

X kadencja



KANCELARIA SEJMU

Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

■ KOMISJI DO SPRAW DZIECI I MŁODZIEŻY (NR 47)

z dnia 17 grudnia 2025 r.

Pełny zapis przebiegu posiedzenia Komisji do Spraw Dzieci i Młodzieży (nr 47)

17 grudnia 2025 r.

Komisja do Spraw Dzieci i Młodzieży, obradująca pod przewodnictwem poseł **Moniki Rosy (KO)**, przewodniczącej Komisji, zrealizowała następujący porządek dzienny:

- rozpatrzenie projektu dezyderatu w sprawie zwiększenia ochrony wizerunku małoletnich w przestrzeni cyfrowej oraz kompleksowego uregulowania kwestii sharentingu, w tym zasad publikowania treści z udziałem małoletnich, ochrony ich danych osobowych oraz pracy małoletnich w internecie;
- rozpatrzenie informacji na temat technologii deepfake w kontekście bezpieczeństwa dzieci i młodzieży, ochrony wizerunku, danych osobowych.

W posiedzeniu udział wzięli: **Paulina Piechna-Więckiewicz** podsekretarz stanu w Ministerstwie Edukacji Narodowej wraz ze współpracownikami, **Magdalena Bochińska** naczelnik wydziału w Departamencie Spraw Rodzinnych i Nieletnich Ministerstwa Sprawiedliwości wraz ze współpracownikami, **Mirosław Wróblewski** prezes Urzędu Ochrony Danych Osobowych wraz ze współpracownikami, **Przemysław Kuna** prezes Urzędu Komunikacji Elektronicznej, **Maciej Siciarek** dyrektor Pionu CSIRT Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego wraz ze współpracownikami, **Katarzyna Hernadez** dyrektor Zespołu Edukacji Cyfrowej i Bezpieczeństwa w Sieci Biura Rzecznika Praw Dziecka, **Konrad Ciesiolkiewicz** zastępca przewodniczącej Państwowej Komisji do spraw przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15, **insp. Michał Pudło** zastępca komendanta Centralnego Biura Zwalczania Cyberprzestępczości, **Patryk Juhre** dyrektor Departamentu Multimediów Krajowej Rady Radiofonii i Telewizji wraz ze współpracownikami, **Katarzyna Staciwa** niezależna ekspertka Ars Expertise, **Zuzanna Jastrzębska-Krajewska** prezes zarządu Fundacji Wspomagania Rozwoju Dzieci Edyty Gruszczyk-Kolczyńskiej, **Danuta Wawrowska** przedstawicielka Zespołu ds. Kobiet przy Naczelnej Radzie Adwokackiej wraz ze współpracownikami, **Wojciech Mulik** dziennikarz portalu Goniec, **Piotr Aszkiełowicz** asystent przewodniczącej Komisji.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Grażyna Kućmierowska** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

Przewodnicząca poseł **Monika Rosa (KO)**:

Dzień dobry.

Szanowni państwo, otwieram posiedzenie Komisji do Spraw Dzieci i Młodzieży.

Witam wszystkich państwa posłów.

Stwierdzam kworum.

Dzisiaj w porządku posiedzenia mamy dwa punkty. Jeden to jest rozpatrzenie informacji na temat deepfake'ów, a drugi rozpatrzenie projektu dezyderatu.

Na początku z racji tego, że mamy kworum, pozwolę sobie zasugerować, aby najpierw rozpatrzyć kwestię dezyderatu, z prostej przyczyny – nie było wniesionych do niego uwag. Dezyderat dotyczy zwiększenia ochrony wizerunku małoletnich w przestrzeni cyfrowej oraz kompleksowego uregulowania kwestii sharentingu, w tym zasad publikowania treści z udziałem małoletnich, ochrony danych osobowych oraz prac małoletnich w internecie. Jest to dezyderat, który wynika z naszej poprzedniej Komisji. Jeśli nikt z państwa posłów nie zgłosi uwag w tym zakresie na tym etapie, to uznaję, że dezyderat w takiej treści, w jakiej został do państwa wysłany, zostaje przyjęty. A ponieważ – co mnie cieszy – uwag nie widzę, to uznaję, że dezyderat został przyjęty i zostanie przekazany do Rady Ministrów, a następnie ta odpowiedź będzie przez nas rozpatrzona.

Zamykając kwestię formalności, pozwolę sobie teraz otworzyć listę powitań. Ponieważ temat dzisiejszego posiedzenia wzbudził zainteresowanie bardzo wielu państwa, witam przede

wszystkim prezesa Urzędu Ochrony Danych Osobowych, pana Mirosława Wróblewskiego – dzień dobry, panie prezesie. Witam serdecznie przedstawicieli Ministerstwa Sprawiedliwości, którzy przedstawiają nam informację w imieniu pana ministra. Witam serdecznie przedstawicieli Ministerstwa Cyfryzacji, a konkretnie NASK – dzień dobry państwu. Witam przedstawicieli Urzędu Komunikacji Elektronicznej, Krajowej Rady Radiofonii i Telewizji, panią Katarzynę Hernandez z Biura Rzecznika Praw Dziecka oraz przedstawicieli organizacji pozarządowych, ekspertów i wszystkich państwa, którzy zgodzili się przyjąć zaproszenie do udziału w tym posiedzeniu.

Nie przedłużając – chciałabym państwu podziękować za to, że możemy się spotkać w tym temacie. Doskonale wiemy, że technologie się rozwijają, że kwestie deepfake'ów są kwestiami bardzo teraz rozbudzającymi wyobraźnię. Szczególnie w kontekście ostatnich wydarzeń, kiedy zdjęcie jednej z nastolatek w Polsce zostało przerobione i następnie nie zostały wyciągnięte z tego żadne konsekwencje. Zarówno Policja, jak i prokuratura odmówiły postępowania w tej sprawie, uznając, że żadne dobro nie zostało naruszone. W tym zakresie została skierowana skarga ze strony UODO, ale ja także pozwoliłam sobie wystąpić do prokuratury z prośbą o ponowne rozpatrzenie tej sprawy.

Wydaje się, że to otwiera nam pole do dyskusji o tym, czy obecnie obowiązujące regulacje są wystarczające, na jakich podstawach prawnych możemy się opierać, decydując w tych sprawach, ale także jakie zmiany wydawałyby się konieczne. Dlatego pozwolę sobie rozpocząć od zaproszenia pana prezesa Mirosława Wróblewskiego do zabrania głosu. Bardzo dziękuję, panie prezesie.

Prezes Urzędu Ochrony Danych Osobowych Mirosław Wróblewski:

Bardzo dziękuję.

Szanowna pani przewodnicząca, szanowni państwo, pozwólcie, że pokrótce przedstawię analizę i stanowisko prezesa Urzędu Ochrony Danych Osobowych w kontekście właśnie deepfake'ów i przekonania Urzędu Ochrony Danych Osobowych o potrzebnych regulacjach.

W mojej ocenie obowiązujące dzisiaj przepisy, zarówno w Polsce, jak i generalnie w Unii Europejskiej, nie są dostosowane do specyfiki technologii deepfake i treści generowanych przez sztuczną inteligencję. Nie zapewniają skutecznej ochrony prawnej. Oczywiście technologię można uznać za neutralną, ale łatwy do niej dostęp, skuteczność wykorzystywania jej do różnych celów, często niezgodnych z prawem i etyką, może właśnie prowadzić do naruszeń praw i wolności, m.in. kradzieży tożsamości, szantażu, nękania, ukazywania ludzi w sytuacjach, które faktycznie nie miały miejsca, oszustw, nawet manipulacji informacyjnej, manipulacji w ramach prowadzonych kampanii wyborczych, czy wręcz polaryzacji społecznej, a nawet zagrożenia dla bezpieczeństwa państwa. Dlatego też w moim przekonaniu niezbędne jest wprowadzenie przepisów prawa, które będą się bezpośrednio odnosić do rozpowszechniania szkodliwych treści w postaci deepfake'ów. Takie stanowisko przedstawiłem w wystąpieniu skierowanym w ostatnich miesiącach do ministra cyfryzacji, pana Krzysztofa Gawkowskiego, na które zresztą ostatnio otrzymałem odpowiedź.

Przywołam kilka spraw, m.in. to sprawa skargi dziennikarki dotycząca zamieszczenia na portalach społecznościowych fałszywych informacji o jej śmierci czy też pobiciu oraz o tym, że trafiła do więzienia. To także sprawa jednego z przedsiębiorców, który rzekomo reklamował produkty finansowe, które miały charakter oszukańczy. Znowu – jego wizerunek został wykorzystany niezgodnie z prawem.

W tej sprawie wydałem w ubiegłym roku dwa postanowienia przeciwko firmie Meta Platforms, ograniczając na maksymalny, trzymiesięczny, termin możliwości przetwarzania tych danych. Skargi na te postanowienia w obu przypadkach zostały oddalone przez wojewódzki sąd administracyjny. Później już Meta cofnęła swoje skargi w tej sprawie. Natomiast sprawę rozpatruje właściwy organ nadzorczy dla siedziby Mety, czyli irlandzka komisja. Także po tej sprawie podjęliśmy z Meta Platforms taką współpracę o charakterze systemowym, która, mając na względzie m.in. tę sytuację, a także inicjatywy podjęte przez inne skargi, wdrożyła narzędzie mające na celu ochronę wizerunku znanych osób i użytkowników mediów społecznościowych przed takimi oszustwami reklamowymi. Jest ono oparte na odrębnej bazie danych, opracowanej na podstawie profili znanych osób utworzonych na platformach społecznościowych Meta. Jeśli obraz w bazie danych jest wykrywany w zeskanowanej reklamie, inicjowana jest taka odpowiednia wewnętrzna procedura mająca na celu usunięcie tego materiału.

Czyli użytkownicy, którzy czują się pokrzywdzeni wykorzystaniem ich danych w reklamach typu celeb bait, mogą zgłaszać problem do Meta, klikając trzy kropki obok takiej pojawiającej się reklamy, wybierając tam instrukcję „Zgłoś reklamę”. Mogę powiedzieć, że takie praktyczne rozwiązania także wzmacniają ochronę i, jak widać, jesteśmy w stanie oddziaływać w tym zakresie także na wielkie platformy. Doceniam te działania, natomiast oczywiście potrzebne jest monitorowanie skuteczności, ponieważ dzisiaj nie jestem w stanie powiedzieć, jak wygląda skuteczność tego mechanizmu. Mam nadzieję, że poprawia on sytuację. Jesteśmy umówieni z przedstawicielami Mety na uzyskanie w najbliższym czasie takich informacji dotyczących skuteczności narzędzia. Oczywiście więc oprócz przepisów istnieje także duże pole. To jest przykład dla poprawienia praktyki w zakresie ochrony, ale na pewno to jest tylko i wyłącznie jeden przykład jednej platformy. A tych przypadków jest znacznie więcej.

Pani przewodnicząca wspomniała w sprawie tzw. deepnews, czyli zjawiska, które jest zresztą też rozpowszechnione w wielu innych krajach i stało się wręcz przyczyną kryzysów społecznych w Wielkiej Brytanii czy w Korei Południowej. Tutaj wniosek prezesa Urzędu Ochrony Danych Osobowych o ściganie w tej sprawie rzeczywiście nie był skuteczny.

Zwróciłem się do prokuratora generalnego, ministra Żurka, o zastosowanie odpowiednich środków wychowawczych oraz podjęcie i rozważenie właściwych kroków względem osób nieletnich, które doprowadziły do stworzenia i rozpowszechniania oraz zachęcania innych osób do rozpowszechniania tego wizerunku. Wiem, że pan minister zadeklarował poważne rozważenie tej kwestii, czekamy więc na dalsze działania. Natomiast mamy także dalsze sygnały, m.in. od lekarzy – już nie będę ich omawiać. Oczywiście państwo też zacie publicznie większą liczbę takich przypadków, bo to dotyczy w dużej mierze także polityków.

Zdecydowanie obowiązujące przepisy nie są wystarczające. Analizowaliśmy je. Oczywiście one w teorii mogą służyć na wielu płaszczyznach do takiej ochrony prawnej, to m.in. ochrona dóbr osobistych, w tym wizerunku i głosu, to także ochrona danych osobowych – przykład sprawy związanej z Metą. Ale ta ochrona mogła być zgodnie z przepisami rozporządzenia tylko czasowa. Dodam jeszcze tylko w tej sprawie, że odrębnie zostało wszczęte postępowanie cywilne. Tam sąd cywilny zgodnie z polskimi przepisami udzielił zabezpieczenia na dłuższy czas, na okres roku, bo na to pozwala Kodeks postępowania cywilnego. Natomiast przepisy prawa karnego potencjalnie mają także zastosowanie, to m.in. znamiona czynu zabronionego, kradzieży tożsamości – art. 190a § 2 Kodeksu karnego, zmuszanie do określonego zachowania – art. 191 Kodeksu karnego, rozpowszechnianie wizerunku nagiej osoby bez zgody – art. 191a, czy też w pewnych przypadkach publicznej prezentacji lub produkcji, rozpowszechniania, przechowywania i posiadania treści pornograficznych – art. 202, zniesławienia, zniewagi czy oszustwa. Natomiast rzeczywiście praktyka jest taka, że poza jednym przypadkiem wyroku sądu w Bydgoszczy nie są nam znane inne przypadki skutecznego wykorzystania tych przepisów. Oczywiście, na poziomie Unii Europejskiej także są rozwiązania, które mogą się częściowo przyczynić do walki z tego typu zjawiskami, na przykład zawarty w art. 50 ust. 4 aktu o sztucznej inteligencji wymóg oznaczania treści o charakterze deepfake jako sztucznie generowanej lub zmanipulowanej, czy też ustawa o świadczeniu usług drogą elektroniczną, aktualnie procedowana w procesie legislacyjnym, która wprowadza do polskiego porządku prawnego przepisy aktu o usługach cyfrowych. Nie będę tego wątku dłużej poruszał, ponieważ zakładam, że przedstawi to Ministerstwo Cyfryzacji.

W pełni się zgadzam, że jeżeli zostaną przyjęte i wejdą w życie te kierunkowe przepisy, to będą mogły dodatkowo służyć, na pewno mogą pomóc i będą stanowić istotny krok w celu wzmocnienia realnej ochrony prawnej. W moim przekonaniu nie będą to jednak rozwiązania wystarczające. Warto chociażby zwrócić uwagę na to, że państwa europejskie, które wdrożyły bądź też wdrażają przepisy DSA, przyjmują takie dodatkowe przepisy. Podam kilka przykładów. Dania, gdzie projekt zmiany prawa autorskiego ma zapewnić konkretne narzędzia do walki właśnie z deepfake’ami poprzez przyznanie prawa do żądania usunięcia deepfake’ów z platform online i dochodzenia odszkodowania za naruszenia w przypadku realistycznych, cyfrowo generowanych imitacji. Ponadto w maju tego roku parlament duński przyjął przepisy kodeksu karnego w zakresie zakazu deepfake’ów przedstawiających prawdziwe osoby w kontekstach seksualnych. Z kolei Senat Belgii przyjął rezolucję zawierającą stanowiska i rekomendacje skierowane do administracji federalnej i terenowej dotyczące deepfake’ów i rozważane są dalsze zmiany prawa. W Niderlandach co prawda nie przyjęto nowej legislacji, ale przepisy niderlandzkiego kodeksu

karnego mają precyzyjne zastosowanie. Natomiast we Francji te zmiany wprowadzono w zakresie dosyć szerokim, m.in. nowe szczegółowe przepisy to ustawa dotycząca wpływów handlowych i zwalczania nadużyć ze strony influencerów w mediach społecznościowych. Art. 5 tej ustawy nakłada na influencerów szczególny obowiązek ujawniania stosowania deepfake'ów. Jeżeli treść została stworzona przy użyciu sztucznej inteligencji, influencer musi zamieścić taką etykietę: wirtualne obrazy. Czyli osobne szczegółowe przepisy, mimo tego, że oczywiście akt o sztucznej inteligencji także będzie mieć zastosowanie. I również ustawa z 21 maja 2024 r., która w części nowelizowała francuski kodeks karny w zakresie mającym na celu zabezpieczenie przestrzeni cyfrowej przez ustanowienie przestępstwa polegającego na użyciu deepfake'ów, czyli wprost regulacja karna w tym zakresie. Na uwagę zasługuje także amerykańska regulacja odnosząca się do nadużyć związanych z deepfake'ami, o nazwie Take It Down Act, Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act, która zawiera definicję cyfrowego fałszerstwa, digital forgery. W tej regulacji dla platform internetowych przewidziano obowiązek usuwania takich deepfake'ów w ciągu 48 godzin od zgłoszenia przez ofiarę. Oczywiście można wskazać, że także w kontekście obowiązujących przepisów mamy do czynienia z rozwijającym się orzecznictwem sądowym. Warto wspomnieć o ostatnim wyroku Trybunału Sprawiedliwości UE z 2 grudnia w sprawie C-492/23, serwisu Russmedia, gdzie trybunał orzekł, że operator internetowej platformy handlowej jako administrator danych osobowych zawartych w ogłoszeniach publikowanych na jego stronie powinien wdrożyć odpowiednie środki techniczne i organizacyjne, aby przed opublikowaniem ogłoszenia można było sprawdzić, czy zawierają dane szczególnych kategorii, na przykład właśnie dane dotyczące zdrowia czy seksualności.

Dlatego też wydaje się, że istnieje taka potrzeba zainicjowania i poważnego rozważenia tych prac. Kwestia nie jest łatwa. Na pewno jest skomplikowana i dlatego zapewniam w przypadku takiej woli i decyzji o tworzeniu takich przepisów wsparcie merytoryczne Urzędu Ochrony Danych Osobowych. Ale możliwe są także takie rozwiązania, które należy rozważyć. W szczególności to zobowiązanie do instalowania systemów automatycznego i skutecznego wykrywania i znaczenia deepfake'ów, wspieranie także działań mających na celu wypracowanie dobrych praktyk w zakresie weryfikacji autentyczności treści, oznaczania fałszywych materiałów. To także wsparcie ofiar cyberprzestępstw opartych na deepfake'ach, na przykład przez stworzenie specjalnych programów pomocy psychologicznej. W Europie takie praktyki także mają już miejsce. Jak wspomniałem, także rozważenie szczegółowych zasad odpowiedzialności karnej i odszkodowawczej osób tworzących i rozpowszechniających szkodliwe deepfake'i. Osoby, których dane osobowe, w szczególności wizerunek, zostały wykorzystane w fałszywych materiałach, powinny mieć możliwość szybkiego i łatwego zgłaszania naruszeń, żądania natychmiastowego usunięcia treści z platform online i także uzyskania zadośćuczynienia za poniesione szkody. Wyroku w sprawie Russmedia nie będę już może bardziej szczegółowo omawiać, ale oczywiście zastosowanie już obecnych przepisów czy ich interpretacja budzi i będzie budzić wątpliwości, kontrowersje, interpretacje. Jednak wydaje mi się, że jeżeli dotychczasowa działalność organów państwa wskazuje na to, że obowiązujące obecnie i wprowadzane przepisy nie są wystarczające i drogą praktyki nie da się uzyskać skutecznej ochrony prawnej, to jednak istnieje pole do rozważenia przyjęcia dedykowanych przepisów.

Oczywiście niezależnie od tego ogromną rolę odgrywa edukacja. Na jednym z posiedzeń Komisji mówiłem o szerokiej działalności w tym zakresie Urzędu Ochrony Danych Osobowych. Te informacje przedstawiał także rzecznik praw dziecka. Na tym więc poprzestanę. Istnieje jednak oczywiście ogromna rola w tym zakresie do wykonania, bo problem dotyczy w dużej mierze ludzi młodych, którzy wykorzystują technologię trochę także w ramach swoistej przemocy rówieśniczej. Tu ogromnie doceniam także działania Ministerstwa Cyfryzacji, Ministerstwa Edukacji Narodowej, w szczególności w ramach programu nowego przedmiotu edukacji zdrowotnej, gdzie ten element edukacji cyfrowej jest niezwykle istotny – i bardzo za to dziękuję – i także przedmiotu edukacji obywatelskiej. Myślę, że tego nigdy nie brakuje. W wydarzeniach, które my realizujemy, uczestniczą także przedstawiciele Policji. Zawsze za to także bardzo serdecznie dziękuję, bo to się przyczynia, powiedziałbym, do prewencji, a prewencja chyba jest jeszcze bardziej ważna niż ściganie tego typu działań.

Niemniej jednak pozwoliłem sobie przedstawić takie stanowisko, ponieważ problem jest realny, dociera do urzędu, ale wynika także z monitorowania przez nas sytuacji w internecie

w tym zakresie. Na tym poprzestanę. Oczywiście jestem do państwa, do pani przewodniczącej dyspozycji.

Przewodnicząca poseł Monika Rosa (KO):

Bardzo dziękuję, panie prezesie.

Oczywiście otworzymy dyskusję po wysłuchaniu wszystkich informacji. Pan prezes mówił o edukacji i teraz pozwolę sobie jeszcze przywitać panią minister Piechnę-Więckiewicz – dzień dobry, pani minister – prezesa Urzędu Komunikacji Elektronicznej pana Przemysława Kunę oraz wiceprzewodniczącego państwowej komisji do spraw pedofilii pana Konrada Ciesiołkiewicza. Dzień dobry.

Pozwolę sobie teraz oddać głos przedstawicielom Ministerstwa Sprawiedliwości z prośbą o przedstawienie informacji i także odniesienie się do informacji pana prezesa Wróblewskiego, szczególnie w kontekście ewentualnych nowych uregulowań. Dla mnie szczególnie interesujące są kwestie dotyczące zakazu tworzenia zdjęć opartych o kontekst seksualny. Bardzo dziękuję. Bardzo proszę, oddają głos. Kto pierwszy z państwa będzie prezentował informację?

Główny specjalista w Departamencie Prawa Karnego Ministerstwa Sprawiedliwości Łukasz Rosiak:

Łukasz Rosiak, Ministerstwo Sprawiedliwości.

Szanowna pani przewodnicząca, szanowni państwo, w pierwszej kolejności pozwolę sobie może przedstawić zagadnienia prawnokarne związane z bardzo istotnym tematem i społecznie wymagającym wspólnej pracy nad uregulowaniem tego zagadnienia, tego problemu. W pierwszej kolejności chciałbym powiedzieć, że częściowo tego zagadnienia dotyczy chociażby Kodeks karny, na przykład art. 190a § 2. Generalnie jest to przestępstwo stalkingu, uporczywego nękania, ale art. 190a § 2 Kodeksu karnego dotyczy tak naprawdę kradzieży tożsamości, czyli można powiedzieć, że podszywania się pod kogoś. Oczywiście to podszywanie musi mieć określony cel. W tym przepisie czytamy chociażby, że karze od 6 miesięcy do lat 8 podlega osoba, która podszywa się pod inną osobę, wykorzystuje jej wizerunek, inne jej dane osobowe lub inne dane, za pomocą których ta osoba, za którą ktoś się podszywa, jest publicznie identyfikowana, i wyrządza jej szkodę majątkową lub osobistą. Oczywiście tutaj jest alternatywa łączna. Może być to szkoda majątkowa i osobista łącznie. Może być też tylko szkoda osobista, nie musi być koniecznie majątkowa. To przestępstwo jest obecnie zagrożone karą od 6 miesięcy do lat 8. Ale mamy jeszcze typ kwalifikowany tego przestępstwa, czyli § 3. Jeżeli następstwem tego czynu jest targnięcie się osoby pokrzywdzonej na własne życie, to wówczas mamy typ kwalifikowany tego przestępstwa, zagrożony karą już od lat 2 do lat 15. Może tak być w przypadku osoby małoletniej. Bez trudu można sobie wyobrazić, że na przykład jakieś dziecko, które zobaczyło swój przetworzony wizerunek, niestety wskutek emocji, stresu może się targnąć na własne życie. Czyli tutaj ustawodawca przewidział sytuację, w której ktoś jest karany za to, że wykorzystuje bezprawnie wizerunek innej osoby w celach właśnie osobistych albo majątkowych, i stworzył też typ kwalifikowany tego przestępstwa, polegający na wyższej już sankcji, gdy dana osoba niestety zdecyduje się targnąć na własne życie. Z tej strony jest już więc tutaj pewien karnoprawny kontekst.

Dalej mamy przepis Kodeksu karnego, który jest zawarty w art. 202, czyli kwestia pornografii. Chodzi konkretnie o art. 202 § 4b. Tutaj mamy taki przepis, że kto produkuje, rozpowszechnia, prezentuje, przechowuje lub posiada – czyli tutaj mamy dużo tych czynności sprawczych możliwych do zastosowania, nie muszą być oczywiście wszystkie, wystarczy jedna – treści pornograficzne przedstawiające wytworzony albo przetworzony wizerunek małoletniego, który uczestniczy w czynności seksualnej, podlega karze pozbawienia wolności do lat 3. Czyli tutaj też może się zdarzyć, że jakieś zdjęcie małoletniego zostanie przetworzone właśnie w takim kontekście seksualnym i wówczas również ustawodawca stworzył typ przestępstwa, właśnie art. 202 § 4b, który jest zagrożony sankcją karną pozbawienia wolności do lat 3. Tu także jest więc takie zahaczenie karnoprawne w niektórych stanach faktycznych, kiedy mamy do czynienia z przetworzeniem przestępstwa.

Możemy się też odnieść chociażby do takiego artykułu jak art. 287 Kodeksu karnego, czyli oszustwo komputerowe. Czyli kto w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody bez upoważnienia wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis

danych informatycznych, podlega karze pozbawienia wolności od 3 miesięcy do lat 5. Bo tutaj może być też tak, że ktoś przechowuje jakieś swoje zdjęcie, a to zdjęcie na przykład zostanie wykradzione albo zostanie w jakiś sposób zmodyfikowane. I tu też w ramach tego oszustwa komputerowego ustawodawca w określonych stanach faktycznych przewiduje sankcje od 3 miesięcy do lat 5.

Oczywiście pojawia się także kwestia ochrony danych osobowych, o której tutaj zostało wiele powiedziane. W ustawie o ochronie danych osobowych mamy przepisy, chociażby art. 107 ust. 1 i ust. 2, czyli właśnie wizerunek jest uznawany przez RODO za taką daną osobową, taką cechę, po której można kogoś po prostu jednoznacznie skojarzyć, zidentyfikować. I oczywiście w typie podstawowym nielegalne przetwarzanie danych jest zagrożone pozbawieniem wolności do lat 2, a w typie kwalifikowanym, jeżeli chodzi o ujawnienie, można powiedzieć, danych szczególnie wrażliwych, jest zagrożone karą pozbawienia wolności do lat 3. Tutaj też ustawodawca przewiduje takie uregulowania, nie tylko w Kodeksie karnym, nie tylko w ustawie karnej, ale także w innych ustawach, jak właśnie ustawa o ochronie danych osobowych. Jeśli więc chodzi o takie zagadnienia, które dotyczą kwestii przetwarzania wizerunku osoby małoletniej, to możemy jeszcze ewentualnie wymienić chociażby klasyczny art. 286 § 1 Kodeksu karnego, czyli oszustwo, wprowadzenie w błąd – to jest penalizacja każdego rodzaju oszustwa.

Możemy jeszcze ewentualnie zastanowić się nad innymi przepisami z zakresu takich przestępstw komputerowych jak przestępstwo utrudniania zapoznania się informacjami – art. 268 Kodeksu karnego, niszczenia danych informatycznych – art. 268a Kodeksu karnego, uszkodzenie danych informatycznych – art. 269 Kodeksu karnego. Oczywiście w grę wchodzi także w pewnych konfiguracjach stanów faktycznych kwestia przestępstw przeciwko wolności seksualnej i obyczajności. Bo może się zdarzyć, że ktoś przetworzy wizerunek osoby małoletniej na przykład w celu szantażowania tej osoby, mogą się więc tutaj też pojawić się różnego rodzaju zbiegi z innymi przestępstwami. Ale jeśli chodzi o kwestie samego przetwarzania danych osobowych, to tak jak wspomniałem, jest już art. 190a § 2 Kodeksu karnego, czyli kradzież tożsamości, która jest zagrożona sankcją w typie podstawowym i typie kwalifikowanym. Jest przede wszystkim też kwestia tego art. 202 § 4b, czyli tych treści pornograficznych przedstawiających wytworzony albo przetworzony wizerunek małoletniego. Czyli tutaj też ustawodawca w pewnym zakresie te kwestie reguluje. Bardzo dziękuję.

Przewodnicząca poseł Monika Rosa (KO):

Bardzo dziękuję.

Naczelnik wydziału w Departamencie Spraw Rodzinnych i Nieletnich Ministerstwa Sprawiedliwości Magdalena Bochińska:

Ja tylko gwoli uzupełnienia dodam, że dostrzegamy problem. Uważamy, że niewątpliwie istnieje taka potrzeba, żeby zwiększyć ochronę małoletnich w przestrzeni cyfrowej. Chcemy uwrażliwiać prokuratorów. Zwracamy również uwagę na edukację i na szkolenia. Co roku wnioskujemy do KSSiP o tematykę dotyczącą ochrony małoletnich, właśnie w tym w kontekście przestępstw cyfrowych.

Realizowany jest także krajowy program przeciwdziałania przestępczości seksualnej wobec małoletnich, który zawiera wiele aspektów dotyczących tego typu przestępczości. Na ukończeniu jest sprawozdanie z jego działania. Zobaczymy, przeanalizujemy, trwają prace analityczne. Ten krajowy program będzie przedłużany. Tak że tutaj w tym kontekście będziemy przyglądać się tej problematyce, ale dostrzegamy już problem. Dziękuję.

Przewodnicząca poseł Monika Rosa (KO):

Bardzo dziękuję za te informacje.

Pozwolę sobie też przywitać pana Michała Pudło, zastępcę komendanta Centralnego Biura Zwalczania Cyberprzestępczości – dzień dobry. Później, gdzieś w trakcie dyskusji, pozwolę sobie też zapytać pana o zdanie, jeśli pan pozwoli. W trakcie dyskusji wrócę również do Ministerstwa Sprawiedliwości z prośbą o wyjaśnienie, czy widzicie jednak państwo potrzebę stworzenia specjalnych uregulowań dotyczących właśnie deepfake'ów w kontekście tego, że być może trzeba po prostu zawrzeć jasno informacje. Nie opierać się tylko na regulacjach, które już obowiązują, ale jednak specjalnie przeznaczonych dla kwestii dotyczących sztucznej inteligencji i deepfake'ów właśnie.

Oddaję głos Ministerstwu Cyfryzacji, NASK. Bardzo proszę.

Dyrektor Pionu CSIRT Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego Maciej Siciarek:

Maciej Siciarek, dyrektor Pionu CSIRT w NASK.

Szanowna pani przewodnicząca, szanowne panie posłanki, panowie posłowie, szanowni państwo, zazwyczaj na tej Komisji występujemy jako NASK, realizując różne zadania z zakresu ochrony dzieci i młodzieży. Natomiast dzisiaj zostaliśmy poproszeni przez Ministerstwo Cyfryzacji, żeby grzecznościowo przedstawić krótko informacje i tezy zawarte w piśmie podpisanym przez ministra Standerskiego i przesłanym na ręce Komisji. Tak że przedstawię te punkty i potem, jeżeli będzie potrzeba wyjaśnienia, to oczywiście w miarę moich możliwości i kompetencji udzielię tych odpowiedzi, nie tylko jako reprezentant Ministerstwa Cyfryzacji w tej chwili, ale również jako NASK.

Droży państwo, w tym dokumencie przekazanym Komisji pierwszą taką ważną tezą są informacje z raportu wykonanego przez NASK, mianowicie „Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów i rodziców”. To badanie zostało wykonane w ramach programu Ogólnopolskiej Sieci Edukacyjnej – OSE i przedstawia kwestie deepfake’ów, wiedzy na ich temat i oddziaływania na dzieci. Najnowsza edycja raportu pierwszy raz opisuje zjawisko wykorzystania sztucznej inteligencji przez uczniów. Aż 70% uczniów zadeklarowało korzystanie z narzędzi AI, jednakże wyłącznie co trzeci wskazał, że zna i rozumie pojęcie deepfake’ów. Z tych nastolatków, które zetknęły się z deepfake’ami, aż 68% uważa je za zagrożenie, a niezależnie od znajomości tego terminu 67% ankietowanych przyznało, że zetknęło się z materiałami, które po zapoznaniu się z definicją zakwalifikowałoby jako deepfake. Nastolatki najczęściej zwracały uwagę na deepfake w postaci obrazu lub zdjęcia, czyli ten aspekt głosowy deepfake’ów pozbawionych obrazu był jakby mniej zauważalny z punktu widzenia tego badania. Jak wynika z badań NASK, wraz z wiekiem i kolejnymi etapami edukacyjnymi rośnie świadomość, precyzja kryteriów oceny wiarygodności informacji w internecie, czyli ten zmysł krytyczności sprawia, że w dzieci w starszym wieku łatwiej rozróżniają te kwestie.

W piśmie przesłanym przez Ministerstwo Cyfryzacji podkreślono również rolę NASK w zakresie prowadzenia w szkołach szkoleń dla dzieci i młodzieży, w tym związanych z deepfake’ami i dezinformacją, zwłaszcza w ramach tzw. cyklu Cyberprofilatyki NASK oraz uzupełnionego przez kursy dostępne w OSE IT Szkoła, oferujące materiały szkoleniowe dla dzieci i młodzieży. Wskazane jest również, że nieodzowna jest kontynuacja organizowania i promowania dedykowanych warsztatów i kursów edukacyjnych dotyczących tematu deepfake’ów niejako w takim trybie ciągłym jako zjawisko wymagające ciągłego tłumaczenia. Kursy dedykowane dla dzieci i ich opiekunów, rodziców, nauczycieli, ale także urzędników i funkcjonariuszy. NASK organizuje tego typu szkolenia również dla Policji i straży pożarnej jako organów państwa, które często są blisko społeczeństwa, zwłaszcza na terenach mniej zurbanizowanych. Wskazano również na konieczność kontynuowania tworzenia kampanii społecznych, które będą poruszały zakres tej materii.

W przedstawionym materiale ministerstwo porusza cały blok kwestii legislacyjnych, które są aktualnie realizowane, w tym ustawy o zmianie ustawy o świadczeniu usług drogą elektroniczną oraz niektórych innych ustaw, które służą wdrożeniu zapisów aktu o usługach cyfrowych. Przewiduje m.in. możliwość wydania przez odpowiednie organy nakazu podjęcia działań przeciwko nielegalnym treściom udostępnianym na platformach cyfrowych. Po drugie, projekt ustawy o systemach sztucznej inteligencji, którego celem jest powołanie w Polsce systemu sprawowania nadzoru nad systemami sztucznej inteligencji, możliwość egzekwowania obowiązków wynikających z wdrażania unijnego rozporządzenia o sztucznej inteligencji. Będzie to dodatkowe narzędzie walki z nadużyciami związanymi ze stosowaniem technologii deepfake.

Ministerstwo Cyfryzacji zwraca również uwagę na prace nad przygotowywanym w resorcie projektem ustawy o ochronie małoletnich przed dostępem do treści szkodliwych w internecie. Zapewne wszyscy wiedzą, że na obecnym etapie został on ograniczony do treści pornograficznych. Projekt w tej formie, po uwagach przekazanych w drugich konsultacjach społecznych, jest obecnie analizowany. W przekazanym materiale są te kwestie legislacyjne z odniesieniem również do tego, co jest w Kodeksie karnym i jakie korzyści możemy osiągnąć poprzez realizację tych ustaw. To jest szczegółowo opisane w piśmie przekazanym na ręce Komisji. Tak że tytułem streszczenia to ode mnie jest wszystko, ale oczywiście pozostają gotowy do odpowiedzi lub zapytania pytań i przekazania ich Ministerstwu Cyfryzacji. Dziękuję uprzejmie.

Przewodnicząca poseł Monika Rosa (KO):

Bardzo dziękuję. Takie pytania z pewnością zapiszemy i prześlemy.

A teraz pozwolę sobie otworzyć dyskusję. Jako pierwszy do zabrania głosu zgłosił się pan poseł Paweł Bliźniuk. Później prosiłabym o zabranie głosu przez Centralne Biuro Zwalczania Cyberprzestępczości, jeśli mogę. Z pewnością poproszę też przedstawicieli państwowej komisji i panią Katarzynę Staciwę. Czy ktoś z państwa jeszcze będzie chciał zabrać głos? Jak nie, to ja później zadam bardzo dużo pytań. Bardzo proszę, pan poseł.

Poseł Paweł Bliźniuk (KO) – spoza składu Komisji:

Dziękuję, pani przewodnicząca.

Cieszę się, że dzisiaj możemy rozmawiać o tak ważnych sprawach. Chciałem podziękować prezesowi UODO i państwu, którzy reprezentujecie urząd, za informacje. Mam jednak pytanie i w takim języku faktów chciałem postawić pewną kwestię, która jest bieżąca. Pracujemy nad DSA, czyli nad wdrożeniem aktu o usługach cyfrowych. Jutro mamy poprawki Senatu. Chciałem zasięgnąć państwa opinii na temat tych proponowanych zmian, które Senat wnosi w swoich poprawkach. Chodzi o ten rygor natychmiastowego wykonania decyzji urzędu dotyczący zablokowania treści, które są szkodliwe. Chyba pan z Ministerstwa Sprawiedliwości wymienił te przepisy karne, które dzisiaj chronią tak naprawdę po fakcie, bo mają wymiar prewencyjny – można wyciągnąć konsekwencje wobec osób, które łamią prawo.

Natomiast mamy rozwiązania, nad którymi pracujemy. Tam jest ten katalog przedmiotowy, jeżeli chodzi właśnie o Kodeks karny, są wymienione enumeratywnie przepisy Kodeksu karnego i one stanowią punkt wyjścia, jeśli chodzi o możliwość blokowania treści. Tymczasem mamy sytuację, w której jest propozycja ze strony Senatu, żeby w pewien sposób ograniczyć szybkie zastosowanie tych przepisów. Tutaj chodzi o wyczerpanie ścieżki odwoławczej od decyzji. Kiedy ktoś złoży skargę do sądu powszechnego, jest termin na złożenie skargi i do momentu, kiedy ten termin nie upłynie, nie można wykonać decyzji. W związku z czym, jeżeli mamy jakąś szkodliwą treść, w tym zastosowanie technologii deepfake, która narusza przepisy prawa karnego, to w myśl tych poprawek nie będzie można zareagować po zaistnieniu przesłanek. Nie będzie można zastosować rygoru natychmiastowego wykonania tej decyzji. W naszym projekcie ustawy, który wyszedł z Sejmu, były przesłanki konkretne. W związku z tym chciałem państwa zapytać o opinię z punktu widzenia ochrony dzieci i młodzieży również przed technologiami deepfake'owymi, czy te zaproponowane zmiany są właściwe. Państwo też wskazywali DSA jako ten akt prawny, który ma w pewnym stopniu chronić dzieci również w zakresie stosowania technologii deepfake, jeżeli chodzi o kwestie prawa karnego. Tam są jeszcze inne zmiany, ale nie chcę już ich poruszać, bo chodzi o pochwalanie pewnych czynów, ale zostaniemy już przy tym rygorze natychmiastowej wykonalności. To jest temat, który będziemy jutro procedować na Komisji, później w Sejmie będziemy głosować nad tymi poprawkami. Chciałem usłyszeć, jakie jest państwa zdanie na ten temat przez pryzmat ochrony praw dzieci i młodzieży, jeżeli chodzi właśnie o te propozycje, które przedłożył nam Senat. I tu państwa, panie posłanki i panów posłów, którzy przysłuchują się tej dyskusji, uczulam na tę kwestię, bo tej debacie na temat wdrożenia DSA w Polsce towarzyszy dużo fake newsów.

Natomiast dzisiaj mówimy o konkretnych i konkretnych sytuacjach, gdzie to zagrożenie dla dzieci i młodzieży w sieci jest dość wysokie. Te propozycje przedłożone przez Sejm, uchwalone w ramach ustawy miały chronić przynajmniej w jakimś zakresie dzieci i młodzież. A dzisiaj wydaje się, że te poprawki Senatu powodują, że te rozwiązania mogą być mniej skuteczne, niż były w pierwotnym założeniu.

Przewodnicząca poseł Monika Rosa (KO):

Bardzo dziękuję.

I teraz proszę pana Michała Pudło.

Zastępca komendanta Centralnego Biura Zwalczania Cyberprzestępczości insp. Michał Pudło:

Dzień dobry, inspektor Michał Pudło, zastępca komendanta Centralnego Biura Zwalczania Cyberprzestępczości.

Szanowni państwo, bardzo dziękuję, że mogę tutaj być i reprezentować nasze biuro. To, o czym chciałem powiedzieć, to chciałem zagwarantować, że bezpieczeństwo dzieci i młodzieży jest dla nas, w naszej działalności najwyższym priorytetem. W tym zakresie mógłbym je opisać

tak, że nasze zadania obejmują kilka profili. Oczywiście zwalczanie i zapobieganie przestępczości, które możemy nazwać ściganiem cyberprzestępców, a w tym przypadku przestępców, którzy łamią prawa dzieci i młodzieży, czyli prowadzenie postępowań przygotowawczych i pracy operacyjnej.

W naszym obszarze dotyczy to w największym zakresie przestępstw produkcji, wykorzystania i rozpowszechniania materiałów zawierających seksualne wykorzystywanie dzieci, czyli tzw. CSAM – ok. 20% postępowań prowadzonych przez nasze biuro to właśnie przestępczość tego typu. Zapewne są państwu znane nasze akcje skierowane grupowo wobec tych przestępców. Finalizujemy postępowania, które później kończą się wydaniem wyroków skazujących. Do tej pory w ramach takich siedmiu akcji przeprowadzonych przez nasze biuro zatrzymaliśmy 477 przestępców.

Natomiast oprócz ścigania przestępców stawiamy tutaj bardzo mocny akcent na profilaktykę i edukację, o czym wspominał już tutaj pan prezes. Przekłada się to na konkretne liczby. W samym tylko 2025 r. przeprowadziliśmy 1 tys. spotkań dedykowanych dzieciom i młodzieży, w których wzięło udział przeszło 100 tys. osób. Te spotkania dotyczą nie tylko cyberbezpieczeństwa, nie tylko zagrożeń w sieci, ale też właśnie ochrony wizerunku, trochę pouczania na temat tego, przed jaką odpowiedzialnością karną mogą stać dzieci. I widzimy tutaj duże zdziwienie. W niektórych przypadkach dzieci bardzo się dziwią, że przesłanie czyjegoś przerobionego zdjęcia może spowodować karalność. Nie ukrywam więc, że dla nas ta profilaktyka jest najważniejsza, bo lepiej zapobiegać, niż leczyć.

Działalność Centralnego Biura Zwalczania Cyberprzestępczości dotyczy także tzw. zagrożenia życia i zdrowia, czyli nasza komórka funkcjonująca przez całą dobę dzięki współpracy z Biurem Rzecznika Praw Dziecka, fundacjami typu Dajemy Dzieciom Siłę czy stowarzyszeniami i nie tylko w zakresie ustalania położenia dzieci, ale też osób pozostających w kryzysie psychicznym. W samym 2025 r. – do dziś – to jest przeszło 2000 czynności tego typu. I zdecydowana większość osób, do których docieramy, to są właśnie małoletni. Przyczyny pozostawania w kryzysie psychicznym są różne, nie tylko związane z zagrożeniami w sieci, ale oczywiście też z sytuacją rodzinną, głównie z sytuacją rodzinną czy rówieśniczą.

To, co chciałbym jeszcze przedstawić, to zaapelować o możliwość faktycznie porozmawiania na temat wprowadzenia do Kodeksu karnego kolejnych przepisów karnych, które mogłyby ściślej penalizować pewne stany faktyczne. Jesteśmy oczywiście świadomi tego, o czym mówił pan z Ministerstwa Sprawiedliwości, że te przepisy są, ale deepfake, bo to jest dzisiaj głównym tematem naszych rozmów, sam w sobie nie jest przestępstwem, tylko on przy dzisiejszym stanie prawnym musiałby być wykorzystany, tak jak pan mówił, w pewnym stanie faktycznym. Kradzież tożsamości to kradzież tożsamości. Deepfake, że ukradziono wizerunek dziecka czy komuś ukradziono tożsamość i podszyto się pod niego, trzeba bardzo konkretnie udowodnić. Ostatnio spotkałem się z ciekawym pomysłem wprowadzenia do Kodeksu karnego przestępstwa po prostu rozpowszechniania deepfake'ów przy wykorzystaniu AI. Kto produkuje, rozpowszechnia, prezentuje, przechowuje lub posiada obrazy, filmy lub głosy wytwarzane, przetwarzane lub zmieniane, w szczególności za pomocą systemu sztucznej inteligencji i mogące wprowadzić w błąd co do ich prawdziwości, przez co wyrządza szkodę majątkową lub osobistą, podlega karze pozbawienia wolności od roku do lat 5. To jest przepis przetłumaczony z kodeksu włoskiego, ale on faktycznie uderza konkretnie w deepfake, który wyrządzając oczywiście szkodę majątkową lub osobistą, sam w sobie byłby wtedy przestępstwem.

Współpracujemy z NASK, za co bardzo panu dyrektorowi dziękuję, bo oczywiście wykorzystujemy materiały edukacyjne w ramach tych spotkań, o których powiedziałem. Współpracujemy z Ministerstwem Edukacji Narodowej, żeby móc docierać do jak największej ilości dzieci i młodzieży, żeby wzmacniać ich bezpieczeństwo i o nie dbać. Jestem do państwa dyspozycji. Bardzo chętnie odpowiem na pytania. Jeszcze raz bardzo dziękuję za zaproszenie.

Przewodnicząca poseł Monika Rosa (KO):

Bardzo dziękuję.

Pani Katarzyna Staciwa. Bardzo proszę.

Niezależna ekspertka Ars Expertise Katarzyna Staciwa:

Pani przewodnicząca, szanowni państwo, bardzo dziękuję za możliwość zabrania głosu. Odniosę się do tego, co zostało powiedziane, z perspektywy mojej pracy polegającej na badaniu

zjawiska wykorzystywania seksualnego dzieci w cyberprzestrzeni. I chciałabym przede wszystkim powiedzieć o tym, że mamy do czynienia z dwiema sytuacjami. Z jednej strony są narzędzia w rękach dzieci. Narzędzia, dzięki którym każde zdjęcie może zostać rozebrane i zmodyfikowane w taki sposób, że będzie przedstawiało dowolną sytuację. Ale z drugiej strony mamy też te same narzędzia w rękach sprawców. Sprawców niejednokrotnie seksualnie zainteresowanych dziećmi. I tutaj jakby dorobek naukowy jest taki, że nie powinniśmy mieć żadnych wątpliwości co do tego, że są to narzędzia, które rzeczywiście błyskawicznie zostają zaadoptowane. Pokazała nam to też sytuacja, kiedy pojawiły się rozwiązania oparte na dark webie. To jest po prostu to, czego potrzeba sprawcom. Kiedyś potrzebowali anonimowej komunikacji, anonimowego porozumiewania się, wymienia treści. Dzisiaj, żeby zaspokoić swoje oczekiwania i fantazje, które niejednokrotnie stoją za kreowaniem dowolnych wizerunków, będą właśnie korzystać i korzystają z narzędzi opartych na wykorzystaniu sztucznej inteligencji. Nie powinniśmy więc mieć żadnych wątpliwości, że są to narzędzia, które służą po prostu zaspokajaniu także takich potrzeb.

I zanim przejdę do konkretnych postulatów czy konkretnych pytań, to jednak odniosę się do wcześniejszych wypowiedzi. Uzupełniłabym wypowiedź pana prezesa UODO, który w kontekście kryzysu społecznego był uprzejmy wskazać dwa państwa, o to, że to jest kryzys globalny, że tak naprawdę wszystkie państwa mają ten sam problem. Bo odpowiadając na pytanie, które dziecko nie jest zagrożone tym, że jego zdjęcie zostanie przerobione bądź wykorzystane w jakiś inny sposób – tylko to, którego wizerunek nie będzie dostępny dla danej osoby. Tak naprawdę więc każde dziecko, którego wizerunek znajdzie się w czyichś rękach, ryzykuje właśnie tym, że ten wizerunek będzie dowolnie przerobiony przy użyciu tych narzędzi.

Z kolei w wypowiedzi przedstawiciela Ministerstwa Sprawiedliwości wielokrotnie pojawiła się narracja polegająca na sformułowaniu „może pojawić się sytuacja”. Zmieniłabym tę narrację w taki sposób, że ta sytuacja się już pojawiła. I to jest też bardzo ważna rzecz, ponieważ mówią o tym dane. Tutaj Ministerstwo Cyfryzacji wskazało, że ponad połowa badanych nastolatków wskazywała na kontakt z deepfake’ami obrazu bądź zdjęcia, ale jest jeszcze jedna ważna informacja w tych badaniach. Mianowicie taka, że jedna trzecia tych nastolatków wskazywała na zastosowanie deepfake’ów czy zastosowanie tych narzędzi w tworzeniu treści pornograficznych. Jest to więc kolejny dowód na to, że dzieci o tym wiedzą. Wiedzą nie tylko o deepfake’ach, ale też o konkretnym celu, jakim jest tworzenie treści pornograficznych bądź materiałów przedstawiających seksualne wykorzystywanie dzieci.

I teraz dane. Tylko z taką refleksją poprosiłabym – czy potrzebujemy więcej cyfr, wyższych cyfr, czy nie powinno nam wystarczyć to, że mamy problem? Dane podmiotu, który reprezentuje amerykańską infolinię NCMEC, to wzrost o ponad 1325% liczby zgłoszeń dotyczących materiałów CSAM związanych z AI między rokiem 2023 a 2024. Natomiast za bieżący rok, do czerwca, te dane pokazują ponad 440 tys. nowych zgłoszeń w porównaniu do tego samego okresu za 2024 r. Tam było 6000 takich zgłoszeń. Jest to więc kolejny przykład na to, ile tego jest. Tylko moje pytanie jest takie, czy jak będziemy mieli za chwilę milion, dwa miliony, to będzie to też coś znaczyło, czy nie powinniśmy się raczej cofnąć do tych pierwszych wskaźników, które mówią o tym, że mamy problem.

Dane brytyjskiej infolinii. Na jednym forum w ciągu zaledwie miesiąca udostępniono ponad 3,5 tys. cyfrowo zmodyfikowanych lub syntetycznych obrazów lub nagrań wideo przedstawiających dzieci w wyraźnie seksualnym kontekście. I ostatnia liczba, która też może państwu dać zamyślenia. Dużo mówimy o zjawisku szantażu na tle seksualnym i organizacja Thorn mówi wyraźnie, ok. 10% zgłoszeń dotyczących finansowego szantażu seksualnego jest związanych z materiałami, które nie są autentyczne. Czyli to pokazuje, że jak najbardziej przerobione, podrobione treści są wykorzystywane do tego, żeby szantażować dzieci.

I teraz refleksja powinna być taka, że rozmawiamy o działaniach reaktywnych. Bardzo dużo tutaj się słyszy o tym, że blokować, reagować, ale na to, co już powstało, co się zadziało. Oczywiście też w tym kontekście możemy patrzeć na wynik prac legislacyjnych nad projektem ustawy o systemach sztucznej inteligencji. Na wyniki tej pracy trzeba będzie poczekać, więc pytanie, które powinniśmy sobie teraz zadać, to: co jeszcze można zrobić teraz, zamiast czekać albo zamiast reagować? Przede wszystkim trzeba wiedzieć. Odpytujemy nastolatki w badaniach, pytamy o ich doświadczenia, o wiedzę na temat deepfake’ów. Świetnie, ale dlaczego nie zwracamy uwagi na sektor prywatny? Które serwisy są najpopularniejsze wśród użytkowników z Polski? Które modele są wykorzystywane i na których platformach są hostowane? I najważniejsze

pytanie: czy polskie przepisy dotyczące bezpieczeństwa online pozwalają na wystosowanie ostrzeżenia do konkretnej firmy? Czy może to spowodować zablokowanie jej usług w Polsce i ewentualnie jakie kary finansowe wchodzi w grę? Czy rozważamy w ogóle takie podejście do problemu?

Ostatnio bardzo dużo uwagi jest skierowanej na Australię i nie z uwagi na to, że wszyscy lubimy jej klimat bądź lubimy kangury, ale to państwo pokazuje nam, wytycza nowe ścieżki. I właśnie australijski urząd eSafety podjął działania przeciwko firmie z Wielkiej Brytanii, która oferowała trzy popularne usługi typu nudify. I doprowadzono do tego – najpierw wystosowano oficjalne ostrzeżenie – że firma zablokowała dostęp do swoich usług w Australii. A w konsekwencji jednocześnie platforma Hugging Face, która hostuje modele AI, wprowadziła nowe zasady, aby ograniczyć ryzyko wykorzystywania modeli AI do tworzenia materiałów o charakterze seksualnym z udziałem dzieci. Jeśli firmy nie będą przestrzegać tych zasad, grożą im wysokie kary finansowe, nawet do 50 mln dol. Wydaje mi się, że to są realne działania.

Natomiast chciałabym wiedzieć, czy przedstawiciele instytucji państwowych mają taką wiedzę, czy została wykonana analiza dotycząca tego kierunku, jakie platformy, jakie narzędzia, w jakich ilościach – i właśnie czy to jest rozważane? Tutaj też z wielką ciekawością i uwagą śledziłam materiały, które zostały przekazane na dzisiejsze posiedzenie. I zauważyłam propozycję pana prezesa UODO, którą chciałabym wzmocnić. Ona dotyczy rozważenia wprowadzenia w krajowym systemie prawa rozwiązań podobnych do kodeksów postępowania przewidzianych w rozporządzeniu nr 2016/679. Takie kodeksy jak najbardziej mają sens, a co więcej, organizacje, instytucje, które zajmują się zwalczaniem wykorzystywania seksualnego dzieci w cyberprzestrzeni, już dostarczają materiały, które mogłyby być podstawą takich kodeksów. Mówię na przykład o publikacji organizacji Thorn, która wyraźnie pokazuje, w jakim kierunku właśnie takie kodeksy powinny zmierzać. Na pewno więc materiałów do inspiracji nie zabraknie. Bardzo dziękuję.

Przewodnicząca poseł Monika Rosa (KO):

Bardzo dziękuję.

Teraz proszę pana Konrada Ciesiołkiewicza, państwowa komisja do spraw przeciwdziałania pedofilii, o zabranie głosu. Bardzo proszę.

Zastępca przewodniczącej Państwowej Komisji do spraw przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15 Konrad Ciesiołkiewicz:

Dzień dobry państwu.

Pani przewodnicząca, ja oczywiście nie dodam prawdopodobnie nic bardziej merytorycznego niż to, co przed chwilą już powiedziano. Bowiem tezy, które my podnosimy, w ogromnej mierze są oparte na podstawie ekspertyzy wykazanej przez panią Katarzynę Staciwę, pana prezesa Mirosława Wróblewskiego oraz NASK, z którego zasobów także czerpiemy. Przede wszystkim chciałbym podziękować panu prezesowi Mirosławowi za odważną egzekucję prawa i podejmowanie działań w obszarach, które są obszarami przez wielu traktowanymi jako szare albo jako nieistotne, jako drugorzędne, wirtualne, czyli mniej realne. Tutaj pan prezes Mirosław Wróblewski i zespół UODO faktycznie wykazuje się w ostatnim czasie szczególną determinacją. I wydaje mi się, że ta sprawa jest o tyle bezprecedensowa... Oczywiście ona ma precedens, na przykład półtora roku temu w Bydgoszczy, ale chciałbym też zwrócić uwagę na statystyki, podawała je Katarzyna.

Kiedy spotykamy się z nauczycielami, trenerami, trenerkami, animatorami społecznymi, to wszyscy podnoszą kłopot wykorzystywania aplikacji z AI umożliwiającej tworzenie deepfake'ów – z kontekstami seksualnymi oczywiście. Musimy sobie też zdawać sprawę, że jeśli chodzi o kontekst seksualny, deepfaki niemalże w 100% skierowane są przeciwko dziewczynkom, dziewczętom oraz kobietom. Jeśli jest wykorzystywany ten aspekt seksualny, to absolutnie przeciwko dziewczynkom i kobietom. Pokazują to różne dane, także polskie, jak widzimy już nawet w kilku przykładach. Organy ścigania widzą ich tylko kilka, a faktycznie mamy z tym do czynienia na skalę prawdopodobnie niemalże masową. Nie wiem, czy „masowa” to jest właściwe sformułowanie, żeby też nie usensacyjniać, ale najprawdopodobniej tak. Ten dostęp dzisiaj jest masowy.

Tutaj pozwolę sobie w imieniu komisji oraz koleżanek i kolegów z zespołu podkreślić – państwo doskonale to wiecie, ale chciałbym to jeszcze powtórzyć – że mam nadzieję, że DSA,

ustawa wdrażająca akt o usługach cyfrowych, zostanie zaakceptowana przez prezydenta. Zobaczymy. Tymczasem po pierwsze chciałem bardzo podziękować i po drugie chciałbym też wyrazić wdzięczność. Cieszę się, że jest z nami pan prezes Urzędu Komunikacji Elektronicznej. Art. 28 DSA sam w sobie mówi o szczególnej potrzebie ochrony osób małoletnich. Implementacja tego prawa zajmie nam bardzo dużo czasu i też uczenia się, to widać zresztą nawet na przykładzie interwencji UODO dotyczącej AI. I tutaj zwracając się do państwa i do pana prezesa – jeśli państwo widzieliby taką potrzebę, bo my ją po prostu widzimy, to zasadnym byłoby, wydaje się, powołanie takiego zespołu, nazwałbym go roboczym, operacyjnym, nie wiem, może nie operacyjnym, może jakimś zespołem koordynacyjnym, który w sposób szczególny zadbałby w ramach polityki doświadczeń Urzędu Komunikacji Elektronicznej o szczególną ochronę osób małoletnich. To jest dzisiaj grupa pierwszego ryzyka, to jest grupa niezadbana.

Urząd Komunikacji Elektronicznej będzie przejmował nowe kompetencje i będzie się też radykalnie zmieniał. Do tej pory, jak wiemy, był szyty na miarę telekomów. Mówię to troszkę dlatego, że sam wywodziłem się przez wiele lat z branży telekomowej. Dzisiaj te nowe regulacje oznaczają też nowe polityki publiczne. Wszyscy będziemy się ich uczyć. Natomiast wszystkie możliwe badania wykazują, że osoby małoletnie są grupą największych podatności na wszelkiego rodzaju manipulacje w sieci. Wielu z nas... na sali nie, ale społecznie wielu z nas myśli, że dotyczy to oczywiście osób dojrzałych wiekowo. Jest dokładnie odwrotnie. Wiemy, że teorie konspiracyjne, dezinformacja dotyczą także młodych ludzi. Pik podatności to 14–16 lat, ale tylko w tym zakresie teorii spiskowych. Jeżeli chodzi o inne zagrożenia, ten wiek oczywiście jest znacznie niższy, o czym mówiła tutaj Katarzyna i także mówiliście państwo.

Jeżeli byłaby więc taka wola, to ja bardzo rekomendowałbym powołanie takiego zespołu roboczego, w którym państwowa komisja bez wątpienia chętnie by się odnalazła. Nawet bardzo chętnie wzięlibyśmy na siebie pewną część pracy. Po prostu jest długa droga przed nami, biorąc pod uwagę, że regulacji w tym zakresie po prostu nie było. Nawet DSA samo w sobie jest zaledwie pierwszym, bardzo drobnym i delikatnym krokiem, jeśli chodzi o ochronę osób małoletnich. Art. 8 wprost wskazuje potrzebę ochrony tej właśnie grupy wiekowej. Dziękuję.

Przewodnicząca poseł Monika Rosa (KO):

Bardzo dziękuję.

Bardzo proszę, pani Katarzyna Hernandez.

Dyrektor Zespołu Edukacji Cyfrowej i Bezpieczeństwa w Sieci Biura Rzecznika Praw Dziecka Katarzyna Hernandez:

Szanowna pani przewodnicząca, szanowni państwo, pozwolę sobie odnieść się do wypowiedzi pana Konrada Ciesiołkiewicza, bo tutaj padło bardzo ważne słowo: „przeciwko”. Te aplikacje tak naprawdę działają przeciwko. Przeciwko dziewczynkom, dzieciom, młodzieży, przeciwko dorosłym. Bo tak naprawdę jaki jest pozytywny aspekt funkcjonowania takich aplikacji, które po prostu pozwalają na kreowanie materiałów tego typu? Ja ich nie widzę, w biurze również nie potrafiliśmy ich w ogóle znaleźć. Dlatego wystosowaliśmy do Ministerstwa Cyfryzacji takie wystąpienie, w którym prosimy o przełożenie odpowiedzialności na platformy cyfrowe świadczące tego typu usługi, żeby po prostu nie dopuścić do tego, żeby można było wykorzystać materiał ukazujący seksualne wykorzystanie dzieci tzw. deepnude. Bo tak naprawdę na taką aplikację trzeba najpierw zaciągnąć zdjęcie z wizerunkiem dziecka, żeby potem móc je dalej procesować. Dlaczego więc nie przeniesiemy odpowiedzialności na takie aplikacje? Teraz mamy takie technologie, że można stwierdzić, że na tym wizerunku jest dziecko i po prostu momentalnie powinien on być odrzucony. Ta aplikacja nie powinna pozwolić dalej go procedować. I co więcej, zaapelowaliśmy o to, żeby w ogóle tego typu aplikacje, na kształt stron oferujących usługi hazardowe, wpisać na listę stron zakazanych i po prostu nie dopuścić do tego, żeby te usługi były dostępne w Polsce. Bo one po prostu działają przeciwko, tak jak tu było już powiedziane. One nie są „dla”, tylko są „przeciwko”, więc po prostu nie potrzebujemy takich stron. I tutaj też zgadzam się z panem Konradem Ciesiołkiewiczem, w tym piśmie również to wskazaliśmy, że apelujemy o powołanie grupy roboczej, bo to jest tak trudny temat, tak nowy temat i tak wielowątkowy, że po prostu musimy się zaangażować wszyscy ponad podziałami, żeby szybko zadziałać, aby wszystkie tego typu usługi były w Polsce niedostępne. I tutaj też deklaruje pełne wsparcie Biura Rzecznika Praw Dziecka, jak zadeklarowaliśmy w tym piśmie, w pracach nad tymi działaniami. Bardzo dziękuję.

Przewodnicząca poseł Monika Rosa (KO):

Ktoś z państwa jeszcze chciałby zabrać głos? Bardzo proszę, pan prezes.

Prezes Urzędu Komunikacji Elektronicznej Przemysław Kuna:

Dziękuję serdecznie.

Pani przewodnicząca, Wysoka Komisjo, szanowni państwo, ja już to wielokrotnie mówiłem. Natomiast podam stan faktyczny, który jest na chwilę obecną, jeżeli chodzi o Urząd Komunikacji Elektronicznej. Faktycznie DSA to nowe wyzwania urzędu i wszyscy to wiemy, jeżeli pan prezydent Nawrocki faktycznie podpisze tę ustawę. Z tego co wiem, to chyba jutro będzie jeszcze głosowana poprawka senacka, więc za chwilę będziemy wiedzieli, czy jesteśmy po tej słusznej, uporządkowanej stronie mocy, czy też dalej będziemy musieli być w tym stanie, w którym jesteśmy.

Jako prezes, jako urząd nie mam w tej chwili narzędzia do tego, żeby coś pozytywnego powiedzieć Komisji. Próbuje posilkować się Irlandią jako tym krajem, który wskazuje te wytyczne – patrząc z punktu widzenia Europy, nie tylko naszego kraju. Co chcę zaproponować? Jeżeli wejdzie DSA, to wiemy, że będzie tam też komisja z natury, ponieważ jest tam zapis mówiący o tym, że przy prezesie UKE będzie komisja, która będzie wskazywała i pokazywała możliwości szybkiego reagowania czy też współpracy w zakresie już generalnie wszystkich treści, które są wskazywane w DSA. Natomiast ze swojej strony podjąłem też takie zobowiązanie i to przekażę, że jeżeli będzie weto i nie będzie możliwości zrobienia tego w ramach ustawy, to tak czy inaczej mam możliwość powołania takiej komisji i ja tę komisję powołam. Chciałbym ją trochę rozszerzyć, bo to nie jest oczywiście tylko kwestia samej młodzieży. Dzisiaj rozmawiamy o młodzieży, tu chyba wszyscy czujemy wagę tego problemu i jak on jest palący. I faktycznie wszystkie te słowa, które tutaj były tu wskazane, są prawdziwe. Znamy te fakty, sami mamy dzieci. Dobra uwaga była chyba też do państwa z Ministerstwa Sprawiedliwości, że post factum to już co najmniej o jeden dzień za późno. I to jest niestety nowa rzeczywistość, z którą się zmierzamy, bo tak jak w DSA są na przykład dwa dni od zgłoszenia na podjęcie działań w przypadku zaufanych podmiotów, to naprawdę musimy w takich kategoriach rozważać możliwość reagowania na te wszystkie działania. Jeżeli to będzie leżało tak jak w tej chwili, nie wiem, 30 dni, to w zasadzie nie ma już większego znaczenia. Oczywiście trochę przez łzę, ale tak jest. Jeżeli czegoś się nie usunie w ciągu najbliższych godzin albo dni, to w świecie wirtualnym przestaje to mieć znaczenie. To więc w zasadzie chyba tyle.

Jeżeli nie będzie tego podpisu pana prezydenta, to w styczniu wrócimy do rozmowy i zapraszam. Wydaje mi się, że tak czy inaczej te przepisy muszą wrócić, a tylko będziemy jeszcze lepiej przygotowani do tego, ja jako urząd, a z państwem jako Polacy, żeby te przepisy stosować w praktyce.

Przewodnicząca poseł Monika Rosa (KO):

Bardzo dziękuję.

Czy ktoś jeszcze z państwa? Jeśli nie, to ja pozwolę sobie teraz zabrać głos.

Po pierwsze, oczywiście Komisja, ponieważ jest Komisją do Spraw Dzieci i Młodzieży, dotyczy dzieci i młodzieży, natomiast to dotyczy również młodych dorosłych, a tak naprawdę dotyczy całego społeczeństwa. Oczywiście dzisiaj skupiliśmy się na kwestiach dotyczących dzieci i młodzieży jako tych najbardziej drastycznych, ale doskonale wiemy, że sztuczna inteligencja i kwestie deepfake'ów dotyczą nas wszystkich w kontekście kradzieży tożsamości, fałszywej reklamy, szantażu, nękania, manipulacji, polaryzacji, ale także wpływu na to, jak funkcjonuje społeczeństwo, szczególnie w okresie tzw. wojny hybrydowej, która toczy się na terenie Polski. Wiemy doskonale, jak duże zagrożenia deepfaki mogą wywołać w zakresie bezpieczeństwa indywidualnego, ale także bezpieczeństwa społecznego. Wydaje mi się więc, że obowiązujące regulacje prawne są, mówiąc krótko, naprawdę niewystarczające. I oczywiście jest tak, że my zawsze będziemy gonić za tym, co się wydarzy w technologiach. Tylko wydaje się, że to jest ten czas, kiedy wszyscy musimy powiedzieć, że spróbujmy dogonić to, co się dzieje w technologiach, szczególnie w tak kryzysowych czasach.

Dlatego dziękując resortom za informacje, przede wszystkim podziękuję CBZC za to, że zwróciło uwagę, że my potrzebujemy tej regulacji, że kwestia rozpowszechniania deepfake'ów musi być karana, musi być jednoznacznie wpisana do Kodeksu karnego. Nie wystarczą nam przepisy, które obecnie funkcjonują. Pani Katarzyna Staciwa, Konrad i przedstawiciele Biura Rzecznika

Praw Dziecka zwrócili uwagę, że nie ma sensu funkcjonowanie jako dozwolonych aplikacji, które pozwalają na rozbieranie zdjęć dziecka. Jest to chyba kwestia, która nie podlega dyskusji, że takie aplikacje nie powinny być dozwolone na polskim rynku, i ta odpowiedzialność rzeczywiście musi być w jakimś sensie po stronie platform cyfrowych, ale nie tylko. Mamy też kwestie zderzania się z fałszywą reklamą, z wykorzystywaniem zdjęć lekarzy, celebrytów, tworzeniem fałszywych informacji dotyczących bezpieczeństwa Polski, różnego rodzaju wydarzeń czy filmów, które wywołują również emocje społeczne i radykalizują także osoby najmłodsze, ale w ogóle nas wszystkich.

Wydaje mi się więc, że koniecznością jest powołanie zespołu, który będzie dążył do zmiany prawa. Raczej w dwóch krokach. Pierwszy, żeby poinformować o tym, jakie mamy obecnie obowiązujące regulacje prawne, bo sytuacja dotycząca umorzenia sprawy rozebrania zdjęć, tak to nazwijmy, stworzenia fake'a z nastolatką wskazuje, że jednak organy państwa nie zawsze mają wystarczającą wiedzę. I to jest coś, co możecie państwo zrobić właściwie już i teraz. Zarówno jeśli chodzi o kwestie Policji, jak i kwestie prokuratury. Nie można powiedzieć, że rozebranie, przedstawienie nagiego zdjęcia nastolatki jest czymś normalnym, dozwolonym i nie ma szkodliwości społecznej. Ale drugą rzeczą jest oczywiście konieczność zmiany regulacji prawnych i stworzenia prawa, które będzie obejmowało właśnie kwestię deepfake'ów.

I ja do tego państwa zachęcam, apeluję. I tak naprawdę będziemy tego jako Komisja pilnować, nie tylko jako Komisja do Spraw Dzieci i Młodzieży, ale wydaje mi się, że generalnie jako parlament. I tutaj do pana prezesa UKE – chyba rzeczywiście ten ciężar w jakimś sensie będzie spoczywał również na panu, ale także na Ministerstwie Sprawiedliwości, bo to kwestie zmiany Kodeksu karnego, na Policji i oczywiście na resorcie cyfryzacji. Nie wiem, czy będziemy do państwa pisać jeszcze osobno w tych kwestiach. Być może napiszemy tak dla formalności. To, co napisane, nie ucieknie. Natomiast w styczniu będziemy sprawdzać po prostu, czy coś się wydarzyło. A jak nie, pójdziemy do pana prezesa UODO i tam zrobimy zespół, do którego państwa zaprosimy ze wszystkimi przedstawicielami instytucji, ale myślę, że tutaj dobra wola chyba nas wszystkich jest wystarczająca, żeby ten proces po prostu się zadział.

A po tym krótkim wstępie pozwolę sobie również udzielić odpowiedzi poszczególnym resortom. Bardzo proszę, resort sprawiedliwości.

Naczelnik wydziału w departamencie MS Magdalena Bochińska:

My się oczywiście przychylamy. Tak jak już wskazałam, widzimy problem i chcemy go rozwiązać po prostu jak najszybciej.

Przewodnicząca poseł Monika Rosa (KO):

Fantastycznie. Bardzo dobra wola.

Resort cyfryzacji i NASK – bardzo proszę, jakiś komentarz jeszcze na koniec.

Dyrektor pionu w NASK-PIB Maciej Siciarek:

Bardziej jako NASK. Znaczący my się również przychylamy. Widzę też taką osobistą potrzebę spojrzenia na wszystkie ustawy, które obejmują ten obszar, i być może w przyszłości większą integrację, ponieważ tych ustaw dotyczących ochronę dzieci i małoletnich, od ustawy o krajowym systemie cyberbezpieczeństwa przez inne ustawy, jest kilka. I pewnie to dobrze, żebyśmy w docelowym modelu osiągnęli spójność, żeby to było jakoś uwzględnione, jakoś też wyróżnione jako szczególnie obszar dalszego zainteresowania i troski.

Przewodnicząca poseł Monika Rosa (KO):

Bardzo dziękuję.

Czy UODO, pan prezes Wróblewski?

Prezes UODO Mirosław Wróblewski:

Szanowna pani przewodnicząca, oczywiście będziemy wspierać te działania, zarówno jeżeli chodzi o kwestie zmapowania dokładnie rzeczywiście wszystkich przepisów, także w kontekście ich rzeczywistego wykorzystania czy w kontekście stworzenia nowej regulacji, ale również ewentualnego wsparcia, jeżeli chodzi o działania szkoleniowe, o budowę wiedzy w tym zakresie. Myślę, że czas jest najwyższy. Przedstawiciel Ministerstwa Sprawiedliwości wskazał możliwe skutki, na przykład przestępstwa kradzieży tożsamości. Wspomniałem o Wielkiej Brytanii i Korei Południowej jako krajach o najbardziej drastycznych przypadkach. Nie chciałem o tym

mówić, ale tam niestety właśnie na skutek stosowania tych aplikacji deepnude i różnego rodzaju szantaży i groomingu wystąpiły przypadki samobójstw i to nie w pojedynczych przypadkach.

Myślę więc, że jest pora na działanie, bo lepiej zrobić to teraz, niż po jakimś tragicznym przypadku przeprowadzać prace legislacyjne w jakimś przyspieszonym tempie. Bardzo dziękuję.

Przewodnicząca poseł Monika Rosa (KO):

Bardzo dziękuję.

Pani minister Piechna-Więckiewicz.

Podsekretarz stanu w Ministerstwie Edukacji Narodowej Paulina Piechna-Więckiewicz:

Szanowna pani przewodnicząca, Wysoka Komisjo, szanowni zebrani, zebrane, my oczywiście jesteśmy tutaj w gotowości i też kwestie poruszane przed chwilą przez pana prezesa związane są tak naprawdę również z profilaktyką suicydalną i przeciwdziałaniem. My w zakresie swoich działań czy dokumentów wypracowanych z organizacjami pozarządowymi, specjalistami, specjalistkami, które wysyłamy systematycznie do szkół – poza wspomnianymi przez pana prezesa przedmiotami – informujemy również rodziców. Znaczący w tych materiałach zawsze są też informacje dotyczące rodziców. Oni jeszcze w wielu wypadkach nie identyfikują wszystkich obszarów zagrożenia, więc przy pomocy tutaj też państwa, różnych instytucji zbieramy tę wiedzę, wysyłamy, upowszechniamy też materiały NASK, Policji. Nie będę się już powtarzać. Jesteśmy więc tutaj w gotowości. Chciałam tylko też wspomnieć o tym, że również w ramach prac państwa Komisji i różnych wniosków, które się pojawiały, w tej chwili w resorcie edukacji współpracujemy też, już w ramach grup roboczych w resorcie, nad wytycznymi dotyczącymi ochrony wizerunku dziecka. I tutaj też pewnie jakiś potencjał legislacyjny jest, chociaż ważne są również wytyczne jako pewne standardy, stworzone także na gruncie obecnie obowiązujących regulacji. Chciałam zgłosić dalszą gotowość Ministerstwa Edukacji Narodowej do prac.

Przewodnicząca poseł Monika Rosa (KO):

Bardzo dziękuję. Myślę, że w wytycznych można zawrzeć jasną informację, że nie wolno bez zgody przetwarzać niczyjego wizerunku i innych danych osobowych. Bo nie jest to wiedza powszechna, szczerze mówiąc.

Mam jeszcze dwie osoby wpisane na listę. Pani mecenas Wawrowska i doktor Konrad Ciesiołkiewicz. Bardzo proszę.

Przedstawicielka Zespołu ds. Kobiet przy Naczelnej Radzie Adwokackiej Danuta Wawrowska:

Dzień dobry, witam państwa serdecznie, panią przewodniczącą i wszystkich wyjątkowych specjalistów, których dzisiaj miałam możliwość wysłuchać.

Chciałabym się odnieść do apelu, który był ogłoszony na początku, chyba przez pana posła, ale ponieważ nie przedstawiliście się państwo, nie mogę przytoczyć nazwiska, o tym, że do projektu DSA, który wyszedł z Sejmu, została wprowadzona czy zaproponowana poprawka Senatu dotycząca braku możliwości albo odrzucenia rygору natychmiastowej wykonalności. Jest to dla mnie bardzo mocna rzecz i zastanawia mnie, dlaczego. Nie znam uzasadnienia poprawek Senatu, ale po wypowiedzi pana prezesa UKE mamy tutaj jakby oczywistą odpowiedź.

Żeby te procedury mogły funkcjonować, to musimy podejmować szybkie działania. Rygor natychmiastowej wykonalności to taka instytucja prawna, która pozwala na wykonanie orzeczenia natychmiast, zanim stanie się ono ostateczne, i umożliwia zaspokojenie roszczeń. Natomiast opóźnienie wykonania tej decyzji byłoby szczególnie szkodliwe. W materii, w której my się poruszamy, działania muszą być podejmowane natychmiast. Wspaniale ktoś powiedział, chyba pani Katarzyna Staciwa, że za miesiąc po prostu nikogo już to nie będzie interesowało. Nam jako prawnikom, mnie jako adwokatce brakuje po prostu narzędzi do tego, żeby skutecznie reagować na tego rodzaju przestępcze działania. Zatem z mojej strony apel do wszystkich państwa – nie wiem, czy my możemy przekazać stanowisko Komisji, jeżeli państwo się zgodzicie, żeby ten rygor natychmiastowej wykonalności w tym projekcie został utrzymany. Dziękuję bardzo.

Przewodnicząca poseł Monika Rosa (KO):

Bardzo dziękuję. Pani mecenas, nie możemy, ponieważ dzisiaj Komisja nie w tym temacie, ale jakby podzielałam opinię i pani mecenas, i pana posła Bliźniuka.

Doktor Konrad Ciesiołkiewicz.

Zastępca przewodniczącej PKDP Konrad Ciesiołkiewicz:

Bardzo krótko. Oczywiście pod wystąpieniem pani mecenas Wawrowskiej podpisuję się całym sobą. Myślę, że też wielu z nas obecnych tutaj na sali. Natomiast chcę powiedzieć tylko o dwóch kwestiach, bo one nie padły. To znaczy, że faktycznie te zmiany... Wiem, że my to wszystko wiemy, ale chciałbym być też trochę ambasadorem tego, co dzieje się w obszarze oświaty, patrząc na panią ministraż, bo faktycznie systemowo jest bardzo dużo dobrych światła. Edukacja obywatelska, edukacja zdrowotna – chociaż wszyscy płacemy, że nie jest obowiązkowa – edukacja medialna, która wchodzi od września przyszłego roku. Wszystkie te przedmioty – edukacja medialna nie będzie przedmiotem, tylko będzie częścią kilku przedmiotów z wiodącą rolą języka polskiego – uwzględniają aspekty, o których tutaj rozmawiamy, i stanowią element systemu prewencji. I to jest niezbędne. I to jest niezwykle, że to się dzieje.

Druga rzecz, którą chcę powiedzieć. To, o czym rozmawiamy, dotyka głębokiego kryzysu, jak wiemy, emocjonalnego zdrowia psychicznego. To tutaj już padało. Dopiero od półtora roku wiemy, jesteśmy bardziej świadomi, że w zasadzie polscy uczniowie nawet w badaniach PISA wypadają... niestety szorują dna. Szorujemy jako społeczeństwo, ale wiemy to dopiero od niedawna, choć szorujemy dawno. Chcę powiedzieć, że mamy wiedzę na ten temat – zawdzięczamy ją również pewnej otwartości – o tych danych na dobrą sprawę relatywnie od niedawna, bo dopiero od półtora roku lub od dwóch lat, z tego co pamiętam.

I trzecia rzecz na koniec, tylko nie chciałbym tutaj brzmieć populistycznie, ale w zeszłym tygodniu ukazał się raport WeProtect, bardzo renomowanej organizacji, której metodologia leży u podstaw naszego planu krajowego przeciwdziałania krzywdzeniu seksualnemu w Polsce na lata 2023–2026. I zjawisko, o którym dzisiaj rozmawiamy, deepfake AI, zostało tam ujęte i pokazane procentowo. Przyrost liczby materiałów CSAM, czyli ukazujących seksualne wykorzystanie dziecka za pomocą AI, to jest wzrost rok do roku 1300%. Celowo mówiłem o tych działaniach systemowych, jak one są wolne wobec rzeczywistości, która pędzi w taki sposób, że w ciągu roku przyrosły one – oczywiście w skali tego wszystkiego, co jest u źródeł tego raportu, czyli danych NCMEC i brytyjskiej Internet Watch Foundation, ale my jesteśmy absolutnie częścią tych danych – 1300% w skali roku. Zobaczmy, jakie wyniki będą w przyszłym roku. Te zmiany więc są bardzo ważne, są krytycznie ważne, ale musimy działać szybko i faktycznie tutaj jeszcze raz podpisuję się pod wystąpieniem pani mecenas Wawrowskiej, że brak tej klauzuli jest trudny do zrozumienia. Dziękuję.

Przewodnicząca poseł Monika Rosa (KO):

Bardzo dziękuję.

Pani Zuzanna Jastrzębska, bardzo proszę.

Prezesk zarządu Fundacji Wspomagania Rozwoju Dzieci Edyty Gruszczyk-Kolczyńskiej Zuzanna Jastrzębska-Krajewska:

Zuzanna Jastrzębska-Krajewska, doktor nauk społecznych, ekspertka w zakresie edukacji najmłodszych dzieci.

Ja w ogóle bardzo państwu dziękuję za tę dyskusję – w sprawach państwa Komisji dopiero raczkuję. Natomiast nie raczkuję w temacie rozwoju myślenia dzieci. I chciałam powiedzieć coś państwu tak na koniec, przysłuchując się. Nie planowałam co prawda dzisiaj mówić, ale jest to bardzo ważna sprawa. Najgorsza w postrzeganiu prawa jest nieświadomość. To znaczy wszystko fajnie. Uświadamiamy dzieci, że na przykład wzięcie noża i skaleczenie jest niebezpieczne. Problem w tym, że wzięcie telefonu i przerobienie swojego rodzinnego zdjęcia na śmieszne nie jest przez nikogo uznawane za niebezpieczne. Na przykład rodzinnie dodajemy tam czapkę Mikołaja itd. Małe dzieci nie rozumieją konsekwencji tego, co robią, a telefony są w ich rękach. Nie mają też świadomości rodzice.

I tutaj wszystkie programy edukacyjne, które zastosujemy... Problem w tym, że kiedy rodzice słyszą, że jest kolejny program, to oni już nawet nie otwierają tych wiadomości. Wiem, że otwieram puszkę Pandory w tym momencie. Ja nie wiem, co z tym zrobić. Natomiast proszę państwa, mamy ogromny problem. Dzieci nie rozumieją, że to jest przekroczenie granic prawa. Rodzice nie rozumieją, że mogą być one przez to sądzone.

Dlaczego państwu o tym mówię? Dwa miesiące temu moja córka stała się ofiarą przemocy, III klasa szkoły podstawowej w Warszawie, dziewięcioletnie dzieci. To jest dla mnie trudne, ale już mówię. Została ofiarą kręgu nielubienia Poli. To się nazywało krąg. To się wydarzyło

na świetlicy, a dzieci powiedziały, że wizerunek, który zamierzają stworzyć, to podobizna mojej córki z nożem w głowie. I kiedy zgłosiliśmy tę sprawę, to rodzice, sami rodzice z tej klasy powiedzieli: dzieci przecież czasem robią takie głupie rzeczy. Kiedy powiedzieliśmy, że to podlega prawu, podlega konkretnie przepisom, że możemy nałożyć na te dzieci sąd rodzinny... To jest ogromny problem, ponieważ ludzie sobie po prostu nie zdają sprawy, że ich dzieci przekraczają prawo. I mimo wszelkich programów, które są zastosowane, mimo lex Kamilek ta sprawa nie została wyjaśniona. Mówię to państwu tylko dlatego, że trzeba być niesamowicie świadomym. Naprawdę ani w dzieciach, ani w ich rodzicach nie ma świadomości przekraczania prawa. I powinniśmy też na to tak patrzeć, poprzez rozwój myślenia. Natomiast to jest puszka Pandory. Oczywiście włączam się jak najbardziej do pracy, którą będę mogła robić z mojej perspektywy. Dziękuję państwu.

Przewodnicząca poseł Monika Rosa (KO):

Bardzo proszę, pani przewodnicząca.

Poseł Barbara Okuła (Polska2050):

Dzień dobry państwu.

Przede wszystkim chciałabym podziękować za tę dyskusję i tutaj też chciałabym podbić właśnie pani głos, bo też miałam takie same refleksje, że ta nieświadomość jest bardzo ważna, ale też poczucie bezkarności. Myślę, że musimy również głośno mówić o tym, jakie kary grożą. I zwiększyć też ścigalność takich przestępstw, bo mam wrażenie, że ta anonimowość w sieci sprawia, że przestępcy nie są ścigani. A tych potencjalnych przestępców, którzy nie mają właśnie tej świadomości, coś skłoni do tego, żeby jednak takie zdjęcie przerobić, żeby ośmieszyć. I nawet myślą, że to nic takiego. I to, co pani powiedziała, rodzice często też bagatelizują, obracają to w żart. A my musimy pokazywać, że to są przestępstwa, że od drobnych rzeczy dzieją się później tragedie, takie, że dziecko zabija dziecko, takie, że dziecko popełnia samobójstwo, bo zostało wielokrotnie ośmieszane. Myślę więc, że to jest ważny temat. Dobrze, że wszyscy tu jesteśmy jednomyślni i świadomi tego, jak ważna jest prewencja. Myślę, że edukacja, świadomość, prewencja ograniczy też popełnianie tych przestępstw, często dokonywanych z takiej właśnie nieświadomości i minimalizowania ich wagi. Myślę więc, że te tematy są bardzo ważne.

Dziękuję również za ten głos o zespole roboczym. Myślę, że to też jest ważne, żeby wspólnie pracować i wypracować dobre rozwiązania, bo one są niewystarczające. Postęp idzie tak do przodu. Dzieci za pomocą sztucznej inteligencji przerabiają te obrazki, cieszą się, bawią się tym. Natomiast to staje się bardzo niebezpieczne. I tutaj też i rola edukacji. Wiem, że są te przedmioty – i dobrze, natomiast często dzieci te przedmioty traktują jako przedmiot dodatkowy i nie biorą pod uwagę, jak to jest ważne.

Chciałam też podziękować za ten głos odnośnie do aplikacji, które powinny wykrywać, że to są obrazy dzieci. Myślę, że to jest proste do zrobienia, bo twarz dziecka jest do wykrycia. To powinno być od razu zabronione. Nie powinno być możliwości w ogóle jakichkolwiek zmian w zdjęciach dzieci. Bardzo dziękuję. Myślę, że takie właśnie Komisje są potrzebne. Pani przewodnicząca, dziękuję za ten temat.

Przewodnicząca poseł Monika Rosa (KO):

Bardzo proszę, pani ministro.

Podsekretarz stanu w MEN Paulina Piechna-Więckiewicz:

Szanowni państwo, ja tylko uściśłę. Edukacja obywatelska jest przedmiotem obowiązkowym. Edukacja medialna w ramach podstaw programowych będzie w przedmiotach obowiązkowych. Z tych wszystkich przedmiotów, o których dzisiaj rozmawialiśmy, tylko edukacja zdrowotna jest w tej chwili przedmiotem nieobowiązkowym. Te decyzje jeszcze przed resortem edukacji.

Kolejna sprawa. Zdajemy sobie sprawę z tego, pan doktor Ciesiołkiewicz trochę o tym powiedział, że do tej pory te kanały, rozmowy z rodzicami nie były właściwie wykorzystywane, i właśnie od półtora roku staramy się to naprawić. Oczywiście jest to trudna grupa docelowa ze względu na to, że nie są bezpośrednim interesariuszem w systemie. Mówię tutaj o zobowiązaniu do uczestnictwa, to jest jakby dosyć istotna sprawa, tak elegancko się wyrażę.

Natomiast jeżeli chodzi o kwestię edukacji prawnej, to my z resortem sprawiedliwości, który – za co bardzo dziękuję – uczynił już wiele pracy i robi coraz więcej, zaprosiliśmy wszystkie zawody prawnicze współpracujące z kuratoriami, od radców prawnych, adwokatów, komorników

i notariuszy. Chcemy – nie tylko w zakresie edukacji obywatelskiej – żeby dzieci od przedszkolaków miały świadomość, jaka jest ich odpowiedzialność cywilna, karna, różna. To też jest dla nas bardzo ważny projekt. Mówię o tym, bo może on się tak bardzo nie przebija do opinii publicznej.

A jeżeli pani, już po Komisji, opowie mi trochę więcej, to też chciałabym usłyszeć. Bardzo jest mi przykro. Dziękuję bardzo.

Przewodnicząca poseł Monika Rosa (KO):

Szanowni państwo, bardzo dziękuję za tę Komisję. Pozwolę sobie jeszcze na kilka takich kwestii. Po pierwsze, temat edukacji medialnej też będzie przedmiotem obrad Komisji, ponieważ nauczyciele są zaniepokojeni tym, w jaki sposób ma to wyglądać. Prosimy więc Ministerstwo Edukacji Narodowej o obecność i wyjaśnienie, w jaki sposób to będzie funkcjonowało.

Również bardzo proszę państwa posłów o wysłanie tematów do prac Komisji.

Z Ministerstwem Sprawiedliwości i UKE uzgodnimy system stworzenia zespołu i liderstwo w tym zespole.

I ostatnia rzecz. Po raz kolejny na tej Komisji dużo padało odnośnie do mediów cyfrowych i zagrożeń. Padł też temat Australii. Ja bym bardzo państwa zaprosiła jako Komisja, jeśli będzie oczywiście zgoda posłów, do tego, abyśmy realnie przedyskutowali temat limitu prawnego wieku dostępu do platform cyfrowych, zapisanego nie w regulaminach, ale w obowiązującym w Polsce prawie, i realnej weryfikacji tego wieku. I czy my sobie ten wiek, po dyskusji, będziemy chcieli ustalić na 13, 14, 15, 16 lat, czy w modelu australijskim, czy francuskim, wydaje się być w tym momencie kwestią wtórną. Ale wydaje się być krytyczną kwestią, już nawet spóźnioną, to, że takiej regulacji ciągle w polskim prawie nie ma. Jeśli więc państwo posłowie nie zgłoszą sprzeciwu, to proponuję taką dyskusję nad założeniami projektu rozpocząć i być może przenieść go już jako projekt komisyjny dalej. Ale to w nowym roku. Bardzo państwu dziękuję za tę Komisję.