowych. Podkreślono, że osoby dorosłe same nie korzystają z możliwości dokształcania (co wynika z badań Eurostatu), dlatego dużo do zrobienia jest w przypadku rodziców i nauczycieli. Jeśli chodzi natomiast o dzieci wskazano, że w nowej podstawie programowej edukacji informatycznej są zapisy dotyczące kompetencji społecznych, przestrzegania prawa i bezpieczeństwa. W nowej podstawie programowej niebezpieczeństwo nowoczesnych technologii jest omawiane, także z uwzględnieniem prewencji .

Zauważono, że zjawiska takie jak profilowanie, targetowanie to w rzeczywistości inwigilacja, przy czym rzekomo istnieje prawo do anonimowości w Internecie. Powstaje pytanie, czy nie jest już pora na próbę regulacji tych zjawisk (coraz więcej krajów decyduje się na działania w tym obszarze) lub przynajmniej nadzoru , przez powołanie odpowiedniej instytucji. Wskazano, że obecnie mnożą się organizacje broniące anonimowości w Internecie, stało się to pewnym sloganem, który się wszędzie przewija i właściwie każde wspomnienie o regulacji

tego zjawiska jest odbierane jak naruszenie prawa konstytucyjnego (choć w Konstytucji, ani w żadnej ustawie, nie ma o tym słowa).

W toku dyskusji podkreślono, że obecnie przestrzenią informacyjną zarządzają algorytmy, które chronione są przez tajemnice handlowe. Przestrzeń informacyjna jest manipulowana (częściowo świadomie, częściowo poprzez ewolucję algorytmów) – potrzebna jest więc możliwość regulowania podmiotów, które prowadzą przepływy wymiany informacji. Jest to jednak trudne zadanie. Kontrola algorytmów wykorzystywanych przez globalne podmioty wydaje się tym trudniejsza, im bardziej ma się świadomość tego, że w Polsce nie ma regulacji dotyczącej choćby okresu przechowywania logów przez podmioty świadczące usługi drogą elektroniczną (kwestie te wynikają jedynie z regulaminów konkretnych podmiotów) – przez co walka z przestępcami zajmującymi się tworzeniem fałszywych sklepów internetowych czy publikacją mowy nienawiści oraz innych treści krzywdzących/*fakenews* jest utrudniona.

Poruszona została również kwestia prawa do prywatności i mediów społecznościowych. Zauważono, że obecnie swoje profile mają również dzieci, które tracą prywatność w bardzo wczesnym okresie. Co istotne ich zdjęcia pojawiają się w mediach społecznościowych, bo są również wrzucane przez rodziców niemal od pierwszych dni po narodzinach dziecka. Kwestia tego, w jaki sposób rodzice korzystają z mediów społecznościowych, naruszając prywatność swoich dzieci jest również istotna.

Postanowiono, że Rada będzie dążyła do przygotowania listy dostrzeganych problemów i proponowanych rozwiązań.

## Spotkanie z Panem Robertem Koślą, Dyrektorem Departamentu Cyberbezpieczeństwa MC oraz przedstawicielem NASK na temat certyfikacji cyberbezpieczeństwa systemów IT w administracji.

Wprowadzając do tematu Pan Paweł Kostkiewicz, Kierownik Ośrodka Standaryzacji i Certyfikacji w NASK podkreślił, że od połowy tego roku obowiązuje tzw. *Cybersecurity Act* (Akt o Cyberbezpieczeństwe). Dokument ten z jednej strony rozszerza mandat Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), a z drugiej strony wprowadza europejskie ramy certyfikacji cyberbezpieczeństwa – na mocy tego dokumentu ENISA będzie się zajmowała przygotowywaniem tzw. europejskich programów certyfikacji, wspólnych dla wszystkich krajów członkowskich.

Podkreślone zostało, że choć rozporządzenie *Cybersecurity Act* nie wymaga implementacji do polskiego prawa, to można spodziewać się pewnych zmian w polskich przepisach - w ustawie o krajowym systemie cyberbezpieczeństwa i ustawie o systemach oceny zgodności.

Wskazano również, że choć rozporządzenie tworzy europejskie ramy certyfikacji cyberbezpieczeństwa, to będą do niego potrzebne akty delegowane. Nad pierwszym takim aktem zawierającym pierwszy europejski program certyfikacji, pracę podjęła już Komisja Europejska - podczas spotkania Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa (ECCG) został oficjalnie zaprezentowany pierwszy kandydacki program, oparty o *Common Criteria,* zgłoszony przez grupę SOG-IS, a Komisja Europejska zleciła ENISIE dalsze prace w tym zakresie. Po przyjęciu i ogłoszeniu dokumentu przez Komisję Europejską powstanie pierwszy, działający, euro-

pejski program certyfikacji. Co istotne, w chwili powstania europejskiego programu certyfikacji wszystkie państwa, które opracowały własne programy certyfikacji oparte o *Common Criteria* będą musiały ten europejski program wykorzystywać.

Odnosząc się do sytuacji Polski wskazane zostało, że od niemal półtora roku trwają prace nad projektem budowy zdolności organizacyjnej do wydawania certyfikatów w Polsce. W projekcie, finansowanym przez Narodowe Centrum Badań i Rozwoju (NCBR), uczestniczą trzy jednostki naukowo-badawcze: Instytut Łączności – Państwowy Instytut Badawczy (IŁ – PIB), Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (NASK PIB) oraz Instytut Technik Innowacyjnych EMAG (ITI EMAG). Zgodnie z przyjętym założeniem w dwóch z nich powstaną laboratoria specjalistyczne (IŁ i EMAG), a trzecia buduje jednostkę certyfikującą (NASK). *Cybersecurity Act* zmienia jednak sytuację, gdyż rozporządzenie to wprowadza pojęcie „jednostka oceniająca zgodność" – która może zarówno prowadzić badania, jak i wydawać certyfikaty. Niemniej jednak polski projekt aktualnie zakłada, że jednostka certyfikująca będzie instytucjonalnie niezależna od laboratoriów. Wskazane zostało, że projekt zakończy się w lutym 2021r., jednak planowane jest, by laboratoria powstały do końca bieżącego roku, a w przyszłym roku prowadzone będą pierwsze, pilotażowe certyfikacje (przedmiot tych pilotażowych działań zostanie jeszcze określony).

Podkreślone zostało, że (niezależnie od budowania zdolności do przeprowadzania badań) bardzo istotne jest, że już obecnie możliwe jest rozpoznawanie wartości certyfikatu wydanego przez inny ośrodek certyfikujący – umiejętność prawidłowej interpretacji wyników badań, które zostały wykonane gdzie indziej, to kompetencja, która przekłada się na bezpieczeństwo.

Wskazano, że aktualne prace nad polskim systemem certyfikacji opartym o *Common Criteria* trwają równolegle do prac nad pierwszym europejskim programem certyfikacji, wynikającym z *Cybersecurity Act*. W pewnym momencie zajdzie więc konieczność harmonizacji tych dwóch ścieżek, niemniej jednak już teraz robione jest wszystko, by polskie procedury były jak najbardziej kompatybilne z tymi europejskimi.

Podkreślono, że w najbliższym czasie można się spodziewać, że do Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa (ECCG) zostaną skierowane kolejne propozycje do stania się programami oceny zgodności. Mogą być to programy certyfikacji obszarów związanych z usługami chmurowymi, IoT, 5G. Co jednak istotne, żeby program oceny zgodności (czyli program, który może kończyć się przyznaniem certyfikatu) w ogóle zaistniał, musi być przygotowany wg ściśle określonych reguł, wskazanych w *Cybersecurity Act* – zakres wymagań jest rozbudowany. Podkreślono również, że *Cybersecurity Act* kładzie nacisk na kompatybilność certyfikacji cyberbezpieczeństwa z systemami oceny zgodności stosowanymi w oparciu o normy zharmonizowane w innych obszarach – stąd istotna rola m.in. Polskiego Centrum Akredytacji.

W dyskusji pojawiło się zagadnienie certyfikacji infrastruktury krytycznej. Pan Robert Kośla, Dyrektor Departamentu Cyberbezpieczeństwa MC podkreślił, że *Cybersecurity Act* zakłada obowiązkową certyfikację komponentów, które będą wykorzystywane w infrastrukturze krytycznej i do świadczenia usług kluczowych w ciągu dwóch lat.

Poruszono kwestię kosztów certyfikowania wyrobów/rozwiązań – pojawiło się pytanie o zdolność polskich firm do tego, żeby ponosić koszty certyfikowania własnych produktów. Zastanawiano się, czy nie powinno powstać jakieś narzędzie wsparcia polskiego przemysłu w zakresie finansowania certyfikacji, by polskie produkty mogły być konkurencyjne i wykorzystywane w różnych zaawansowanych wdrożeniach. Podkreślono jednak również, że bardzo istotne jest promowanie polskich certyfikowanych rozwiązań na innych rynkach.

Na koniec dyskusji postanowiono, że na jednym z kolejnych posiedzeń Rada ponowi zaproszenie dla obecnych na tym spotkaniu Gości, by omówić temat bezpieczeństwa systemów teleinformatycznych administracji publicznej, gdyż jest to bardzo istotna tematyka i Rada będzie próbować przedstawić rekomendacje w tej sprawie.

## Wolne wnioski.

Członek Rady - organizator konferencji „Europejskie Forum Cyberbezpieczeństwa CYBERSEC" w Katowicach, zaprosił członków Rady do udziału w wydarzeniu.

Wiceprzewodniczący poprosił o ostatnie sugestie i uwagi dotyczące rekomendacji w zakresie finansowania projektów cyfryzacyjnych w kolejnej perspektywie budżetowej UE, by projekt stanowiska Rady w tej sprawie mógł zostać przedstawiony przy okazji kolejnego posiedzenia.

# Uczestnicy posiedzenia:

## Członkowie Rady:

1. Joanna Adamczyk
2. Izabela Albrycht
3. Jacek Czarnecki
4. Krzysztof Dyki
5. Krzysztof Głomb - Wiceprzewodniczący
6. Paweł Gora
7. Agnieszka Gryszczyńska
8. Michał Kanownik
9. Anna Beata Kwiatkowska
10. Tomasz Łukawski
11. Dariusz Milka
12. Józef Orzeł - Przewodniczący
13. Włodzimierz Schmidt
14. Sebastian Szymański

## Zaproszeni goście:

15. Robert Kośla, Dyrektor Departamentu Cyberbezpieczeństwa w MC
16. Paweł Kostkiewicz, Kierownik Ośrodka Standaryzacji i Certyfikacji w NASK

## Sekretariat Rady i pracownicy Ministerstwa Cyfryzacji:

17. Jacek Paziewski, Dyrektor Biura Analiz i Projektów Strategicznych w MC
18. Monika Skrzyńska, Zastępca Dyrektora Biura Ministra w MC
19. Katarzyna Stopińska MC
20. Justyna Grzegorek MC