

X kadencja



KANCELARIA SEJMU

Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

■ KOMISJI DO SPRAW DZIECI I MŁODZIEŻY (NR 22)

z dnia 20 marca 2025 r.

Pełny zapis przebiegu posiedzenia Komisji do Spraw Dzieci i Młodzieży (nr 22)

20 marca 2025 r.

Komisja do Spraw Dzieci i Młodzieży, obradująca pod przewodnictwem poseł **Moniki Rosy (KO)**, przewodniczącej Komisji, rozpatrzyła: – informację na temat regulacji Unii Europejskiej dotyczących CSAM.

W posiedzeniu udział wzięli: **Michał Gramatyka** sekretarz stanu w Ministerstwie Cyfryzacji wraz ze współpracownikami, **Małgorzata Pawelec** dyrektor Departamentu Prawa Europejskiego w Ministerstwie Sprawiedliwości wraz ze współpracownikami, **Paulina Piechna-Więckiewicz** podsekretarz stanu w Ministerstwie Edukacji Narodowej wraz ze współpracownikami, **Kamil Kisiel** zastępca dyrektora Departamentu Spraw Międzynarodowych i Migracji w Ministerstwie Spraw Wewnętrznych i Administracji, **Piotr Drobek** dyrektor Departamentu Innowacyjności i Zarządzania Danymi w Urzędzie Ochrony Danych Osobowych, **Antonio Labrador Jimenez** przedstawiciel Komisji Europejskiej, **Katarzyna Hernandez** dyrektor Zespołu Edukacji Cyfrowej i Bezpieczeństwa w Sieci w Biurze Rzecznika Praw Dziecka, **Anna Kolińska-Śnieg** prokurator w Prokuraturze Krajowej, **John Carr** przedstawiciel OBE, **Salla Huikuri** przedstawiciel ECPAT, **Konrad Ciesiołkiewicz** i **Joanna Napierała** przedstawiciele Państwowej Komisji do spraw przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15, **Monika Golik** zastępca Dyrektora Biura Kryminalnego w Komendzie Głównej Policji, **Bartosz Furgala** zastępca komendanta w Centralnym Biurze Zwalczania Cyberprzestępczości, **Maciej Groń** ekspert do spraw regulacji prawnych i współpracy naukowej w Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego wraz ze współpracownikami, **Maria Broedner** osoba pierwszego kontaktu, przedstawiciel Komitetu Ochrony Praw Dziecka, **Katarzyna Katana** i **Magdalena Witecka** przedstawiciele Fundacja Dajemy Dzieciom Siłę, **Patrycja Lubomirska** społeczny współpracownik senatora Rzeczypospolitej Polskiej Jolanty Hibner, **Katarzyna Staciwa** niezależny ekspert, **Hubert Taładaj** przewodniczący Zespołu Stałego ds. Młodzieżowych Rad Polskiej Rady Organizacji Młodzieżowych, **Danuta Wawrowska** członek Zespołu do spraw Kobiet przy Naczelnej Radzie Adwokackiej, **Alicja Zielińska** przedstawiciel Fundacji Korczaka.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Magdalena Kowalska** i **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 serdecznie panie i panów posłów. Witam zaproszonych gości. Witam pana ministra Michała Gramatykę, sekretarza stanu w Ministerstwie Cyfryzacji wraz ze współpracownikami. Witam przedstawicieli Ministerstwa Edukacji Narodowej, Ministerstwa Zdrowia, Urzędu Ochrony Danych Osobowych. Witam panią prokurator Annę Kolińską-Śnieg z Prokuratury Krajowej. Witam serdecznie panią Katarzynę Hernandez z Biura Rzecznika Praw Dziecka. Witam przedstawicieli Państwowej Komisji do spraw przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15 – pana Konrada Ciesiołkiewicza i panią Joannę Napierałę wraz ze współpracownikami. Witam serdecznie panią Monikę Golik z Komendy Głównej Policji. Witam przedstawicieli Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego. Witam przedstawicieli wszystkich zaproszonych organizacji.

Nasze dzisiejsze posiedzenie Komisji jest wyjątkowe, ponieważ mamy gości z zagranicy. Na państwa biurkach leżą słuchawki, tłumaczenie będzie symultaniczne. Witam serdecznie przedstawiciela Komisji Europejskiej, pana Antonio Labradora Jimeneza. Witam serdecznie gości z Wielkiej Brytanii – pana Johna Carra i panią Sallę Huikuri z ECPAT.

Temat dzisiejszego posiedzenia to informacja na temat regulacji Unii Europejskiej dotyczących CSAM. Pozwolę sobie zmienić nieco zwyczajowy harmonogram Komisji i najpierw do głosu dopuścić ekspertów, a później prosząc o opinię, komentarz i stanowisko ministra do spraw cyfryzacji.

W związku z tym bardzo proszę o zabrania głosu przez panią Katarzynę Staciwę.

Niezależna ekspert Katarzyna Staciwa:

Dzień dobry państwu. Nazywam się Katarzyna Staciwa. Będę dzisiaj mówić z perspektywy przede wszystkim policjantki, która nosiła mundur przez dwadzieścia sześć lat, zajmowała się tym zagadnieniem nie tylko w Polsce, ale i poza granicami kraju – w Europejskim Urzędzie do Spraw Walki z Cyberprzestępczością. Uzupełnię tę perspektywę o perspektywę naukowca, psychologa, seksuologa. Podpierając się współpracą z podmiotami na całym świecie, współpracą w ramach projektów europejskich, chciałabym, żeby ta perspektywa była jak najbardziej szeroka, żeby dostarczyła argumentów na temat tego zjawiska. Ale też muszę ostrzec, że ta prezentacja nie będzie łatwa w odbiorze. Długo zastanawiałam się jaką przyjąć dzisiaj narrację i rzeczywiście chyba najbliższą mi do narracji polegającej na mówieniu prawdy bez koloryzowania tego jak jest, na podpieraniu się faktami, potwierdzonymi informacjami przez międzynarodowe podmioty. To będzie ta perspektywa. Mam nadzieję, że dostarczy ona państwu informacji niezbędnych do tego, żeby podejmować właściwe decyzje. Skupię się na czterech blokach informacji. Opowiem trochę o zjawisku, opowiem o faktach i liczbach w tym zakresie. Wyjaśnię, na czym polega rola dostawców usług, takich jak podmioty, które dostarczają poszczególne rozwiązania w internecie. Zostawię państwa z pewnym przesłaniem, prosząc o refleksję zarówno instytucjonalną, jak i osobistą.

Dla zrozumienia tej dziedziny bardzo ważny jest podział na zachowania i na treści audio-wizualne. Jeśli chodzi o zachowania, to mamy tutaj dość szeroki katalog – od uwodzenia, nagabywania, szantażu na tle seksualnym, ale mamy też do czynienia z nowymi kierunkami rozwoju zjawiska. Jednym z nich jest np. child abuse pyramid sites, czyli taka forma zapraszania do wymiany linkami, które dają dostęp do treści CSAM i treści w – uwaga – tzw. otwartym internecie, a nie takiej części internetu, gdzie trzeba rzeczywiście szczególnie szukać tych treści. To polega na tym, żeby zapraszać coraz więcej osób, które mogą być zainteresowane takimi treściami i umożliwiać, żeby poprzez szerowanie dalej tych linków, skupiały się one na dołączaniu kolejnych osób, a dzięki temu zyskują one nagrody w postaci jeszcze większego dostępu do tych treści. To jest też ogromne zagrożenie w postaci funkcjonowania grup zamkniętych w obszarze szyfrowanej komunikacji tzw. end-to-end encryption. Jest to na podobieństwo sekt. Polega to na tym, że osoby potencjalnie zainteresowane seksualnie dziećmi, ale też nie tylko, bo motywacja tych sprawców jest bardzo różna, dosłownie łowią dzieci, zapraszając je na taki obszar, bo dokładnie wiedzą, że ten obszar nie jest monitorowany. Raportowanie z tego obszaru praktycznie nie istnieje. Nakazują tam pewne zachowania, które nawet trudno określić. Natomiast pozostali uczestnicy takiej grupy przyglądają się takim zachowaniom, patrzą, jak dziecko przystosowuje się do poleceń, które często są bardzo poniżające. Im większa aktywność takiej grupy, tym bardziej drastyczne są zachowania. Oczywiście ostatni obszar to materiały wytworzone za pomocą sztucznej inteligencji. Jest ich coraz większa ilość. Są dostrzegane przez infolinie współpracujące w ramach stowarzyszenia In Hope, ale o tym za chwilę.

Druga część, druga perspektywa patrzenia na to zjawisko to właśnie treści pornograficzne z udziałem małoletniego, czyli terminologia na gruncie naszego Kodeksu karnego. Natomiast, jeśli chodzi o dwa podstawowe akty prawne w tym obszarze – Konwencję z Lanzarote i dyrektywę unijną, to znajdują się tam dokładne definicje, co jest taką treścią. Na zasadzie wykluczenia możemy wiedzieć, co taką treścią nie jest. Czas skończyć z narracją w postaci „jakieś zdjęcia, jakieś materiały”. To są treści, na których zostało uchwycone wykorzystywanie dziecka. To są dowody przestępstwa, nic innego. Tak powinniśmy je nazywać, a nie posługiwać się terminem „pornografia dziecięca”, który nie oddaje tego, czym rzeczywiście są te materiały. W kolejnej edycji dyrektywy, w recast, który w tej chwili jest praktycznie na ukończeniu, tego sformułowania już nie będzie.

Zanim o liczbach, tak jak mówiłam – długo zastanawiałam się, jaką przyjąć tutaj narrację i chciałabym, żebyśmy patrzyli na to zjawisko z jedynej właściwej perspektywy, a jest nią perspektywa pokrzywdzonego dziecka. Dla mnie takim dzieckiem jest np. Ania. Ania ma dwanaście lat, lubi taniec, lubi zwierzęta, jest aktywna w mediach społecznościowych. Tak jak wiele nastolatek w jej wieku, rozmawia w mediach społecznościowych z potencjalnymi przyjaciółmi. W którymś momencie zaczyna konwersację z chłopcem, tak jej się wydaje. Konwersacja zaczyna być coraz bardziej intensywna i przeradza się w relację romantyczną. Ania zaczyna być proszona o zdjęcia. Najpierw wysyła niewinne zdjęcia. Później zaczyna być proszona o zdjęcia klatki piersiowej. W odpowiedzi na te zdjęcia zaczyna otrzymywać takie zdjęcia, które ją przerażają. To są chwile, kiedy po raz pierwszy widzi członka mężczyzny, kiedy pierwszy raz widzi akt masturbacji.

Przede wszystkim nie prosiła o te zdjęcia. Dostała je w ramach tzw. sekretu. Podkreśliłam też bardzo wyraźnie wyrażenia, które często mają miejsce w takich konwersacjach, ponieważ takie wyrażenia powinny być flagowane przez dostawców usług. Pokażę to za chwilę na przykładzie. W pewnym momencie Ania nie chce już stosować się do poleceń, ale już nie może, ponieważ sprawca posiada jej zdjęcia, które wysłane np. do grupy rówieśniczej będą ją narażały na wstyd, na poczucie przegranej, na problemy. Już to nie jest przyjemny sekret, ale jest to szantaż na tle seksualnym – zmuszanie do określonego zachowania. Bardzo proszę, żebyśmy mieli Anię w naszych myślach, bo Ania ma wiele twarzy. Ania może być koleżanką naszej córki z klasy, może być dzieckiem sąsiadki, bo nasze dzieci tak funkcjonują na ten moment.

Zanim o liczbach, Ania w tym wypadku miała siedemnaście lat. To jest część aktu oskarżenia w bardzo drastycznej sprawie. Myślę, że nawet nie powinnam czytać tych treści, bo sami państwo możecie się z nimi zapoznać. To jest to, co się dzieje. Tak wyglądają tego typu sprawy. Nie słyszymy o nich na co dzień. Zajmuje się nimi dość wąska kategoria specjalistów – policjantów, prokuratorów. Natomiast nie mówimy o nich wystarczająco często, bo też trudno jest posługiwać się takim językiem. Trudno wyobrazić sobie nam – ludziom skalę bestialstwa i skalę cierpienia, jakie jest po drugiej stronie.

Ania może mieć też jedenaście lat. To jest kolejna sprawa i kolejny fragment z tego samego aktu oskarżenia. Mam nadzieję, że ogląda nas prokurator, który prowadził tę sprawę, którego serdecznie pozdrawiam i gratuluję odwagi, ponieważ w tej sprawie został postawiony zarzut zgwałcenia w cyberprzestrzeni, czyli zgwałcenia bez wyraźnego kontaktu z dzieckiem, bez fizycznego kontaktu. Tak jak państwo widzicie, tego typu okoliczności zostały potraktowane jako zgwałcenie z uwagi na to, że miała miejsce ingerencja w ciało dziecka. Mówimy o dwóch jedenastoletkach. Bardzo chciałabym, żeby to to tutaj wybrzmiało. Taka jest perspektywa Ani – jedenastoletniej, siedemnastoletniej.

Teraz przejdźmy do liczb, bo za tymi liczbami jest nieskończona liczba takich dziewczynek. Każda z tych liczb to jest indywidualna tragedia dziecka o imieniu „Ania”. To są dane, które upubliczniło wiele organizacji międzynarodowych – Childlight czy National Center for Missing & Exploited Children. Ta druga organizacja prowadzi amerykańską hotline, czyli odpowiednik naszego „Dyżurnetu”. Jako jedyna monitoruje raporty od sektora prywatnego. Skala zachowań jest ogromna. Jeśli chodzi o fakty i liczby dotyczące tym razem obrazów, to mamy do czynienia z bezprecedensowymi pikami w każdej statystyce. Proszę zobaczyć, 36 mln raportów, które otrzymała ta infolinia w 2023 r., nie ma jeszcze danych za rok 2024 r., ale podejrzewam, że będą one jeszcze wyższe, jeżeli chodzi o same liczby co do zgłoszeń.

Bardzo potrzebne jest zastanowienie się nad kategorią nowych materiałów, czyli takich, które jeszcze nigdzie nie zostały sklasyfikowane przez żadną z 55 infolinii funkcjonujących na całym świecie. To znaczy, że materiały tego typu to materiały producenckie, czyli takie, które mogą dotyczyć dziecka wykorzystywanego w czasie rzeczywistym. Nie są to materiały historyczne, które krążą w internecie od dawna, ale materiały, które pojawiają się, ponieważ ktoś je upublicznił i np. mogą być podstawą szantażu. 140% to procentowa liczba wzrostu w ostatnich trzech latach takich raportów, kiedy infolinia przekazywała dane do organów ścigania, ponieważ dotyczyły dziecka znajdującego się w bezpośrednim zagrożeniu.

Jeśli chodzi o bardzo istotny wgląd w materiały szczególnej kategorii, czyli kategorii A – penetracja, sadyzm, bestialstwo, to tutaj brytyjska infolinia dysponuje bardzo cennymi danymi. Ona pokazuje skalę zjawiska w tzw. dark webie i mówi o liczbie ponad 3500 danych tego typu. Brytyjska infolinia zauważa też dzielenie się modelami sztucznej inteligencji, które pomagają kreować takie materiały. Pewnie zauważyliście państwo informację o tym, że istnieje też tzw. dark Chat GPT, który pozwala potencjalnemu sprawcy wytworzyć sobie taką konwersację, która zaprosi dziecko i będzie podsuwała temu sprawcy taką narrację, żeby była ona jak najbardziej skuteczna z jego punktu widzenia. Tego typu rozwiązania też już istnieją. Kolejne dane z tego samego miejsca, to dane dotyczące np. grupy wiekowej 3–6 lat. Myślę, że one mówią same za siebie i powinny nam uświadamiać to, że za tymi procentami jest znowu nasza Ania, znowu jest to dziecko, które ma charakterystyczną twarz, ma charakterystyczny kolor oczu, ma charakterystyczne włosy pewnego koloru, które być może jest kochane przez rodziców. Nie jest to prawidłowa teoria, że tego typu zachowania dotyczą dzieci zaniedbanych emocjonalnie, absolutnie nie. Najczęściej sprawca wybiera przypadkowe dziecko – takie, które jest zaciekawione konwersacją i wcale nie musi uciekać się do jakiejś szczególnie wyrafinowanej socjotechniki.

To jest moment rozwoju dziecka, ciekawości, eksplorowania własnej seksualności. Za tymi liczbami stoją dramaty poszczególnych postaci.

Teraz cofnijmy się w czasie. Cofnijmy się do momentu, kiedy zdjęcie Ani jest upublicznione przez sprawcę. Tutaj będę opowiadać o działaniu reaktywnym. Bardzo wyraźnie chcę je odróżnić od działania proaktywnego. Sprawca ma pierwsze zdjęcie Ani z jej intymnymi częściami ciała. Co robi? Upublicznia je w internecie i takie zdjęcie zauważa ktoś inny – użytkownik internetu, który zupełnie przypadkowo napotkał na takie treści np. w środowisku peer to peer. Taki użytkownik zgłasza np. URL, pod którym znajdują się tego typu treści. Zgłasza te treści do infolinii inhope, do polskiego „Dyżurnetu” w naszym lokalnym wydaniu i wtedy takie treści są oznaczone jako CSAM. To konkretne zdjęcie jest skategoryzowane jako przedstawiające treści, gdzie małoletni jest wykorzystywany seksualnie. Ale tu jest za późno, dlatego że to zdjęcie musi ktoś zauważyć. To zdjęcie funkcjonuje w cyberprzestrzeni do momentu aż zgłosi to inny użytkownik. Natomiast mamy do czynienia z działaniem proaktywnym. Tutaj jeszcze takie krótkie wyjaśnienie, jeżeli chodzi o to, na czym polega działanie reaktywne. Działanie reaktywne polega na przypisaniu zdjęciu wartości hash. Hash to nic innego jak kombinacja liter i cyfr. To jest główna podstawa do cross checkowania tych treści. Założmy, że zdjęcie Ani stwarza pytanie, czy ta treść jest znana, czy któryś podmiot na świecie ją widział. Zdjęcie Ani jest za pomocą algorytmów tłumaczone na hash. W tym samym momencie ktoś inny chce sprawdzić, czy to zdjęcie jest już gdzieś w bazie danych i porównuje tylko hash. Nie musi widzieć żadnego zdjęcia. Jeśli chodzi o bazy danych hash, które istnieją na świecie, to w 2023 r. miała miejsce bardzo zaawansowana kontrola danych zbieranych przez tę amerykańską organizację i okazało się, że poprawność kwalifikacji sięga prawie 100%. Mamy tutaj do czynienia z bardzo wiarygodnymi danymi.

Teraz działanie proaktywne, czyli takie, które może być ukierunkowane albo na grooming, czyli te zachowania, które wcześniej prezentowałam, albo na nowy CSAM, czyli nowe zdjęcie, które jeszcze nigdzie nie zostało obejrzone i przez nikogo nie zostało zakwalifikowane jako CSAM. Dlaczego jest to takie istotne? Dlatego że znowu z tyłu głowy mamy Anię, która czeka na pomoc. Jej zdjęcie być może funkcjonuje gdzieś w cyberprzestrzeni, ale nie musi czekać na to aż ktoś zgłosi je do infolinii. To jest działanie proaktywne. Mamy tutaj zapis wzięty z aktu oskarżenia. Widzicie państwo to kluczowe zdanie – „jeżeli nie przekażesz mi zdjęć, nie nagrzesz filmu, to upublicznisz zdjęcia”. Algorytmy, którymi operuje sektor prywatny, pozwalają na wychwycenie takich dialogów. Ale pozwalają też na wychwycenie nowych zdjęć Ani, czyli takich, które jeszcze nigdy nie były obejrzone. Takie treści są znowu zgłaszane do amerykańskiego centrum, które oczywiście powiadamia organy ścigania.

Bardzo krótko o roli sektora prywatnego. W tej chwili istnieje tylko i wyłącznie amerykański system, który tak działa. Istnieje on, dlatego że w Stanach Zjednoczonych amerykańskie podmioty, dostawcy usług z siedzibą w tym kraju są prawnie zobowiązani do tego, żeby raportować przypadki ujawnienia tzw. oczywistego CSAM. Natomiast nie ma prawnych wymogów dotyczących proaktywnych działań, czyli takich, które dotarłyby do Ani w pierwszej kolejności, zanim zdjęcie będzie zgłoszone przez użytkownika cyberprzestrzeni, zanim trafi właśnie do infolinii. Bardzo ważna, kluczowa dla nas informacja jest taka, że tak naprawdę większość z raportów otrzymywanych przez ten podmiot dotyczy zgłoszeń spoza Stanów Zjednoczonych.

Co to oznacza dla nas? Oznacza to, że teoretycznie 1600 podmiotów dostawców usług zarejestrowało, żeby składać takie raporty właśnie do amerykańskiej infolinii. W tym były to podmioty z naszego obszaru – z obszaru Unii Europejskiej. Ale tylko 16% z nich zdecydowało się na dobrowolne praktyki, czyli takie, kiedy podmiot nie jest zobowiązany właśnie tym federalnym prawem Stanów Zjednoczonych. Jak to działa w praktyce? Otóż działa tak, że tylko 245 podmiotów rzeczywiście raportowało w 2023 r., a 5 z nich odpowiadało za ponad 90% tych zgłoszeń. Jak państwo myślicie, które to pięć podmiotów? Zaraz powiem, zaraz rozwiążemy tę zagadkę. Natomiast to, o czym mówi to centrum, czyli National Center for Missing & Exploited Children mówi o tym, że bardzo często te raporty nie zawierają szczegółów, które pomogłyby działać organom ścigania. Dlaczego? Dlatego że znowu nie ma prawnych wymogów, które mówiłyby, jak mają wyglądać takie raporty. Posłużę się jeszcze jednym przykładem. Będzie nim sytuacja, kiedy wchodziła w życie dyrektywa ePrivacy. W Europie nastał popłoch wśród podmiotów sektora prywatnego, dlatego że niewiadomo było, jak ich zachowanie, czyli te dobrowolne praktyki, zostaną odczytane właśnie na gruncie tej dyrektywy ePrivacy i jeszcze jednego aktu w pakiecie, czyli electronic communication scout. Co się stało? Centrum to odnotowało ogromny

spadek w raportach z obszaru Unii Europejskiej. Był on widoczny w porównaniu sprzed wejścia w życie tej dyrektywy i po wejściu w życie. Dlaczego? Bo ta praktyka była niejasna. Nie była do końca precyzyjna, pewna. Jedynym sposobem, żeby można było kontynuować te praktyki, było tymczasowe odstępstwo od zapisów tej dyrektywy.

Rozwiązuję w tej chwili zagadkę, jeśli chodzi o te 5 podmiotów. Mamy tutaj przedstawione liczby: Facebook – 17 mln, Instagram – 11 mln, Google, Snapchat... Ale przecież dzieci są obecne w mediach społecznościowych. Dlaczego Twitter to tylko 600 tys.? Dlaczego Tik Tok to też 600 tys.? Dlaczego Discord to tak mało? Przecież dzieci tam są. Dzieci nie są obecne w aplikacjach, które nie pozwalają na komunikowanie się, tylko są właśnie obecne w aplikacjach z komunikatorami.

Znowu problem dotyczący raportowania. Rola dostawców usług, hostingu lub łączności interpersonalnej jest jeszcze bardziej widoczna w świetle badań fińskiej organizacji Protect Children. Tutaj mamy podział na to, jak działają sprawcy. Ta organizacja zadała w zasadzie dwa pytania – w jaki sposób się kontaktują... Drugie pytanie dotyczyło tego, gdzie znajdują CSAM? Proszę zobaczyć, że social media, to jest dalej góra tego diagramu. No właśnie, tam są dzieci. Teraz, jeśli wrócimy do danych dotyczących raportów, to chyba mamy do czynienia z jakąś sprzecznością, a co najmniej luką, którą trzeba zaadresować.

Tę lukę ma za zadanie zaadresować wniosek, nowa regulacja proponowana w maju 2020 r. – wniosek dotyczący rozporządzenia ustanawiającego przepisy, mające na celu zapobieganie niegodziwemu traktowaniu dzieci w celach seksualnych i jego zwalczanie. Jest to próba uregulowania na terenie Unii Europejskiej podobnego schematu dostarczania raportów, jak ten, który funkcjonuje w Stanach Zjednoczonych. Dlaczego? Bo przede wszystkim nie chcemy być zależni tylko od jednego systemu, dlatego że w Europie dzieje się równie dużo, co w Stanach Zjednoczonych. A przede wszystkim, dlatego żeby organy ścigania mogły właściwie reagować. Na ten moment mamy do czynienia z pewną fikcją sprowadzoną nierzadko do narracji, która polega na wyborze pomiędzy prawem do prywatności użytkowników cyberprzestrzeni, a prawem dzieci do ochrony. Czy ta narracja jest właściwa? Według mnie nie, dlatego że w podobny sposób da się zabezpieczyć prawa tego dwojakiego rodzaju. Apelują o to też osoby, które doświadczyły wykorzystywania seksualnego, szczególnie w szyfrowanym obszarze. Te osoby apelują w ten sposób, że nazywają ten obszar „niebem dla pedofilów”, może nie jest to fortunne określenie, ale odbija się ono w mediach społecznościowych. Sama nie nazwałabym w podobny sposób tego typu zjawiska, natomiast wydaje mi się, że warto słuchać i warto wyprowadzać refleksję z tego, jak mówią o tym osoby, które doświadczyły tego zjawiska.

Krótkie spojrzenie na to, gdzie właściwie jesteśmy. Z jednej strony patrzymy na system amerykański, a z drugiej mamy do czynienia z firmami, które otwarcie mówią, że one wykorzystują swoje technologie do tego, żeby zapewniać higienę swoich usług i wykorzystują te technologie, które na gruncie rozporządzenia budzą pytania, stwarzają problem, jak daleka jest ingerencja w sferę prywatności użytkowników cyberprzestrzeni? To jest wycinek ze strony Microsoft i on wyraźnie mówi, że nie tylko używa systemu hashowania, ale jak sami tutaj napisali, używa text-based classifiers. To jest właśnie to, w jaki sposób możemy wykryć konwersację Ani ze sprawcą, zanim dojdzie do najgorszego. To się już dzieje, tylko to, co chcemy osiągnąć, to chcemy uregulować to na tyle, żeby skutecznie działać, żeby organy ścigania dostawały takie pakiety informacji, które pozwolą na podjęcie właściwych działań, ale wcześniej, żeby rola dostawców usług była taka, że to po ich stronie będzie wykrywanie tego typu zachowań. Microsoft mówi wyraźnie – my to robimy, wykrywamy konwersacje, wykrywamy grooming, czyli to zachowanie polegające na uwodzeniu i równie dobrze działamy w obszarze posługiwania się hashami. Przyznajmy wreszcie, że to się dzieje, ale nie robią tego wszyscy – system dobrowolny się nie sprawdził. Nie działa system polegający właśnie na pozostawieniu wyboru dostawcom. Jak państwo widzieli, taki niewielki odsetek firm, które rzeczywiście raportują to jest zbyt mało, żeby ten system był szczelny i skuteczny.

Podsumowanie. Nasze wydarzenie jest jednym z wielu wydarzeń opartych na przypomnieniu nam wszystkim o Konwencji o prawach dziecka. Z wielkim zainteresowaniem patrzyłam na ulotkę opracowaną przez UNICEF. Poszczególne artykuły są interpretacją właśnie z tej ulotki. Mówimy też o prawie do prywatności w wykonaniu samych dzieci. Mówimy o tym prawie w art. 16 w taki sposób, że nikt nie ma prawa do ingerencji w twoją prywatność, chyba że robi to ze względu na dobro twoje lub twoich bliskich. Chyba najwyższym naszym zobowiązaniem zarówno prywatnym, jak i instytucjonalnym jest dbanie o dobro dziecka i ochronę przed wykorzystywaniem seksualnym. To jest to, co obiecujemy dzieciom. A jak dalecy jesteśmy

od tego? Realia mówią same za siebie. Przyszła mi też do głowy metafora, czy nie ma tutaj podobieństwa z odpowiedzialnością za zaniechanie. Jeśli nie pomagamy na ulicy człowiekowi, który jest ofiarą bójki, kiedy widzimy takie zdarzenie, to Kodeks karny zobowiązuje nas do tego, żeby zainterweniować. Oczywiście tam są pewne warunki, kiedy nie powinniśmy tego robić, ale porównajcie państwo bójkę na ulicy i tę Anię, która jest przerażona, wystraszona, sama, czekająca na pomoc, na kogoś, kto zauważy to zachowanie i robi to na poziomie technologicznym.

Skończmy z przesłaniem, że nasze dzieci są naszą teraźniejszością i przyszłością. To jest przesłanie ze strategii unijnej. Miejmy je z tyłu głowy, kiedy przyjdzie nam decydować o losach tego wniosku. Sama nie umiałabym lepiej powiedzieć o tym, co jest dla nas najważniejsze. Bardzo dziękuję.

Przewodnicząca poseł Monika Rosa (KO):

Bardzo dziękuję za to wstępne wystąpienie, które pokazuje jak krytyczny jest moment, w którym jesteśmy – wzrostu skali seksualnego krzywdzenia dzieci i wzrostu liczby materiałów wzrastających poprzez takie krzywdzenie seksualne. Miejmy taką świadomość, że to się dzieje wirtualnie, to jest taka realna krzywda, taka sama, jak ta, która wydarza się namacalnie w realnym świecie. Bardzo dziękuję pani Katarzynie Staciwie. My, wspólnie z panią Katarzyną, z Państwową Komisją do spraw przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15, z Fundacją Dajemy Dzieciom Siłę i innymi partnerami społecznymi, pracujemy też w ramach 35-lecia Konwencji o prawach dziecka. Ten element dotyczący zwalczania CSAM jest naszym elementem w ramach tej inicjatywy społeczno-parlamentarnej.

Teraz oddaję głos dla Państwowej Komisji do spraw przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15. Pani Joanna Napierała przedstawi studium przypadku, a pan Konrad Ciesiołkiewicz przedstawi jeszcze dane z innych raportów.

Przypominam jedną rzecz, musimy zakończyć naszą Komisję o godz. 13.00, bo o 13.15 są głosowania, więc prosiłabym o pewną dyscyplinę czasową, żebyśmy mieli jeszcze czas na odniesienie się ministerstwa, a przede wszystkim na wysłuchanie gości z zagranicy. Bardzo proszę.

Przedstawiciel Państwowej Komisji do spraw przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15 Joanna Napierała:

Dzień dobry państwu. Nazywam się Joanna Napierała. W Państwowej Komisji koordynuję Departament Postępowań Indywidualnych, czyli tych, które są prowadzone na etapie postępowania przygotowawczego bądź przed sądem. Jako studium przypadku wybrałam dla państwa jedną sprawę, która w zasadzie w najbardziej syntetyczny sposób może pokazać możliwe ryzyka i w zasadzie wady Kodeksu karnego – prawa karnego prawa materialnego i Kodeksu karnego wykonawczego.

Ta sprawa obejmuje co najmniej piętnastu pokrzywdzonych, w tym dziesięciu w wieku 10–14 lat. Sposób działania tego sprawcy jest w zasadzie jednakowy wobec wszystkich pokrzywdzonych. W zasadzie za każdym razem używa telefonu i aplikacji np. Messenger, Snapchat, Instagram, Whatsapp. Sprawca buduje zaufanie, żeby była jasność, to budowanie zaufania dzieci nie trwa miesiącami, to jest raptem kilka dni, te znajomości najdłużej trwały dwa miesiące. Sprawca nakłania pokrzywdzone, używa kamer, nagrywa małoletnie, kiedy dokonują czynności, o które prosi i ponadto później rozpowszechnia zdjęcia lub nagrania pozostałym osobom.

Pokrzywdzona nr 1, którą będziemy tutaj omawiać, miała czternaście lat. Wobec niej sprawca najpierw rozpoczął tradycyjne budowanie zaufania, a następnie prosił o zdjęcia. Najpierw były to zdjęcia w zasadzie tylko elementów ciała, a następnie całego ciała. Na końcu były to zdjęcia części intymnych ciała. Chcę państwu przedstawić, że wykorzystałam fragmenty aktu oskarżenia i protokołów z zeznań pokrzywdzonych, a także ich rodziców. One momentami mogą być gorszące, ale myślę sobie, że jeżeli dzieci są narażone na takie treści, to tym bardziej państwo powinniście mieć świadomość, jakie otrzymują treści. Dziewczyna mówi tak: „Ja ulegałam, bo nie chciałam mieć człowieka na sumieniu. Myślałam, że on się zabije.”. Przez to, że sprawca stworzył taką więź zaufania i zakochania tej dziewczyny, żeby wyzyskać od niej kolejne nagrania z czynności seksualnych, stosował szantaż i groził jej, że podetnie sobie żyły. Rzeczywiście robił to przed kamerą. W związku z tym ona miała realne obawy, że sprawca dokona zamachu na swoje życie. Finalnie zmusił tę dziewczynę do wysyłania kolejnych zdjęć, a na końcu do prezentowania swoich miejsc intymnych za pośrednictwem kamery internetowej. Z tych czynności wykonywał zrzuty z ekranu. Dziewczynka w protokole

używa takich słów: „Ja nigdy wcześniej nie włożyłam sobie palców do pochwy. On raz na żywo mnie obserwował, jak to robię.” Co to oznacza? Dziewczyna nawet nie miała świadomości ani pojęcia o tym, jakiego rodzaju czynności seksualne ona może wykonywać w przeszłości albo w ogóle wykonywać to, o co ktoś może prosić. Sprawca proponował także odbycie stosunku seksualnego. W przypadku tej pokrzywdzonej, sprawcy zarzucono art. 197 Kodeksu karnego, czyli zgwałcenie, doprowadzenie za pomocą groźby do innych czynności seksualnych. Tak jak wspomniała wcześniej w swojej prezentacji Katarzyna – to się dzieje i to w tej chwili jest kwalifikowane jako przestępstwo zgwałcenia. Proszę sobie wyobrazić, że w uzasadnieniu do wyroku, sąd wskazywał, że okolicznością łagodzącą do wymiaru kary jest to, że te czynności nie są z kontaktem fizycznym i w związku z tym nie są tak brutalne.

W przypadku drugiej pokrzywdzonej, która ma trzynaście lat, ponownie miało miejsce nawiązywanie relacji przez komunikator, są rozmowy. Sprawca zaczyna pytać o jej doświadczenia seksualne. Wielokrotnie namawia do wysyłania zdjęć. Proponuje nawet, gdzie mogą odbyć stosunek seksualny. Nakłania do wysyłania zdjęć gołego ciała, do wysyłania zdjęć jej narządów intymnych. W ostateczności, żeby uzyskać kolejne zdjęcia i nagrania, grozi jej zgwałceniem i opublikowaniem zdjęć w internecie.

Kolejna pokrzywdzona to dwunastolatka. Ponownie jest internetowy związek za pośrednictwem Facebooka, Messengera, Instagrama. Sprawca nakłania do wysyłania najpierw zdjęć stóp, a później zdjęć narządów intymnych. Wysyła zdjęcia swojego członka. Wykorzystuje uczucie pokrzywdzonej. Straszy zerwaniem. W związku z tym małaletnia po raz kolejny wysyła zdjęcia. W ten sposób doprowadza ją co najmniej raz do wykonywania innej czynności seksualnej, tu jest to masturbacja przy zapisie wideo. Dziewczynka to wysyła.

Jeszcze dodam, że w stosunku do tych wszystkich dziewcząt wizerunek na zdjęciu przedstawia dzieci odpowiednie do ich wieku. One każdorazowo w znajomości przedstawiały, informowały o swoim wieku.

Kolejna pokrzywdzona to dziesięcioletka. Sprawca ponownie nawiązuje kontakt za pośrednictwem komunikatora. To jest raptem kilka dni, żeby zbudować jej odpowiednie zaufanie, żeby przekonać dziewczynkę do tego, że należy jej to wysłać. W tym przypadku najpierw nastąpiło wysłanie zdjęć swojego ciała, później części intymnych. Naleganie na to, żeby nagrała wideo, na którym dotyka swoich miejsc intymnych. Dziewczynka to robi. Możecie sobie państwo przeczytać fragment z protokołu.

Kolejna pokrzywdzona to dwunastolatka. Ponownie nastąpiły bardzo szybkie prośby o zdjęcia nagiego ciała, narządów intymnych w zamian za obietnicę kupna sprzętu elektronicznego. Dziewczynka z nadzieją, że rzeczywiście otrzyma taki sprzęt, nagrywa części swojego ciała.

Pokrzywdzona nr 6 – jedenastolatka. Bardzo szybko pojawia się temat seksualny. Sprawca dopytuje, czy dziewczynka ma za sobą już doświadczenia seksualne, czy wie co to jest „palcówka”. Skoro dziecko może usłyszeć te słowa, to myślę, że państwo też powinni mieć świadomość tego, jak to brzmi.

Jakie są skutki dla tych dziewcząt? Część z nich miała myśli samobójcze, próby samobójcze. Mają stwierdzony stres pourazowy. Wymagają terapii, na którą rodzice nie zawsze mają środki finansowe.

Jeśli chodzi o fragmenty zeznań rodziców, to możecie się też zapoznać z tymi trzema. Dziecko unika kontaktu z internetem, byliśmy u psychologa, ale ono nie chce rozmawiać, jest bojaźliwe. Jeden z rodziców powiedział też, że obawiał się, że gdyby te zdjęcia wypłynęły i ona by się o tym dowiedziała, to prawdopodobnie nie dojechałaby do domu.

Jakie są skutki dla sprawcy? Chyba najbardziej łagodne ze wszystkich możliwych, dlatego że przy piętnastu pokrzywdzonych orzeczono mu karę łączną 5 lat 6 miesięcy pozbawienia wolności. Dodam, że sprawca ma też możliwość ubiegania się o warunkowe przedterminowe zwolnienie po odbyciu połowy kary. Z praktyki zawodowej wynika, że wątpliwe jest, żeby je tak wcześniej uzyskał, ale jest to możliwe. Orzeczono w stosunku do niego zakaz zbliżania się do pokrzywdzonych na 10 lat i zakaz kontaktowania. Kontakt i tak był internetowy, więc zasadniczo jest to dosyć fikcyjny zakaz. Orzeczono zakaz wykonywania działalności związanej z edukacją. Pan był bezrobotny, w związku z tym wątpliwe jest, że w przyszłości będzie wykonywał tego rodzaju zawody. No i orzeczono też zadośćuczynienie od tysiąca do trzynastu tysięcy. Nie ma niczego, nie ma środków karnych, które zabezpieczyłyby dzieci przed krzywdzeniem w internecie. One dotyczą tylko i wyłącznie kontaktu fizycznego. Na trzydzieści wyroków znalazłam dwa, w których sąd zastosował środek karny w postaci zakazu kontaktowania się

z małoletnimi przez komunikatory i drugi, w którym przy zawieszeniu kary pozbawienia wolności, sąd zastosował taki obowiązek. Myślę sobie, że dobrze, jest jakiś trend i trzeba to kontynuować, trzeba nakłaniać sądy, żeby orzekały takie środki. Myślę sobie też, dlaczego sądy tego nie stosują. Dlatego że nie można tego wyegzekwować.

Co w związku z tym może zrobić państwo? Analizując ten przypadek zastanawiałam się, jak można wzmocnić instytucje prawa karnego. Byłaby taka możliwość, tylko ona z kolei chroni przed kolejnym popełnieniem przestępstwa tylko przez sprawców, którzy zostali już ukarani. Można by ewentualnie rozwijać taką myśl, żeby zastosować elektroniczny system dozoru sprzętów elektronicznych, ale to i tak nigdy nie będzie wystarczające, bo w zasadzie nie można ograniczyć możliwości korzystania z kolejnych sprzętów, które może nabyć, bo tego nikt nie kontroluje. Kurator nie będzie miał wglądu w tego rodzaju aktywności. Druga rzecz to jest edukacja małoletnich. Jak wiemy, jest ona ograniczona, a przynajmniej dostęp do niej nie jest faktycznie powszechny, bo decydują o tym rodzice. Można zastanowić się nad minimalnym wiekiem korzystania z social mediów. Chyba najbardziej skuteczne wydaje się wychwytywanie treści szkodliwych tak, żeby bezpieczne były nie tylko dzieci, które doświadczyły już przemocy, skrzywdzenia w sieci, ale też te dzieci, które jeszcze tego nie doświadczyły, a mogłyby doświadczyć wobec sprawców dotychczas niekaranych. Dziękuję bardzo.

Przewodnicząca poseł Monika Rosa (KO):

Bardzo proszę.

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

Bardzo dziękuję. Nazywam się Konrad Ciesiołkiewicz. Po tych doskonałych wystąpieniach pani Joanny Napierały wiceprzewodniczącej Państwowej Komisji i pani Katarzyny Staciwy w tym wprowadzeniu, może powiem o kilku takich dosłownie uzupełniających aspektach. Nie wiem, czy państwo zwróciliście uwagę, ale prezentowane przed chwilą przez panią Joannę Napierałą osoby pokrzywdzone, poza jedną, były w wieku, w którym teoretycznie w ogóle nie powinno ich być na platformach tzw. społecznościowych, ani w komunikatorach prowadzonych w zasadzie w większości te same platformy. Według regulaminu tych platform, wiek dostępu do nich to trzynasty rok życia. W tej samej sali dziesięć dni temu prezentowaliśmy wyniki rynkowych badań „Internet dzieci”, w których pokazywaliśmy, jaki jest w Polsce stan osób małoletnich korzystających dzisiaj z aktywności sieciowej, aktywności internetowej. 58% osób w wieku 7–12 lat jest obecne na platformach społecznościowych. 58% to jest 1,6 mln dzieci. Przy wyłączeniu YouTube, ponieważ jest to platforma, która faktycznie posiada możliwość aktywności dzieci młodszych pod kontrolą rodzicielską, to jest 1,4 mln dzieci. To jest także ponad 50% korzystających z tzw. kategorii serwisów erotycznych, a mówiąc wprost chodzi o treści pornograficzne. To nie jest żadne odkrycie, bo wiemy z badania „Nastolatki 3.0”, że 1,3 mln nastolatków regularnie korzysta z najbardziej popularnego serwisu pornograficznego, a 800 tys. korzysta z dwóch najbardziej popularnych serwisów hazardowych. Jak wszyscy wiemy, serwisy hazardowe są dostępne dla osób od osiemnastego roku życia z racji ryzyk, uzależnień behawioralnych, które są szczególnie niebezpieczne w tym właśnie wieku. Zresztą to samo dotyczy serwisów erotycznych.

Pewnie, jak wszyscy tutaj wiemy, przypuszczamy, że najbardziej popularną platformą społecznościową jest Tik Tok, na którym mamy 760 tys. dzieci w wieku 7–12 lat. Ich wszystkich teoretycznie tam nie ma. Także teoretycznie nie ma tych wskazanych osób pokrzywdzonych, dlatego że w raportach, które otrzymują branże, które otrzymujemy my jako obywatele i obywatelki, a także otrzymują organy państwa, które także są reprezentowane tutaj na sali, wszystkie osoby, które tutaj pokazano są to osoby z wyższym statusem wiekowym. Natomiast cała branża zarówno platform, jak i branża reklamy i marketingu, wszystkie podmioty gospodarcze doskonale wiedzą, że to są dzieci. Inaczej nie mielibyśmy tych danych. Dane, które pokazaliśmy dziesięć dni temu, są danymi doskonale znanymi od lat i badanymi oraz regularnie raportowanymi przez panel badawczy polskiego internetu od ponad 20 lat, polskich badań internetu oraz Geniusa – pewnie doskonale państwu znane pop-upy, które raz na jakiś czas wyskakują na ekranach naszych komputerów. To nie są nowe dane. To są nowe dane z punktu widzenia opinii publicznej i naszej tutaj. Na to chciałem zwrócić uwagę, że również dzieci, których historie opowiadały zarówno Katarzyna, jak i Joanna, są dziećmi, których teoretycznie według wszelkich raportów tam nie ma, a wiemy, że są. Podmioty, które za to odpowiadają, zarządzający tymi podmiotami, także o tym wiedzą. Nie chodzi mi w tej chwili o to, żeby szukać

i upatrywać w nich kozłów ofiarnych, ale takie są fakty. Odpowiedzialność za to powinna być wzięta w pierwszej kolejności, właśnie za te podmioty, które stanowią podstawowe środowisko życia i rozwoju młodych ludzi, którzy spędzają tam wiele godzin dziennie. Na samej platformie, powiem enigmatycznie, o chińskich korzeniach dzieci spędzają średnio 2 godziny 11 minut dziennie, logując się po kilkadziesiąt razy dziennie. Logowanie się 20 razy dziennie, to jest średnia logowania się do tej aplikacji przez dzieci w wieku 7–12 lat, czyli tych, które teoretycznie nie istnieją na tej platformie. Powtarzam się, więc może nie będę tego więcej powtarzał.

Jeszcze uzupełniając chciałem powiedzieć do tego, co powiedziała sama pani Katarzyna Staciwa, opierając się właśnie na analizie dla Komisji sejmowej autorstwa pani Katarzyny Staciwy, na której widać, że także przejrzała dane Internet Watch Foundation, która proaktywnie przeszukuje sieć. To jest kategoria wiekowa grupy dzieci w wieku 7–10 lat. Ponieważ Katarzyna tego nie powiedziała, to patrząc bokiem, pozwolę sobie na to. To jest kategoria materiałów self generated content, czyli materiałów, które wytwarzają same dzieci. Historie, o których opowiadała Joanna są również historiami, w których dzieci wytwarzają kontent. Nie wytwarzają go samodzielnie, tak należy zakładać i tak zakładają zarówno IWF, jak i WeProtect, i NCMEC, że są to dzieci, które robią to pod wpływem delikatnie mówiąc manipulacji, a często także szantażu i zastraszania. Pomiędzy 2019 r. a 2023 r. obserwujemy wzrost materiałów tego rodzaju, ukazujących krzywdzenie, ukazujących je w kontekście seksualnym. Zwróciła na to uwagę Katarzyna Staciwa. Przeglądając dziesiątki tabel bardzo często nie zwracamy na to uwagi. To jest wzrost o 1816% z jednoczesną informacją IWF o tym, że mocno rośnie dynamika kategorii wiekowej 3–6 lat, która związana jest z wielogodzinnym używaniem aplikacji dla osób powyżej trzynastego roku życia, a także niektórych powyżej osiemnastego roku życia, przez dzieci w wieku 3–6 lat.

Rośnie również liczba materiałów wrzucanych do sieci, dzielących się na komunikatorach, czyli naszych Messengerach, Whatsappach i innego rodzaju komunikatorach innych aplikacji, dla grupy dzieci w wieku 3–6 lat, które są tam uwodzone i wydaje im się, że to jest zabawa. Wydaje mi się, że te dane powinny zapaść nam w pamięć szczególnie, kiedy uwzględnimy badanie i estymację „WeProtect” znaną kilkorgu z państwa, jeżeli chodzi o raport. 69% dzieci w Polsce doświadczyło jednej z czterech form, które są tutaj pokazane, tzw. krzywdzenia seksualnego w sieci. Nie są to dane, które odbiegają od sześciu innych badanych krajów w tym samym badaniu. Ale to, co odbiega w polskich warunkach i czym się wyróżniamy, to jest najwyższy wskaźnik braku zaufania do zaufanego dorosłego, do którego zwraca się dziecko w sytuacji, kiedy doświadcza trudnej sytuacji, także sytuacji krzywdzenia w sieci. Myślę, że to nam wszystkim powinno dać także sporo do myślenia. To był taki komentarz uzupełniający.

Dlaczego stare materiały są tak ważne? Dlaczego materiały, o których mówiła Katarzyna są tak ważne? Być może to dzisiaj jeszcze padnie, ale według instytucji kanadyjskiej, 70% dzieci, które doświadczyło krzywdzenia seksualnego i wiedzą, że zostało to uwiecznione na zdjęciu lub materiale wideo, często do końca swojego życia żyje w nieustannym poczuciu lęku przed tym, że zostanie to ujawnione. Niestety w 30% tak się stanie. Oznacza to, że potrzeba nieustannego czyszczenia sieci z materiałów, które są już czyszczone, ale potem ktoś je znowu wrzuca czy to z dark webu albo znowu wypływają. Ta potrzeba jest bardzo ważna. To nie jest ten aspekt ratowania dziecka, gdy krzywda dzieje się tu i teraz, ale ratowania dobrostanu człowieka, często dorosłego, przez kilkadziesiąt kolejnych lat jego życia.

W większości tych sytuacji rzeczywiście mieliśmy do czynienia z groomingiem, czyli z uwodzeniem. Joanna mówiła, że te historie w najdłuższym odcinku czasowym trwały dwa miesiące. To jest bardzo długo. We Protect, który badał uwodzenie w sieci w grach online... Mówimy sobie to uczciwie powiedzieć i jeszcze raz powtórzyć, że dzisiaj platformy społecznościowe oraz gry online są głównym miejscem krzywdzenia seksualnego, do którego dochodzi, jeśli chodzi o dzieci. Średnia, która została podana przez WeProtect to jest 45 minut. To nie są dwa miesiące, to jest średnia. Według badania i raportu WeProtect, najdłuższy czas uwodzenia w grach online to jest 28 dni. Rekord to 19 sekund. Co to oznacza? Oznacza to, że w tym czasie dochodzi do granicy kontaktu o charakterze zdecydowanie seksualnym, gdzie dochodzi do dialogów o charakterze seksualnym, gdzie dochodzi do wymuszania materiałów zdjęciowych, wideo. Rekord – 19 sekund, średnia – 45 minut, najdłuższy czas – 28 dni. Można powiedzieć, że materiały, o których mówiła Joanna, zawyżają tę średnią. Warto mieć na uwadze, jak bardzo skrócił i skraca się ten czas budowania wiarygodnych informacji o sobie przez dorosłego, który krzywdzi.

Dane, które już widzieliśmy, bo mówiła o nich Katarzyna i jednocześnie pokazują, co jest dzisiaj głównym miejscem krzywdzenia i gdzie tego rodzaju materiały, o których dzisiaj rozmawiamy, są wyszukiwane. Sami potencjalni sprawcy szukający tych materiałów mówią, że 77% z nich znajduje je w serwisach otwartych, w otwartym internecie. Nie potrzebują do tego dark webu, wystarczą im do tego serwisy pornograficzne, które również, jako ekosystem, niestety posiadają w swojej przestrzeni bardzo wiele materiałów absolutnie przestępczych, czyli tych, które pokazują krzywdzenie dziecka – CSAM. Są to także komunikatory oraz platformy społecznościowe. Dlatego właśnie tak bardzo ważne jest uświadomienie sobie, że godzenie się na ten stan rzeczy, jeżeli chodzi o platformy... Nie będę przedłużał, bo przewodnicząca wyłączy mi za chwilę mikrofon. Sprawa jest bardzo poważna, bo spełniają wszelkie kryteria przemocy o charakterze instytucjonalnym. My nie rozmawiamy o przemocy, która jest enigmatyczna lub efemeryczna, ona jest zarządzana przez konkretne przedsiębiorstwa. Decyzje na temat regulacji w tym zakresie podejmują decydenci, czyli parlamenty konkretnych państw Unii Europejskiej, organizacji międzynarodowych. Śledząc taką ścieżkę, ja już z państwem nie będę przechodził tego śledzenia, bo już o tym rozmawialiśmy i jeszcze wielokrotnie będziemy do dyspozycji... Kiedy weźmiemy pod uwagę czy jest świadomość wśród tych podmiotów i tego ekosystemu na temat tego stanu rzeczy – tak, jest. Jaka jest zatem postawa? Czy jest dokonywany właściwy wysiłek w celu ochrony? Nie, nie jest wykonywany właściwy wysiłek. Czy na dzisiaj są podejmowane właściwe, konkretne działania? Na dzisiaj tych działań nie mamy. Jest próba uregulowania ich po stronie Unii Europejskiej. Jaki jest tego skutek? Na dzisiaj tego skutku nie widzimy. System opiera się na totalnym wolontariacie. Według mojej najlepszej wiedzy oznacza to, że dane, o których powiedziała Katarzyna, że dane nie są najbardziej precyzyjnie powiedziane na dzisiaj, ponieważ według mojej wiedzy Meta nie informuje dzisiaj, nie raportuje w przestrzeni Unii Europejskiej. To oczywiście wynika również z prawa europejskiego. Ci najwięksi informują, ale informują o tym, co uznają za właściwe do poinformowania. W skrócie rzecz ujmując, nie mamy dzisiaj nawet przekonania, że nawet te firmy, które informują i raportują, to słusznie i dobrze, że to robią, ale dzisiaj nie ma instrumentów, które sprawdziłyby, na ile to wszystko jest i na ile są to właściwe treści. Dziękuję bardzo.

Przewodnicząca poseł Monika Rosa (KO):

Bardzo dziękuję.

Teraz bardzo proszę, przedstawiciel Komisji Europejskiej. Pan Antonio Labrador Jimenez.

Przedstawiciel Komisji Europejskiej Antonio Labrador Jimenez:

Dzień dobry. Przepraszam, że nie będę mówić po polsku. Dziękuję za zorganizowanie tej dyskusji. Chciałbym powiedzieć parę słów na temat propozycji ustawodawczej. Jest to jedna z kilku inicjatyw Komisji Europejskiej na rzecz przeciwdziałania tego rodzaju przestępczości. Dochodzi również do analizy i przeglądu prawa karnego z uwzględnieniem nowych zjawisk, takich jak treści generowane przez sztuczną inteligencję, wymagane działania od osób współpracujących z dziećmi itd.

Proponujemy skupienie się na dwóch wątkach ustawodawczych. Po pierwsze, chodziłoby o to, żeby powstał nowy europejski ośrodek do spraw przeciwdziałania tego rodzaju przestępczości. Taki ośrodek miałby nasilić zwalczanie tego rodzaju przestępczości w Unii Europejskiej. Jeśli nadchodzi zgłoszenie od podmiotu prywatnego, to trzeba upewnić się, czy jest to raport poprawny, czy nie zawiera błędów, czy jest to zgłoszenie, które może stać się podstawą dalszych działań. To będzie również duży zasób wiedzy, który zostanie zgromadzony. Drugie działanie będzie polegało na nałożeniu pewnego obligo na podmioty prywatne w zakresie przeciwdziałania i rozpowszechniania tego rodzaju materiałów i przeciwdziałania groomingowi. A więc wykrywanie, raportowanie, usuwanie czy też blokowanie, to wszystko będą działania wiążące się z obliżem prawnym.

Chciałbym skupić się na może kluczowej sprawie. Rozporządzenie zawiera różne kierunki działania. Większość z nich została już uzgodniona. W Radzie, w Parlamencie Europejskim nie budzą one kontrowersji, ale są tematy wrażliwe. Mianowicie jest to wykrywanie treści tego rodzaju w prywatnej komunikacji, dlatego że to działanie narusza istotne prawa. Z jednej strony mamy prawa dziecka, prawa do ochrony, prawo do integralności, prawo do przeciwdziałaniu poniżającemu traktowaniu. Z drugiej strony mamy prawo do prywatności i prawo do ochrony danych osobowych. Prawdopodobnie największe naruszenie prywatności to właśnie dystrybucja, rozpowszechnianie materiałów pornografii dziecięcej. Oczywiście dzieje się to bez

zgody dzieci. Mamy także prawa podstawowe dotyczące wszystkich użytkowników internetu – prawo do prywatności, prawo do ochrony danych osobowych. Trzeba pamiętać, że żadne z tych praw podstawowych nie ma charakteru bezwzględnego, absolutnego. Trzeba jakoś zważyć i zrównoważyć fundamentalne i podstawowe prawa dziecka z jednej strony i z drugiej strony, równie ważnej, prawa podstawowe, jak prawo do prywatności innych użytkowników.

Dlaczego wykrywanie w prywatnej komunikacji jest tak ważne? Tutaj leży istota problemu. Jeśli sprawcy wymieniają materiały związane z pornografią dziecięcą, to robią to kanałami prywatnymi, zwykle szyfrowanymi, poddanymi enkrypcji, żeby trudniej było ich złapać. Ponad 80% zgłoszeń z sektora prywatnego to właśnie raporty dotyczące prywatnej komunikacji. Chciałbym również powiedzieć, że w ciągu ostatnich lat czterokrotnie wzrosła liczba zgłoszeń na temat groomingu czy również wymuszania informacji. Ma to miejsce w pierwszych godzinach kontaktu. Grooming to bardzo ekstremalna forma przestępczości, ma również niezmiernie przemocowe, drastyczne formy, co pokazują te zgłoszenia. Wykrywanie w prywatnej komunikacji jest ważne, bo być może jest to jedyny sposób przeciwdziałania dalszemu wiktymizowaniu dzieci. Dzieci są zbyt małe by rozumieć, że są wiktymizowane, że stają się ofiarami i że mogą skontaktować się z organami ścigania. Opiekunowie, rodzice także nie zgłaszają tych rzeczy, ponieważ zwykle o tym nie wiedzą. Opiekunowie, rodzice zwykle nie wiedzą, że ma miejsce takie niegodziwe traktowanie ich dziecka, więc nie kontaktują się z Policją. Jedyny sposób ochrony dziecka przed dalszym poniżającym traktowaniem jest wykrywanie obrazów w momencie, kiedy sprawcy je dystrybuują. Wtedy można to zgłaszać, wtedy użytkownicy widzący te obrazy, te treści mogą je zgłaszać. Rzeczywiście od piętnastu lat wykrywane są tego typu w prywatnej komunikacji, więc mamy już silne dowody pokazujące setki, tysiące dzieci w Unii Europejskiej, w tym w Polsce, które zostały uchronione przed dalszą wiktymizacją właśnie dzięki temu, że zgłoszenia dotyczyły prywatnych form komunikacji. Takie działanie ma również skutek prewencyjny. Jeśli tego typu obrazy, treści znikają z obiegu, to osłabia się również popyt na nie. Jeśli ktoś korzysta z tego typu treści, to chce eskalować, chce więcej takich materiałów, a rosnący popyt przekłada się na coraz większą ilość takich treści. Prawie połowa osób szukających tego typu materiałów stara się również fizycznie zwiktymizować dziecko. Tego typu działania mają również skutek prewencyjny, poza tym, że chronią, ratują konkretne dzieci.

Dzisiaj zgłoszenia mają charakter wolontaryjny, dobrowolny, więc zgłoszenia dotyczą tego, co dany podmiot chce zgłosić z zakresu, jaki chce pokazać i przypadków, jakie chce odkryć. Tylko 5 firm odpowiedzialnych jest za ponad 90% wszystkich zgłoszeń. To oznacza, że większość podmiotów nic nie robi w tej sprawie. Rozporządzenie będzie wymagać, będzie to obbligo prawne wykrywania tego typu treści. Kwestie, kiedy i co wykrywać będą oczywiście ograniczane konkretnymi warunkami, parametrami, nadzorem sądowym. Będzie potrzebne stworzenie tych samych jasnych warunków dla wszystkich graczy tego rynku.

Reasumując, co robią, a czego nie robią technologie wykrywania? Technologie wykorzystane do wykrywania treści pornografii dziecięcej w prywatnej komunikacji to te same, które wykrywają spam, malware i inne. Technologie odpowiadają tylko na pytanie, czy taki materiał może być materiałem pornografii dziecięcej – tak czy nie. Te programy, systemy nie rozumieją treści, one nie rozumieją czego dotyczą dane treści. To jest taki radar czy foto kamera. Ona może tylko stwierdzić, z jaką prędkością porusza się pojazd. To jest taki czujnik dymu w domu. Jeśli pojawia się dym, to alarm się włącza. Tak samo, jak magnes, który przyciąga tylko metal, ale nie przyciąga innych materiałów. Jest to to samo naruszenie prywatności w prywatnej komunikacji, bo jest to naruszenie z użyciem technologii, które dzisiaj chronią nasze komputery przed wirusami, przed spamem czy przed przestępstwami cybernetycznymi. W Polsce istnieje prawo, które chroni użytkowników przed spamowymi SMS-ami. Aby było to możliwe, software musi analizować wszystkie wiadomości tego rodzaju i blokować te, które zostają uznane za spam. To nie jest nowa technologia czy nowe podejście. To jest raczej problem programowo-polityczny.

Trzeba zadać sobie pytanie, czy chcemy stosować technologię w zastosowaniu do prywatnej komunikacji, aby chronić nasze komputery i telefony komórkowe? Jeśli tak, to powiedzmy, że ta sama technologia będzie chronić nasze dzieci przed tymi koszmarными przestępstwami. Odpowiedź jest dzisiaj w rękach władzy ustawodawczej – w Parlamencie Europejskim, ale również w Radzie. Naturalnie, problem nie zniknie, nawet gdyby zaprzestano detekcji w prywatnej komunikacji. Dzieci nadal będą cierpieły, tyle że w ciszy i przez wiele lat. Dla Komisji Europejskiej kluczowe jest to, aby rozwiązanie było skuteczne, aby skutecznie chroniło dzieci. Będziemy dalej współpracować z Parlamentem Europejskim i z Radą,

aby zapewnić pożądaný skutek. Mamy również nadzieję zapewnić współpracę z państwem właśnie w tym kierunku. Bardzo dziękuję.

Przewodnicząca poseł Monika Rosa (KO):

Bardzo dziękuję za to wyjaśnienie.

Teraz poproszę o zabranie głosu panią Magdalenę Witecką z Fundacji Dajemy Dzieciom Siłę i panią Salę Huikuri z ECPAT.

Specjalistka do spraw bezpieczeństwa dzieci w internecie w Fundacji Dajemy Dzieciom Siłę Magdalena Witecka:

Może najpierw ECPAT.

Przewodnicząca poseł Monika Rosa (KO):

Dobrze, zatem najpierw ECPAT. Bardzo proszę.

Przedstawiciel ECPAT International Salla Huikuri:

Dzień dobry. Zdaje się, że mają państwo moją prezentację?

Przewodnicząca poseł Monika Rosa (KO):

Nie. Może mogłaby pani uruchomić teraz swoją prezentację?

Przedstawiciel ECPAT International Salla Huikuri:

No dobrze, to w takim razie będzie bez slajdów, nie ma problemu.

Dzień dobry, nazywam się Salla Huikuri i pracuję dla ECPAT International. Siedziba organizacji znajduje się w Bangkoku w Tajlandii, ale pracuję w Helsinkach w Finlandii. To dla mnie zaszczyt, cieszę się, że mogę wystąpić przed państwem w imieniu ECPAT. Zrzeszamy 134 organizacje ze 110 krajów na całym świecie. Zajmujemy się położeniem kresu seksualnemu wykorzystywaniu dzieci. Technologie cyfrowe stale się rozwijają, w związku z tym rosną także wyzwania związane z tym, jak zabezpieczać dzieci przed tym zagrożeniem. Wszyscy musimy zdać sobie sprawę z tego, że zmiany wymagane są pilnie. W politykach w przepisach uznajemy istnienie tych zagrożeń oraz proponujemy rozwiązania, które stworzą bezpieczną przestrzeń dla dzieci w świecie internetu. Ten wniosek państw członkowskich to konstruktywny krok na przód. Mamy nadzieję, że dzięki temu wzmocnimy ochronę dzieci w całej Europie. Cieszymy się, że Polska wykazała się przywództwem w wyznaczeniu tego jako priorytet. Mamy nadzieję, że w nowym projekcie tego wniosku będą uwzględnione nasze uwagi.

Chcę poruszyć trzy główne obszary, które należałoby wzmocnić w proponowanym wniosku tak, żeby można było skutecznie reagować. Po pierwsze, obowiązkowe zgłaszanie przypadków wykorzystywania dzieci, kwestie szyfrowania end-to-end i powołanie mocnego, silnego centrum unijnego na rzecz ochrony dzieci. Ważne jest, żeby dostawcy usług, platformy, organy ścigania, a także decydenci polityczni współpracowali ze sobą tak, aby skutecznie reagować, a także zapobiegać wykorzystywaniu seksualnemu dzieci.

Zacznę najpierw od tego obowiązku zgłaszania. To jest jeden z najważniejszych mechanizmów, który umożliwia nam walkę z wykorzystywaniem seksualnym dzieci. Dzięki temu przypadki takiego wykorzystywania będą zgłaszane, sprawcy będą ukarani, a dzieci ochronione i otrzymają odpowiednie wsparcie. Dostawcy usług online, a także edukatorzy i profesjonalści i inne podmioty miałyby obowiązek zgłaszać odpowiednim organom podejrzenia wykorzystywania seksualnego. Bez takiego obowiązku nie będzie zgłaszanych zbyt wiele przypadków, a sprawcy będą nadal szkodzić dzieciom i nie będą ponosić za to żadnych konsekwencji. Taki obowiązkowy system powinien zawierać kilka elementów – wykrywanie, zgłaszanie, a także działania następcze. Pokrótce opowiem każdy z tych komponentów.

Najważniejszym krokiem jest zadbanie o to, żeby wykrywać takie przypadki, bo jest to absolutnie pierwszy krok. Jeśli nie będziemy w stanie ich wykrywać, to nie będziemy w stanie nic z tym zrobić. Zatem platformy internetowe powinny mieć takie automatyczne narzędzia np. wykrywania z wykorzystaniem sztucznej inteligencji, ale także inne, aby wykrywać i usuwać takie materiały. Tak jak powiedział mój przedmówca – takie rozwiązania są już dostępne. Chodzi o to, żeby wykorzystywać je do tego, żeby wykryć nowe materiały czy to wideo, czy inne i zapobiec dalszemu szkodzeniu dzieciom. Ale nie możemy ograniczać tego tylko do działań po stronie platform internetowych. Potrzebujemy także profesjonalistów edukatorów, tych osób, które blisko pracują z dziećmi i powinny one być w stanie szybko wykryć objawy takiego wykorzystania, a także zgłaszać tego rodzaju podejrzenia. Chodzi o takie podejście proaktywne,

dzięki któremu będziemy mogli szybciej interweniować i tym samym zapobiegniemy długofalowym szkodom i ochronimy dzieci. Bez skutecznego wykrywania niestety cały czas te materiały będą dostępne, ofiary będą narażone na dalsze cierpienie, a sprawcy nie będą ponosili za to konsekwencji. Po drugie, kiedy mamy już wykrycie, to potem trzeba je zgłosić do agencji ochrony dziecka, do organów ścigania tak, żeby móc prowadzić odpowiednie działania. Dostawcy usług, lekarze, nauczyciele, wszyscy, którzy pracują z dziećmi powinni mieć obowiązek, żeby od razu zgłaszać tego rodzaju zdarzenia. Żeby system działał, potrzebujemy jasnych procedur i jasnych standardów, żeby takie osoby dokładnie wiedziały, do kogo dokładnie zgłaszać takie zdarzenie i jakie po kolei podejmować kroki. Nie może być tak, że takie osoby będą bały się ponoszenia konsekwencji, będą niepewne, będą wiedziały, jakie obowiązki prawne na nich spoczywają. Powinien zostać także ustanowiony mechanizm anonimowego zgłaszania. Dzięki temu osoby indywidualne będą mogły bez obaw zgłaszać takie przypadki. Bez takiego zgłaszania, dzieci będą w stałym zagrożeniu.

Po trzecie, mieliśmy już wykrywanie, mieliśmy zgłaszanie i teraz w końcu kolejny krok, który obejmuje przeprowadzenie dochodzenia i ocenę zgłoszeń. Kiedy są już dowody, należy ścigać przestępców i ich skazać, żeby nie mogli więcej krzywdzić dzieci. Także na platformach internetowych spoczywa pewna odpowiedzialność. Muszą one zgłaszać przypadki wykorzystywania, usuwać takie szkodliwe materiały, a także współpracować z organami ścigania. Poza tym mamy tu do czynienia z przestępstwem transgranicznym. Dlatego też konieczna jest współpraca międzynarodowa, i to bliska, tak, żeby sprawcy nie mogli uciekać za granicę przed wymiarem sprawiedliwości. Bez podjęcia stosownych działań, takie zgłoszenia pozostaną tylko na papierze, a dzieci nie będą chronione. Dlatego organy ścigania powinny dysponować odpowiednimi zasobami, odpowiednimi uprawnieniami, żeby miały możliwość współpracy w wymiarze międzynarodowym, żeby zadośćuczynić ofiarom.

Po czwarte, nie możemy kończyć na tych trzech krokach, bo dla dzieci, dla ofiar konieczne jest stałe wsparcie i ochrona. Konieczny jest dostęp do odpowiednich usług wsparcia, pomocy, i to także w całym procesie i po jego zakończeniu. Dzieci, które doświadczyły tego rodzaju sytuacji, nie powinny być wtórnymi ofiarami. Bez takich działań następnych niestety pojawia się ryzyko traumy dla takich dzieci. Musimy zadbać o dzieci i to nie tylko teraz, ale także w przyszłości. W nowym proponowanym rozporządzeniu wszystkie platformy internetowe powinny mieć obowiązek proaktywnego zgłaszania tego rodzaju podejrzeń materiałów. Platformy muszą przestrzegać wszystkich przepisów dotyczących ochrony dzieci, a także prywatności, bo bezpieczne, szyfrowane wysyłanie wiadomości nie może stać na drodze ochrony dzieci. Powinny być ustanowione odpowiednie wymogi, ale przede wszystkim najważniejsza jest ochrona dzieci. Nie możemy stawiać ich życia i zdrowia na szali w obliczu interesów korporacyjnych. W imię ochrony danych nie możemy pomijać takich przypadków. W ramach przepisów o obowiązkowym zgłaszaniu mierzymy się z twardą rzeczywistością. W tym momencie, co roku tysiące takich przypadków nie są wykrywane, a niestety poszkodowani nie mają dostępu do żadnej pomocy ani wsparcia i cierpią w samotności. Musimy zadbać, żeby każde dziecko w Europie było chronione, żeby zgłaszać każdy przypadek, żeby każdy sprawca poniósł odpowiedzialność za to, co robi. To Europa musi ustanowić globalne standardy ochrony dzieci. Musimy działać teraz, bo każdy moment niepodejmowania działań oznacza zagrożenie dla naszych dzieci. W kontekście tego wniosku, musimy nałożyć obowiązek na platformy proaktywnego wykrywania i zgłaszania materiałów zawierających przypadki wykorzystywania seksualnego dzieci. Przede wszystkim naszym priorytetem powinno pozostać bezpieczeństwo dzieci. Bez takiego obowiązkowego mechanizmu zgłaszania wiele takich przypadków pozostanie niewykrytych. To jest nasza odpowiedzialność, aby wzmocnić ten mechanizm i procedurę.

Po drugie, szyfrowanie end-to-end oraz bezpieczeństwo dzieci. Szyfrowanie to bardzo ważna funkcjonalność służąca ochronie prywatności. Dzięki temu tylko nadawca i odbierający mają dostęp do komunikacji między nimi. Natomiast są to ważne gwarancje, ale wiążą się z nimi pewne zagrożenia związane z tym, że poprzez szyfrowanie jakiejś wiadomości nie możemy wykryć i zgłosić przypadku wykorzystania seksualnego. W takim wypadku tylko wysyłający i odbiorca ma dostęp do takiej wiadomości. Platformy nie mogą skanować takiej wiadomości w poszukiwaniu materiałów z wykorzystaniem seksualnym dzieci. Oczywiście jest to ważne narzędzie służące ochronie prywatności, ale niestety oznacza także, że takie materiały mogą później krążyć w sieci, nie możemy ich wykryć. Wiele dostawców usług ma zautomatyzowane systemy, takie jak PhotoDNA, hash matching itd. Dzięki takim systemom możliwe jest zidentyfikowanie takich

materiałów i ich zgłoszenie. Natomiast w momencie stosowania takiego szyfrowania bez odpowiedniej gwarancji, takie technologie są nieskuteczne. Niestety uniemożliwiają one proaktywne wykrywanie, zgłaszanie i usuwanie nielegalnych treści. Grooming, który ma miejsce w takich wiadomościach jest znacznie trudniejszy do wykrycia dla organów i dla platform, tym samym trudniej jest podjąć działania w takim przypadku. Poza tym szyfrowanie to poważna przeszkoda stojąca na drodze organów ścigania, bo przestępcy mogą wykorzystywać szyfrowanie i tym samym utrudniać chociażby przedstawienie dowodów w prokuraturze. Oczywiście ochrona prywatności jest ważna, ale nie może to oznaczać pełnej swobody dla przestępców. Powinniśmy być w stanie mieć dostęp do takich treści w momencie, kiedy jest tak dużo przypadków wykorzystywania dzieci. Powinniśmy być w stanie śledzić niektóre wiadomości i tym samym podejmować działania. Mamy nadzieję, że dzięki temu uda nam się zidentyfikować pewne wzory zachowań groomingowych i tym samym podjąć działania na rzecz prewencji.

Sztuczna inteligencja może być także wykorzystywana do tego, aby wykrywać wczesne oznaki groomingu. Modele sztucznej inteligencji mogą analizować metadane, pewne wzory językowe, a także sygnały behawioralne. Bywa tak przecież, że osoby dorosłe wielokrotnie podejmują rozmowy, konwersacje z osobami małoletnimi. To także jest jakiś wzorzec zachowania. Musimy zadbać o bezpieczeństwo dzieci, a także o przestrzeganie zasad szyfrowania. Zgłaszanie przez użytkowników to także jest kolejna rzecz, którą możemy zrobić, żeby użytkownicy i poszkodowani byli upodmiotowieni w całym procesie. Platformy powinny wykorzystywać odpowiednie narzędzia, żeby także inni użytkownicy mogli oznaczać takie wiadomości, treści czy też zachowania o charakterze groomingowym. Moderatorzy mogą bardzo szybko dokończyć oceny, czy takie zgłoszenie jest zasadne i ewentualnie przekazać je do organów ścigania. Platformy powinny dać także jasne wytyczne dotyczące tego, w jaki sposób można sprawować chociażby kontrolę rodzicielską.

W końcu ważne jest wzmocnienie współpracy pomiędzy branżą a organami ścigania. Konieczne są programy oznaczania, które będą poprawiały bezpieczeństwo dzieci w szyfrowanym środowisku. Konieczne jest powołanie takich programów, dzięki którym NGO, eksperci, profesjonalści będą mogli je wykorzystywać do tego, żeby zmniejszyć takie ryzyka. Tacy eksperci będą mogli lepiej i sprawniej zgłaszać np. grooming czy nielegalne treści z poszanowaniem szyfrowania. Takie podejście jest także ważne dla organów ścigania i organizacji ochrony dzieci, żeby mogły współpracować z platformami i żeby mogły zadbać o to, żeby szyfrowanie nie stało na drodze sprawiedliwości ochrony dzieci.

Podsumowując, szyfrowanie nie może być wykorzystywane jako swego rodzaju tarcza. Oczywiście wiemy, że prywatność jest ważna, ale prawa dzieci nie mogą być niechronione w szyfrowanych wiadomościach. Powinny być lepsze mechanizmy zgłaszania. Konieczna jest bliższa współpraca pomiędzy branżą a sektorami i organami ścigania. Dzięki temu uda nam się znaleźć wyważone podejście, które będzie służyło ochronie praw podstawowych dzieci.

Ostatnia rzecz, o której chcę powiedzieć, to konieczność powołania takiego silnego centrum ochrony dzieci, o tym mówił już pan Labrador. Popieramy powołanie do życia takiego centrum ochrony dzieci, żeby skoordynować wszystkie wysiłki, żeby prowadzić działania transgraniczne, żeby skutecznie reagować w przypadkach seksualnego wykorzystywania dzieci. Europejskie centrum ochrony dzieci jest niezbędne, dlatego że nasze działania podejmowane do tej pory, żeby zwalczać wykorzystywanie dzieci są niepełne, niespójne, a tym samym nieskuteczne w tym wymiarze transgranicznym. Dzięki takiemu centrum będziemy mogli lepiej chronić dzieci. Po pierwsze, będziemy mogli uzupełnić pewne luki, które istnieją, jeśli chodzi o współpracę organów ścigania. Dzisiaj rzeczywiście istnieje próba wyważenia różnych praw podstawowych, więc taki europejski ośrodek mógłby być źródłem wytycznych i najlepszych praktyk. Taki ośrodek wzmocni współpracę transgraniczną, bo wykorzystywanie seksualne dzieci ma charakter transgraniczny. Natomiast działania organów ścigania mają głównie charakter krajowy, więc tego rodzaju ośrodek mógłby wzmocnić współpracę międzynarodową i wspólne operacje. Detekcja, a więc wykrywanie i prewencja także mogłyby być tam wypracowane w kontekście rozwiązań technologicznych, które ułatwią takie działania bez naruszania innych praw podstawowych. Dalej wsparcie na rzecz ofiar. Bardzo często to wsparcie jest nieadekwatne i niewystarczające.

Po piąte, taki ośrodek mógłby być także źródłem skutecznych aktów prawa. Ośrodek mógłby wspierać instytucje ustawodawcze w przygotowaniu projektów właściwych aktów prawa, równoważących wszystkie prawa podstawowe. Byłby to ośrodek działań skoordynowanych, działań eksperckich i podejmujących działania, które będą spójne, skuteczne i odnoszące skutek zgodny

z prawami podstawowymi. Wobec tego chcielibyśmy zachęcić polski parlament, aby rzeczywiście działać na rzecz takich rozwiązań europejskich, które zwiększą poziom ochrony dzieci poprzez właściwe zaangażowanie operatorów prywatnych, ich właściwe raportowanie i usuwanie treści groomingowych i pornograficznych. Chodzi również o to, aby platformy mogły działać coraz bardziej proaktywnie z poszanowaniem innych praw podstawowych. Jednak powinny istnieć właściwe zasady, które regulują przyjmowane działania i rozwiązania na rzecz łagodzenia i zmniejszania ryzyka. Europejski ośrodek dobrze wpisuje się w ramy unijne i globalne. Będzie również chronił ofiary, a także wspierał je.

Wszyscy mają prawo do bezpieczeństwa w sieci, a w szczególności to prawo mają dzieci. To od nas zależy, czy Europa będzie liderem ochrony dzieci przed niegodziwym traktowaniem w celach seksualnych i wykorzystywaniem seksualnym. To my jesteśmy zobowiązani do działań w tej mierze. Wzywamy również polski parlament do działań na rzecz lepszej ochrony tak, by dziecko nie pozostawało bez ochrony w świecie cybernetycznym.

Przewodnicząca poseł Monika Rosa (KO):

Teraz tak, o godz. 13.00 kończymy Komisję niezależnie od tego, co by się stało, więc ponieważ Fundacja Dajemy Dzieciom Siłę jest częścią ECPAT, to bardzo proszę o zwięzłość.

Specjalistka do spraw bezpieczeństwa dzieci w internecie w Fundacji Dajemy Dzieciom Siłę Magdalena Witecka:

Dzień dobry. Będę mówić o bezpieczeństwie dzieci online. Rozumiem, że już dużo państwo usłyszeli i zostało powiedziane, ale bardziej z takiej perspektywy pomocy bezpośredniej... Nie będę się rozwodzić, że nasza wizja i misja to jest stworzenie takich warunków dla dzieci i młodzieży, żeby były jasne reguły reagowania na przemoc i żeby dzieci wiedziały, jak po nią sięgać, kiedy coś się dzieje, tak samo jak i dorośli. Myślę, że dużo już było tutaj powiedziane o badaniach i jak wygląda ta rzeczywistość. Było też powiedziane o tym, że trochę ta rzeczywistość w statystykach nie oddaje tego, co naprawdę się dzieje. Tak tylko zostawiam państwa z taką konkluzją, że świat online, w którym uczestniczą dzieci, tam nie ma dorosłych. Jeżeli nawet w jakiś sposób są, to nie jest poruszana ta wiedza np. à propos tych szkodliwych treści pornograficznych czy niebezpiecznych kontaktów. Oczywiście nie chcę w żaden sposób straszyć, ale myślę, że to jest rzeczywistość, jeżeli sobie pomyślimy, że prawie 1/5 dzieci, zanim ukończyło 9 lat, miało kontakt ze szkodliwymi treściami, to jest to czwórka dzieci w dwudziestoosobowej klasie. To już są dzieci, które muszą przetwarzać te treści, przeważnie dzieje się to niekoniecznie w asyście osób dorosłych.

Tylko nadmienię, że jestem jedną z osób z zespołu Poradni Dziecko w Sieci. To jest Poradnia fundacyjna, która zajmuje się wszelkim rodzajem pomocy bezpośredniej w sytuacjach zagrożenia, cyberprzemocy, wykorzystywania online szkodliwych treści i kontaktów. Z tej perspektywy trochę chciałabym podzielić się z państwem naszym doświadczeniem. Zostało tu powiedzianych dużo słów, ale myślę sobie, że nikt nie dyskutuje z tą koniecznością wprowadzania i wspomagania dorosłych, rodziców i profesjonalistów w ochronie dzieci w świecie online.

Chciałam podzielić się z państwem taką perspektywą naszego doświadczenia na bazie case'u. Zastrzegam, że obowiązuje nas tajemnica, więc nigdy nie dzielimy się case'ami naszych klientów czy pacjentów, bo po prostu nie możemy. Chciałam podzielić się takim przypadkiem, który składa się z doświadczeń z naszej pracy. Tak jak zaznaczam – jest on stworzony na potrzeby naszego spotkania. Oddaje to, z czym mierzymy się na co dzień, szczególnie w przypadku takich treści o charakterze seksualnym, tworzonym też przez dzieci. Chciałam opowiedzieć państwu historię Marysi. Marysia ma jedenaście lat i trafiła do naszej poradni zgłoszona przez nauczycieli. Została zgłoszona z tego powodu, że okazało się, że w klasie po prostu pojawiają się treści pornograficzne z jej udziałem. Dzieci rozsyłały sobie głównie te treści na Whatsappowej grupie szkolnej. Takim głównym kanałem dystrybucji tych treści, które tworzyła Marysia, był Snapchat. Dla rodziców to była rzecz, której nie byli w stanie ani kontrolować, ani nie byli w stanie dokumentować tych „snapów” w procesie uzyskiwania pomocy. Te doświadczenia online dziecka zostały dopiero jakoś udokumentowane i obrobione przy pomocy pedagoga szkolnego. Chciałam powiedzieć to w takim kontekście, że to nie jest historia tylko jednego dziecka, tylko zanim to wypłynęło, to te treści krążyły po klasie. Dzieci były zachęcane przez siebie nawzajem do oglądania tego. Było to trochę z ciekawości, trochę ze zdziwieniem. Najbliższe koleżanki Marysi były też zachęcane do tworzenia takiego samego kontentu. Kontakt ze sprawcą miał miejsce poprzez Roblox i Discorda w grupie związanej z tą grą. Potem sprawca przeniósł się

na Telegram, co było skuteczne pod wieloma względami, jeżeli chodzi o niekontrolowanie tych treści przez dorosłych. Chcę to podkreślić, że nawet, jeżeli rodzice, w jakimś momencie zaczynają reagować, są czujni...

W tej sytuacji zanim rodzice z dzieckiem do nas trafili, to zabrali dziecku wszystkie sprzęty, ale po pewnym czasie okazało się, że dziecko nadal produkuje, nawiązując kontakty nie tylko z tą jedną osobą, która je do tego nakłaniała, ale też szukając kontaktu z innymi zainteresowanymi osobami, akurat tutaj przez Snapchata i przez specjalne konto, do którego współprowadzenia zaprosiła swoją koleżankę z klasy i to dzięki temu zaistniała szybsza i mocniejsza reakcja na to, czego doświadczała dziewczynka. Wysyłając te materiały dziecko korzystało z telefonów innych bliskich sobie dzieci albo z telefonu cioci, pod której była opieką w momencie, kiedy rodzice pracowali, a dziecko było w domu.

Podsumowując to, chciałabym tylko podkreślić, że po pierwsze, ten rodzaj krzywdzenia dzieci nigdy nie dotyczy jednego dziecka, ale zawsze to jest taka sytuacja, na którą dziecko czy młoda osoba, bo z naszej praktyki doświadcza tego szczególnie dużo młodych nastolatków, jest bohaterami tego typu historii. Młode osoby zawsze są krzywdzone i nie ma tutaj niuansów. To, z czym mierzy się dziecko, w przypadku krzywdzenia jest takimi typowymi konsekwencjami. To jest poczucie straty, winy, wstydu, poczucie straty swojego ciała, złość, zaburzenia nastroju. Mówię o tym szczególnie o tym poczuciu winy i wstydu, bo gdy myślimy o tym, że tylko system rodzinny czy szkoła mogłyby reagować na takie sytuacje, to proszę zobaczyć, jaka jest trudna sytuacja na wielu poziomach, żeby w ogóle zgłosić takie doświadczenie w przypadku dziecka, które, jak wspominało tutaj wiele osób, często nie jest świadome tego, że jest to krzywda, jeśli jednocześnie dostaje za to uwagę. Łatwiej jest, gdy dziecko jest zastraszane, ale gdy dostaje uwagę i może czerpać z tego przyjemność, to tym bardziej.

Wiem, że nasz czas się kończy, więc chcę tylko podkreślić, że to jest bardzo duża krzywda związana z rozwojem seksualnym. Też jest to pewien taki rodzaj krzywdzenia i zaangażowania w tę czynność i powoduje to, że bardzo często te materiały nie są produkowane jednorazowo. Sam charakter obiegu tych materiałów sprawia, że dziecko jest narażone na ciągłe wykorzystywanie i produkowanie nowych materiałów i zatacza duże kręgi, bo to jest takie wydarzenie społeczne, które też angażuje inne dzieci i rodziców.

Zakończę tylko tym slajdem. Wszyscy się nad tym zastanawialiśmy, państwo nad tym też debatowali, mówili o tym wcześniej moi poprzednicy, ale myślę sobie, że dzieci w tym świecie są trochę jak takie króliki doświadczalne, a z drugiej strony są jak na dzikim zachodzie, bo nie wiadomo, co się zdarzy. Tym bardziej potrzebujemy stwarzać te struktury, żeby to nie było takie doświadczenie, gdzie nie ma struktury, gdzie nie można zgłaszać albo to zgłaszanie jest nieefektywne. Dziękuję bardzo.

Przewodnicząca poseł Monika Rosa (KO):

Dziękuję bardzo pani Magdalenie Witeckiej z Fundacji Dajemy Dzieciom Siłę.

Teraz pan John Carr. Zbliżamy się do końca czasu, więc bardzo proszę o ograniczenie swojej wypowiedzi do dziesięciu minut.

Przedstawiciel OBE John Carr:

Dzień dobry. Muszę przeprosić, dlatego że mój ojciec był Polakiem i urodził się w Żyrardowie, a dorastał w Łodzi, ale ożenił się z Irlandką, więc w domu mówiono tylko po angielsku. Muszę przeprosić, że nie będę mówił po polsku.

Kilka słów na temat prawa brytyjskiego. Mieszkam w Londynie, od 1995 r. zajmuję się ochroną praw dziecka. W 1996 r. założyłem brytyjską Internet Watch Foundation. Niedawno brytyjski parlament przyjął ustawę online safety act – ustawa o bezpieczeństwie w sieci i weszła ona w życie w 2023 r. Nasz urząd regulacji, Ofcom dzisiaj zajmuje się także internetem i od października 2023 r. opracowuje szczegółowe przepisy, które mają wdrożyć naszą ustawę. De facto one weszły w życie w poniedziałek w tym tygodniu. Nasze rozstrzygnięcia prawne są odzwierciedleniem propozycji złożonych przez Komisję Europejską w tym nowym projekcie rozporządzenia, które ma służyć przeciwdziałaniu wykorzystywaniu seksualnemu dzieci. De facto nasze rozstrzygnięcie zachowuje zręby wcześniejszych propozycji, również Komisji Europejskiej. Otóż wszystko rozpoczyna się od oceny ryzyka. Każdy oferent usług w sieci, a więc media społecznościowe, ale nie tylko społecznościowe, bo też inne, wszystkie od poniedziałku muszą przeprowadzać ocenę ryzyka i przedstawiać ją do wglądu urzędowi regulacji. W szczególności do końca bieżącego miesiąca platformy te muszą przedstawić szczegółowe

oceny ryzyka i propozycje działań właśnie w zakresie zwalczania, przeciwdziałania materiałom wykorzystującym seksualnie dzieci.

Tam, gdzie pokazuje to ocena ryzyka lub rozstrzyga o tym urząd regulacji, czy istnieje ryzyko wystąpienia tego rodzaju materiałów, platforma jest zobligowana do podjęcia działań na rzecz ograniczenia ryzyka dystrybucji takiego materiału. Jeśli dana platforma opóźnia się lub odmawia, jeśli chodzi o wdrożenie właściwych rozwiązań technicznych, by zmniejszyć wolumen takich nielegalnych treści, to regulator może zastosować wiążące nakazy, mówiące o konieczności zastosowania technologii ograniczającą dystrybucję takich treści. Same platformy decydują, jakie technologie chcą wykorzystać, ale jeśli nie wybiorą żadnej albo wybiorą takie, które są niezadowolające dla urzędu regulacji, wówczas urząd może wymagać od nich zastosowania konkretnych instrumentów.

Słyszeliśmy o PhotoDNA, to już istnieje od 2009 r. W ciągu szesnastu lat nie ma ani jednego przypadku popełnienia błędu – wszczęcia postępowania czy skazania ze względu na błąd zastosowanej technologii. Po prostu do chwili obecnej błąd nie wystąpił, aby np. dziecko pływające w falach morza zostało niewłaściwie uznane za nielegalną treść. Ta i inne technologie działają skutecznie, bo potrafią wykrywać tego rodzaju treści. Za pomocą tego systemu wykryto 36 mln treści na 1500 różnych platform. 17 mln obrazów pochodziło tylko z Facebooka. Ile z Apple? 267, nie tysięcy, nie milionów, ale 267. Dlaczego tyle? Dlaczego Apple zgłosił tak niską liczbę obrazów tego rodzaju? To bardzo proste – oni już stosują enkrypcję w przeciwieństwie do Google'a, Microsoftu, Tik Toka i pozostałych. Apple odmawia poszukiwania nielegalnej treści dziecięcej. Stąd tylko 267 przypadków. One zaistniały tylko, dlatego że ktoś włączył te treści do profilu widocznego poza treścią szyfrowaną. Otóż Apple ma pełną wiedzę, że inne platformy działają inaczej. W sierpniu 2021 r. Eric Friedman, który do dziś jest jednym z dyrektorów Apple, powiedział, że Apple najgorzej radzi sobie, jeżeli chodzi o właśnie dostępność tej treści w chmurze. Apple oferował dobre rozwiązanie techniczne, które umożliwiało wykrywanie tej treści, ale odstąpił od niego i nie chciał go zastosować. Co pokazuje przypadek Apple? Mianowicie to, że platformy messagingowe stały się głównym obszarem, w którym rozgrywa się przestępczość wobec dzieci. Musimy znaleźć sposób na poradzenie sobie z tym problemem, a więc wymianą materiałów, ale również przeciwdziałaniu groomingowi i innym działaniom, o których mówili moi przedmówcy. Ja może skupię się na materiałach.

Platformy messagingowe dzielą się na dwie kategorie – te, które stosują kodowanie i enkrypcję, i te, które tego nie robią. Ta druga kategoria, a jest w niej sporo podmiotów, może robić to, co Meta i inni od 2009 r. i stosować instrumenty jak PhotoDNA i inne technologie wykrywające obrazy i zgłaszanie ich właściwym organom tak, aby nie były już dalej rozpowszechniane. Praktycznie mówiąc, organy ścigania i nasze sądy nie mogą właściwie działać, ponieważ nie dostają dostępu do materiałów inkryminujących, jeśli tego typu technologie nie działają i nie wykrywają tej treści. Silna enkrypcja robi to, że daje ochronę sprawcom, której nie możemy zaoferować ofiarom. Żaden traktat międzynarodowy dotyczący praw człowieka, ani żadna konwencja międzynarodowa nigdy nie stwierdziła, że ochrona prywatności jest prawem bezwzględny, absolutny, niepodlegającym żadnym ograniczeniom. Nie mówią o tym też akty praw krajowych. W każdej jurysdykcji, w każdej konwencji, w każdym traktacie międzynarodowym mówi się o prawie do prywatności jako o prawie podstawowym, ale jest to jedno z wielu praw. W teorii i orzecznictwie zwykle równoważy się prawa wobec działań organów ścigania, ale nie można tego równoważyć z zerem, a silna enkrypcja, silne kodowanie zawsze skutkuje w ten sposób. Takie działanie prywatnych podmiotów, platform powoduje, że organy ścigania są nieme, sądy są nieme, bo po prostu nic nie mogą skutecznie zrobić, aby wszczynać postępowania chroniące prawa innych, w tym wypadku prawa dzieci, które są wykorzystywane seksualnie, a ich wizerunek jest rozpowszechniany internetowo.

De facto mówimy, że taki proceder rzuca rękawicę praworządności. Oczywiście stosujemy zasadę praworządności, ale musimy przyjmować takie działania... Wiadomo, że organy ścigania, Policja nie mogą działać w oparciu o widzimisię, to są działania regulowane i mają podstawę prawną, a tym bardziej postępują tak sądy. Musimy znaleźć sposób, aby organy ścigania i sądy mogły ugruntowywać, chronić zasadę praworządności. W tej sytuacji wygląda to tak, że prywatne podmioty, czy prywatne osoby, właściciele Telegramu i inni sami decydują o tym, że powstaje wielka przestrzeń wykorzystywana przez przestępców, do której sądy nie mają dostępu. Zdarza się tak, że Policja, organy ścigania mogą uzyskać dostęp do szyfrowanych wiadomości, ale nie można tego robić na dużą skalę. Nie można przecież polegać na dobrej woli drugiej strony,

żeby udostępniła dostęp do tych wiadomości. Nie może być tak, że grupa prywatnych osób, grupa prywatnych przedsiębiorstw decyduje o tym, czy organy ścigania będą miały taki dostęp. To wszystko miało być poufne, ale nie jest, otóż ta sprawa była w tym tygodniu, w poniedziałek i chodziło o to, żeby Apple zaczęło dysponować takim instrumentarium, które umożliwiłoby organom ścigania dostęp do treści takich wiadomości w momencie, kiedy mamy do czynienia z osobą podejrzaną. Nie wiemy jak to się zakończy, ale już wkrótce się tego dowiemy.

Tak, czy tak bardzo ważnym jest, żeby nasze działania się powiodły, bo w innym wypadku pojawia się taka luka, którą mogą wykorzystywać przestępcy. To tyle z mojej strony. Mam nadzieję, że Unia Europejska w końcu zgodzi się i że zostaną przyjęte takie przepisy w duchu tego wniosku zaproponowanego przez Komisję Europejską. Jesteśmy liberalną demokracją i nią pozostaniemy. Nic w zapisach Unii Europejskiej nie stanowi żadnego zagrożenia dla praworządności, a wręcz przeciwnie, myślę, że w tym wniosku Komisji Europejskiej chodzi przede wszystkim o to, żeby podtrzymywać praworządność.

Przewodnicząca poseł Monika Rosa (KO):

Dziękuję bardzo, panie Carr.

Dyskusję przeprowadzimy na innym posiedzeniu Komisji, bo ten temat jeszcze będzie podejmowany. Natomiast prosiłabym jeszcze pana ministra Gramatykę, aby przez te parę minut krótko skomentował, odniósł się, powiedział, co się dzieje w ministerstwie. Bardzo proszę.

Sekretarz stanu w Ministerstwie Cyfryzacji Michał Gramatyka:

Bardzo dziękuję. Szanowni państwo, szanowni goście z zagranicy, z całym szacunkiem dla tego, co powiedział pan John Carr, który jest jednym z autorów tej ustawy, my teraz w Polsce pracujemy nad podobnymi przepisami, a zatem niezwykle dziękuję za tę pracę, którą państwo wykonali nad tym projektem ustawy.

Temat CSAM jest dość istotnym elementem prac Ministerstwa Cyfryzacji, jest dość istotnym elementem polskiej prezydencji, dlatego że wymaga ustalenia, w jaki sposób to zjawisko będzie rugowane z internetu, czyli w jaki sposób te materiały, które przedstawiają seksualne wykorzystywanie dzieci, mogą być rugowane z internetu. W tej pierwszej unijnej propozycji znalazła się propozycja, która jest w zasadzie nie do zaakceptowania zarówno przez Polskę, jak i przez parę innych krajów. Jest to propozycja maszynowego wykrywania i identyfikowania treści przedstawiających seksualne wykorzystywanie dzieci. Wiele krajów wspólnoty europejskiej uznało, że ta propozycja o tyle mocno wkracza w prywatność użytkowników, że w zasadzie prace nad tą dyrektywą utknęły w martwym punkcie. Na dzisiaj nie jest możliwe osiągnięcie porozumienia, które będzie przeprowadzało balans pomiędzy ochroną dzieci, ochroną małoletnich. W zasadzie chyba nie ma żadnych wątpliwości, że ta ochrona powinna być maksymalnie rozwinięta z wykorzystaniem wszystkich narzędzi technologicznych, z wykorzystaniem wszystkich środków, ale z drugiej strony stawiamy prywatność użytkowników. Oznacza to, że wiele krajów wspólnoty europejskiej nie chce zgodzić się na to, żeby treści naszych prywatnych rozmów prowadzonych na komunikatorach były maszynowo skanowane pod kątem identyfikacji treści CSAM, dlatego że tego typu pozwolenie na maszynowe skanowanie treści jakkolwiek jest słuszne pod kątem znalezienia treści przedstawiających seksualne wykorzystywanie dzieci, to może zostać w dość łatwy sposób przeorientowane na treści innego rodzaju. Wtedy mamy do czynienia z masową kontrolą korespondencji, która nie powinna być kontrolowana.

W tym momencie trwają daleko posunięte negocjacje, jak wybrnąć z tego pata, w jaki sposób dogadać się, porozumieć się pomiędzy tym, co wszyscy widzą jako niezbędne, czyli zapewnienie dzieciom niezbędnej ochrony i tym, co również wszyscy widzą jako niezbędne, czyli zapewnienie każdemu z nas stosownej prywatności w prywatnych konwersacjach. Nie sądzę, aby udało się osiągnąć kompromis do końca polskiej prezydencji. Nie sądzę, żeby w ogóle udało się osiągnąć kompromis, jeżeli nie zostanie zaproponowany jakiś inny mechanizm, który nie będzie tak głęboko wchodził w prywatność użytkowników. To jest tak naprawdę istota dyskusji nad tego typu rozwiązaniami, jak przeprowadzić balans pomiędzy tym, co jest potrzebne, czyli ochroną dzieci i tym, co również jest niezbędne, czyli ochroną prywatności. Różne państwa na różne sposoby radzą sobie z tym zagadnieniem. Większość krajów nie radzi sobie w zasadzie w ogóle. Dlatego właśnie te kanały szyfrowanej komunikacji, czyli wszystkie komunikatory bezpośrednio bazujące na usługach IP typu Whatsapp, Messenger, Signal i inne tego typu oferty, są niestety kanałem, przez który są niestety rozpowszechniane obrazy seksualnego wykorzystywania dzieci.

Będziemy oczywiście raportować, jak będą wyglądały dalsze prace. Dzisiaj w zasadzie ta dyskusja utknęła w impasie. Pewnie w momencie, kiedy ta dyskusja posunie się w jakimkolwiek kierunku, to będziemy informować Wysoką Komisję na ten temat. W Ministerstwie Cyfryzacji ten temat jest ulokowany w Departamencie Cyberbezpieczeństwa. Ja jestem tu gościem, jako że w Ministerstwie Cyfryzacji prowadzę inne tematy związane z ochroną małoletnich.

Jestem bardzo wdzięczny przede wszystkim za te wszystkie prezentacje, które dzisiaj obejrzałem. Jestem wdzięczny za zaproszenie zagranicznych gości. Z uwielbieniem patrzę na pana Johna Carra, dlatego że te brytyjskie rozwiązania legislacyjne są i zawsze były wzorem dla rozwiązań, które powstają w Polsce i to zarówno tych, które powstają w rządzie, jak i tych, które powstawały w projekcie obywatelskim. To trzeba podkreślić, bo to są dobre i działające rozwiązania. Myślę, że doczekamy się kiedyś w Polsce podobnych rozwiązań.

Warto jeszcze wspomnieć o jednym elemencie, który nie został tutaj zaadresowany, elemencie, który wynika z rozwoju technologii, czyli o algorytmach sztucznej inteligencji, które masowo potrafią rozbierać dowolne zdjęcie, pozbawiać go odzienia. Potrafią też implementować tego typu obrazki do internetu, co potem staje się gigantycznym problemem. To jest temat, o którym można przeczytać po wprowadzeniu informacji na temat „nudify”. Nie chcę tutaj epatować, jak to dokładnie wygląda. Generalnie uważam, że epatowanie takimi treściami nie służy ofiarom.

Jestem bardzo zadowolony i dumny z tego, że Komisja robi tak dużo, żeby w ogóle uświadomić istnienie tego typu zagrożeń. To jest pierwszy krok, który musimy wykonać. Bardzo dziękuję.

Przewodnicząca poseł Monika Rosa (KO):

Bardzo dziękuję, panie ministrze.

Tak jak mówiłam – dyskusję odbędziemy w późniejszym terminie. Dziękuję państwu i zamykam Komisję.