

## PROTOKÓŁ z XLV posiedzenia Rady do Spraw Cyfryzacji, które odbyło się 27 stycznia 2023 roku, o godzinie 13:00 w formie wideokonferencji.

Wpływ zastrzegania numeru PESEL na przeciwdziałanie kradzieży tożsamości lub ograniczenie jej skutków – Pani Agnieszka Gryszczyńska; Pan Krzysztof Zieliński, Dyrektor Departamentu Cyberbezpieczeństwa w Urzędzie Komisji Nadzoru Finansowego; Pani Anna Wojczakowska, Zastępca Dyrektora Departamentu Bankowości Komercyjnej w Urzędzie KNF; Pan Paweł Jaskulski, BNP Paribas Bank Polska SA, CSIRT – Digital Fraud oraz przedstawiciele Departamentu Zarządzania Systemami KPRM: Pan Maciej Górski, Dyrektor DZS; Pani Katarzyna Kopytowska, Zastępca Dyrektora DZS; Pan Przemysław Chiluta, Naczelnik Wydziału Zarządzania Danymi i Jakości Usług DZS.

Pan Wiceprzewodniczący Dariusz Milka przywitał zaproszonych gości, a następnie przekazał prowadzenie punktu Pani Agnieszce Gryszczyńskiej.

Pani Agnieszka Gryszczyńska podziękowała gościom za przyjęcie zaproszenia do dyskusji dotyczącej projektu *ustawy o zmianie niektórych ustaw w związku z zapobieganiem kradzieży tożsamości*. Nawiązała do [uchwały nr 7 Rady ds. Cyfryzacji](#), w której Rada wypowiedziała się w sprawie problemu kradzieży tożsamości. Kradzież tożsamości jest problemem dostrzegalnym – wśród przedstawicieli organów ścigania, polityków, mediów oraz pokrzywdzonych, których ten problem dotyka. Problematyka kradzieży tożsamości jest złożona i szeroka. W związku z rozwojem cyberprzestępczości zaobserwowano coraz więcej podszyć pod różne osoby. Celem działania sprawców jest wyrządzenie szkody osobie poprzez podszywanie się pod tą bądź inną osobę. Wśród przestępstw często obserwowanych są czyny, w których dochodzi do podszycia się pod inną osobę w sytuacji nawiązywania relacji o charakterze gospodarczym, zaciągania zobowiązań finansowych, ale również podpisywania różnego rodzaju umów, np. o świadczenie usług telekomunikacyjnych. Bardzo dużym problemem jest wykorzystanie fałszywej tożsamości na etapie korzystania z elektronicznych usług, tzn. zakładania kont poczty elektronicznej, rejestracji nazw domenowych czy korzystania z mediów społecznościowych. Pani A. Gryszczyńska wspomniała, że w ww. uchwale Rady podkreślone zostało zapewnienie lepszych mechanizmów weryfikacji tożsamości. Wskazywano również, że do potwierdzania cudzej tożsamości nie powinien być wystarczający numer PESEL, ponieważ nie jest on tajemnicą i znajduje się w jawnych rejestrach publicznych.

Jako pierwszy w dyskusji głos zabrał Pan Dyrektor Maciej Górski wskazując, że celem DZS jest dostarczenie nowej usługi zapewniającej ochronę w przypadku, gdy dojdzie do przestępstwa. Zauważona została ogromna potrzeba społeczna i realna obawa obywateli przed przejęciem ich tożsamości w cyfrowym świecie. Pan Dyrektor przekazał informację, iż ze wszystkich analizowanych uwag do projektu ww. ustawy wybrzmiała jedna zasadnicza uwaga, tj. obawy

o procesy, które dzieją się w czasie rzeczywistym. Pan Dyrektor wyjaśnił, że nie było celem ograniczanie rozwoju innowacyjnych usług finansowych odbywających się w czasie rzeczywistym, a przepisy omawianego projektu ustawy zostaną tak zmodyfikowane, aby wskazanego ryzyka nie było.

Pani Dyrektor Katarzyna Kopytowska poinformowała, że celem DZS jest prewencyjna ochrona obywateli, którzy otrzymują możliwość zastrzeżenia swoich danych. Ustawa stanowi także o ochronie następczej. Celem ustawy jest również zaszczepienie w obywatelach myślenia o zabezpieczeniu swoich danych, zanim zostaną wobec nich zrealizowane złe zamiary.

Pan Dyrektor M. Górski doprecyzowując zgodził się z przedmówczynią i wskazał, że intencją projektu nie jest regulacja zabezpieczeń stosowanych przez sektor bankowy czy sposobu przeciwdziałania fałszerstwom dokumentów tożsamości.

Pan Naczelnik Przemysław Chiluta odniósł się do uchwały Rady ds. Cyfryzacji i zwrócenia uwagi na konieczność przede wszystkim elementu weryfikacji tożsamości swojego klienta. Projekt omawianej ustawy trzeba rozpatrywać komplementarnie i kompleksowo z innym aktem, tj. projektem *ustawy o zmianie niektórych ustaw w związku z rozwojem e-administracji*, przewidującym takie narzędzia jak udostępnianie wizerunku z rejestru dowodów osobistych podmiotom, które potrzebują we właściwy sposób i na odpowiednim poziomie zweryfikować tożsamość swoich klientów.

Pan Naczelnik wskazał, że projekt omawianej ustawy przewiduje obligatoryjność weryfikacji zastrzeżenia numeru PESEL, w przypadkach z góry określonych przepisami ustawy. Należy zwrócić uwagę, że nie wyklucza on możliwości weryfikacji i uzyskiwania informacji o zastrzeżeniu numeru PESEL również w innych sytuacjach. Pojawia się sformułowanie interesu faktycznego - jeśli podmiot wykaże interes faktyczny, będzie mógł wykorzystywać informację o takim zastrzeżeniu dla wzmocnienia swoich własnych procesów wewnętrznych, bez zagrożenia sankcją wynikającą z projektu ustawy. W dalszej części swojej wypowiedzi Pan Naczelnik wskazał, że trudno byłoby zastrzec całą tożsamość danej osoby. Wyjaśnił, że pojawiają się prośby obywateli o zastrzeżenie numeru PESEL, mających obawę o wypłynięcie swoich danych. Zgłaszane się także sytuacje, gdy do takich zdarzeń już doszło. Wskazane zostało, że według statystyk Komendy Głównej Policji dwa główne przestępstwa, których dotyczy kradzież tożsamości, to oszustwo i podszycie się pod inną osobę.

Podkreślono, że regulacja ma charakter interdyscyplinarny, ponieważ ingeruje w kodeks postępowania cywilnego, w prawo konsumenckie i w prawo bankowe. Zdecydowano się na wydzielenie tego rejestru z systemu rejestrów państwowych, aby podmioty, które będą chciały potencjalnie dołączyć się i integrować, mogły zrealizować działanie w szybki sposób. Szczególny nacisk położono na łatwość podłączenia się i możliwość szybkiego skorzystania z usług, ze względu na nałożenie określonych obowiązków na pewne podmioty. Dostęp do informacji o zastrzeżeniu bądź braku zastrzeżenia danego numeru PESEL musi przebiegać w sposób prosty, łatwy, szybki i nieodpłatny, zarówno dla obywateli jak i dla podmiotów

integrujących się. W samym rejestrze zastrzeżeń numeru PESEL zdecydowano się na minimalizację danych osobowych.

Pan Naczelnik wspominał o uwagach do projektu ustawy zgłaszanych przez różne podmioty. Krótco streścił i scharakteryzował najistotniejsze zmiany planowane do uwzględnienia w projekcie ustawy. Wskazał wprowadzenie zasady, zgodnie z którą umowy nie będzie można zawrzeć w dniu dokonania zastrzeżenia numeru PESEL. Wiązało się to z chęcią zabezpieczenia pewnych potencjalnych sytuacji oszustw, kiedy pojawią się próby dokonania zastrzeżenia numeru PESEL w momencie zawierania umowy. Planowana jest zmiana projektu ustawy w tym kierunku, aby w szczególności umowy zawierane na odległość, dla których możliwa jest rejestracja dokładnej chwili zawarcia umowy, przewidywały możliwość zastrzeżenia/wycofania numeru PESEL w czasie rzeczywistym i od razu możliwość zawarcia takiej umowy. Pozostawiono zasadę, zgodnie z którą umowy nie można zawrzeć w dniu dokonania zastrzeżenia numeru PESEL dla umów, co do których dokładna chwila zawarcia nie jest rejestrowana, np. papierowej. Drugą istotną kwestią jest zmiana siatki terminologicznej. Pojęcie niedopuszczalności dochodzenia roszczeń zostanie zmodyfikowane na brak możliwości dochodzenia zaspokojenia roszczeń, które to pojęcie funkcjonuje na gruncie kodeksu cywilnego. Dla sądów planowane jest dodatkowo powstanie usługi pozwalającej na sprawdzenie historii weryfikacji danego numeru PESEL przez określone podmioty, ze wskazaniem wyniku i określeniem czasu w jakim dany podmiot otrzymał wynik weryfikacji. Do ustawy planowane jest także wprowadzenie i wprost odwołanie się do pojęcia konsumenta w rozumieniu kodeksu cywilnego, w celu rozwiania wątpliwości co do zakresu stosowania tych regulacji.

Nastąpią doregulowania w ustawie o spółdzielczych kasach oszczędnościowo-kredytowych i w ustawie o usługach płatniczych, aby unormowaniem otoczone zostały także kredyty płatnicze i kredyty w rachunku bankowym, obejmując tym instytucje pieniądza elektronicznego oraz małe instytucje kredytowe, które takie usługi mają poświadczyć. Wprowadzono wprost wyłączenie usługi sprawdzenia wyniku dotyczącego informacji o podmiocie weryfikującym czyjeś dane dla np. służb prowadzących postępowania. Rozszerzono katalog przypadków zastrzeżenia z urzędu numeru PESEL. W połowie lutego br. DZS planuje na stronie internetowej KPRM udostępnić pierwsze środowisko integracyjne, zapewniające możliwość zadawania pytań i testowania odpowiedzi w ramach weryfikacji zastrzeżenia numeru PESEL. Przewidziany został czas na dostosowanie się integratorów do usług bez negatywnych konsekwencji oraz na ewentualne postulaty z zakresu usprawnienia aspektów technicznych.

Po wystąpieniach przedstawicieli Departamentu Zarządzania Systemami KPRM, głos zabrał Pan Dyrektor Krzysztof Zieliński, który na początku swojej wypowiedzi wskazał, że projekt ustawy jest oceniony pozytywnie przez Urząd KNF. To dodatkowe narzędzie, które pozwoli zabezpieczyć się obywatelom przed działaniami przestępców czy cyberprzestępców, skutkującymi utratą środków finansowych. Przepisy ustawy chronią nie tylko klientów, ale także instytucje finansowe, ponieważ udzielane i niespłacane kredyty obciążają finansowo

podmioty udzielające tych kredytów. W pewnym stopniu projekt ustawy i narzędzie docelowo wprowadzone, ograniczą ryzyka zmierzające do wyłudzenia środków finansowych z wykorzystaniem kradzieży tożsamości. Zauważono, że projekt ustawy nie zabezpiecza wszystkich scenariuszy działalności cyberprzestępczej wyłudzających środki finansowe. Pan Dyrektor podał przykład tzw. fałszywych inwestycji. Z uwagi na bardzo dobre przygotowanie scenariuszy socjotechnicznych, obywatele chcą tak bardzo zainwestować pieniądze, że nawet jeżeli rozwiązanie blokowania nr PESEL zostanie wprowadzone, to z pewnością znajdą się scenariusze, które namówią obywateli do wyłączenia tej blokady. Pan Dyrektor wspominał także, że w ocenie Urzędu KNF nie będzie to narzędzie wykorzystywane przez większość społeczeństwa, a za wprowadzeniem go ustawą, powinna zmierzać również duża kampania informacyjna. Mając na uwadze informacje na temat działań cyberprzestępczych i modeli socjotechnicznych, osoby nieświadome mogą z tego narzędzia nie korzystać. Poza tym takie rozwiązanie może też dać mylną pewność, że zablokowanie swojego numeru PESEL zapewnia bezpieczeństwo we wszystkich aspektach korzystania z Internetu. Należy mieć świadomość, że wspomniana regulacja nie rozwiązuje problemu z włamaniem na konto bankowe i kradzieżą środków finansowych.

Kolejny element, który może być wykorzystywany przez przestępców we wspomnianych scenariuszach, to kampanie phishingowe czy kampanie socjotechniczne mówiące o blokadzie konta czy nr PESEL i zachęcające do kliknięcia w link. Ponadto zauważono istnienie ryzyka, że samo narzędzie spowoduje pewnego rodzaju ograniczenie swobód i wolności w zaciąganiu kredytów i z tego powodu pewna grupa osób zrezygnuje z zastrzeżenia nr PESEL.

Dostrzeganym zagrożeniem jest ryzyko ataków na infrastrukturę zapewniającą możliwość weryfikacji informacji o zastrzeżeniu numeru PESEL danego obywatela. Do rozważenia pozostaje po stronie infrastruktury zabezpieczenie całego systemu i procesu. Zatrzymanie udzielania pożyczek w związku z niedostępnością, awarią systemu lub działaniami zewnętrznymi wpłynie zarówno na podmioty rynku finansowego udzielające pożyczek, jak również spowoduje perturbacje społeczne.

Pani Dyrektor Anna Wojczakowska, przedstawiła stanowisko Urzędu KNF z perspektywy stabilności rynku finansowego. Odnosząc się do głosów, które pojawiły się w kontekście istotnego zmniejszenia popytu na kredyt konsumpcyjny, wskazała, że nie widać zagrożenia dla rynku finansowego w kontekście włączenia omawianej usługi. W ocenie Urzędu KNF ewentualne zmniejszenie impulsywnego kupowania nie będzie miało istotnej skali i nie będzie wpływało na istotne zmniejszenie popytu na kredyt. Należałoby się ograniczyć w ramach tych rozważań (jeżeli byłaby potrzeba natychmiastowego wyłączenia usługi) do kredytów głównie konsumpcyjnych na zakup towarów i usług, które w ramach portfeli banków zajmują ok. 2% całości należności gospodarstw domowych. Wydaje się, że więcej jest plusów związanych z włączeniem takiej usługi ze względu na bezpieczeństwo banków, ponieważ spłacalność kredytów zaciągniętych na osoby, nie będące w stanie ich uregulować jest utrudniona. Stwierdzono, że wprowadzenie omawianego rozwiązania pozwoli na wyeliminowanie bądź zmniejszenie transferu środków z banku do przestępców na koszt

klienta i finalnie poprawi kwestie jakości oraz stabilności bazy kredytowej banków w stopniu, w jakim jest ona narażona na tego typu działania przestępcze.

Pan Naczelnik P. Chiluta skomentował, iż ma świadomość braku możliwości uchronienia wspomnianym rozwiązaniem wszystkich osób. Być może tych najmniej świadomych uda się uchronić, np. osoby starsze.

Pani A. Gryszczyńska zwróciła uwagę na aspekt możliwości zastrzegania numerów PESEL niepełnoletnich, którzy mogą występować w obrocie gospodarczym oraz być właścicielami nieruchomości.

Pan Dyrektor M. Górski wskazał, że na podstawie informacji uzyskanych z rynku, nie wykazuje obaw o popularność usługi. Jedyna obawa obejmuje osoby, które są mniej wyedukowane w zakresie cyfryzacji. Pan Dyrektor wykazał zaskoczenie postulatem, aby usługę zastrzegania numeru PESEL aktywować w domyślny sposób. Być może należałoby częściowo wprowadzić takie rozwiązanie, jak np. domyślne zastrzeżenie PESEL dla danych grup.

Pan Dyrektor K. Zieliński odnosząc się do tej wypowiedzi wskazał, że lepiej jednak odejść od pomysłu różnicowania grup z uwagi na brak kryterium, którym można byłoby się posłużyć, aby nie narazić się na krytykę ze strony obywateli czy też mediów.

Jeden z członków Rady wyraził daleko idące wsparcie dla omawianej inicjatywy dostrzegając aspekt komunikacyjny, który jest niezwykle istotny. Wrażono obawę, że przy złym rozumieniu obywatele przestaną chronić PESEL, ze względu na świadomość jego zastrzeżenia, co jednak nie działa w stu procentach do wszystkich usług cyfrowych. Wskazano także na kwestie zapisów prawnych w zakresie regulacji dot. identyfikacji bądź uwierzytelnienia. Jako temat do dyskusji uznano zapewnienie spójności pomiędzy omawianą regulacją a np. unormowaniami dotyczącymi podpisów kwalifikowanych w Polsce, ponieważ w myśl dzisiejszych regulacji w podpisie kwalifikowanym umieszczany jest numer PESEL.

Pan Naczelnik P. Chiluta odniósł się do powyższej wypowiedzi wskazując, że projekt ustawy był przedmiotem obrad Komisji Wspólnej na Zespole Społeczeństwa Informacyjnego Rządu i Samorządu Terytorialnego, gdzie zostało wyrażone zadowolenie w imieniu samorządów z faktu, iż urzędnicy będą mieli narzędzie stwarzające możliwość zabezpieczenia się przed negatywnymi skutkami ujawnienia w podpisie numeru PESEL. Ponadto zweryfikowanie zastrzeżenia numeru będzie wymagało autentykacji.

Pani A. Gryszczyńska podziękowała za udział w tej ważnej dyskusji uznając, że temat wymaga dalszego i głębszego potraktowania.

Aspekty podmiotowości i praw dziecka w środowisku cyfrowym – Pan Konrad Ciesiołkiewicz; Pani Magdalena Bigaj, Prezeska Fundacji Instytut Cyfrowego Obywatelstwa oraz przedstawiciel Biura Rzecznika Praw Dziecka Pan Mecenass Tomasz Darkowski.

Pan Konrad Ciesiołkiewicz przedstawił prawa i podmiotowość dziecka w środowisku cyfrowym na podstawie rekomendacji Komitetu Praw Dziecka ONZ. Komitet Praw Dziecka przygotowuje tzw. komentarze ogólne, które precyzują i przekładają dane prawa dziecka na określony obszar. Odniesiono się do Komentarza nr 25 z 2021 r. dot. środowiska cyfrowego. Wskazano, że Konwencja opiera się czterech filarach. Podstawowa zasada konwencji to wymóg kierowania się dobrem dziecka, przed wszystkimi innymi grupami społecznymi, jako pierwszym filtrem, który powinny brać pod uwagę instytucje publiczne, organizacje czy przedsiębiorstwa.

W skrócie zostały omówione poszczególne filary, tj. dobro dziecka; zakaz dyskryminacji; prawo do życia, przeżycia i rozwoju oraz poszanowanie poglądów dziecka.

Konwencja o prawach dziecka zawiera art. 42 zobowiązujący państwa - strony tej Konwencji do promowania praw dziecka. W konsekwencji tego zapisu znajduje się we wspomnianych rekomendacjach punkt 125, który stanowi o zobowiązaniu do promowania praw dziecka w środowisku cyfrowym.

Pani Prezes Magdalena Bigaj na początku swojego wystąpienia wspomniała, że powód borykania się z różnymi problemami związanymi z podmiotowością dziecka w Internecie i podmiotowością użytkowników Internetu wynika z konieczności weryfikacji swojego podejścia do nowych technologii – nie są one tworzone jako neutralne narzędzia, których użycie zależy wyłącznie od nas. Najpopularniejsze serwisy, platformy i aplikacje projektowane są w taki sposób, aby pozyskiwać uwagę bez końca, wszystkimi możliwymi metodami, bez względu na koszty. Miarą sukcesu w świecie nowych technologii jest zasięg i zaangażowanie. Najbardziej bezbronną grupą wobec takich działań są dzieci i młodzież. Problemатyczne używanie nowych technologii ma w wielu przypadkach znamiona uzależnienia behawioralnego i takie skutki dla zdrowia.

Pani Prezes wspomniała, że strach przed nowymi technologiami, pejoratywizowanie ich czy demonizowanie również nie jest drogą do wypracowania standardu życia w ich otoczeniu, ponieważ one nie przestaną funkcjonować w naszym życiu.

Obecnie jesteśmy w drodze od biomasy do podmiotu. Od zeszłego roku widać zintensyfikowanie działań związanych z odzyskaniem podmiotowości w świecie cyfrowym. Nie istnieje świat wirtualny, czyli mniej prawdziwy, do którego należałoby przywiązywać mniejszą wagę. Po regulacjach na poziomie europejskim można dostrzec jednak, że w pewien sposób to tak funkcjonowało. W roku 2000 powstał akt o handlu elektronicznym, obowiązujący przez prawie 22 lata. Dopiero w zeszłym roku powstały akty Digital Services Act i Digital Markets Act. Poza tym brakuje globalnych dobrych praktyk i skutecznych rozwiązań systemowych chroniących dzieci i młodzież. Oprócz tego zauważany jest brak

kompleksowej edukacji cyfrowej społeczeństwa, a w związku z tym błędne przekonania na temat nowych technologii. W badaniach widać, że przede wszystkim niewłaściwe używanie urządzeń ekranowych jest problemem we wszystkich grupach wiekowych. Niewydukowani dorośli modelują zachowania dzieci i nie potrafią wprowadzić ich w świat cyfrowy. Nastolatki spędzają w sieci średnio (dane z NASK) 4h 50m dziennie. Co 10. spędza 8 h i więcej. Badania pokazują, że poziom higieny cyfrowej osób dorosłych jest bardzo niski we wszystkich grupach wiekowych. W efekcie niskiej świadomości społecznej mamy coraz wcześniejszy wiek pierwszego kontaktu z pornografią - np. dziś jest to 11 lat. Ponadto istnieje zjawisko normalizacji seksualizacji przekazu, a także rośnie skala cyberprzemocy. W efekcie niewłaściwego używania urządzeń ekranowych oraz ich zaprojektowania mamy do czynienia z degradacją wszystkich obszarów dobrostanu – zarówno poczucia własnej wartości, wpływu na otaczający świat, bycia częścią społeczeństwa, ale również negatywnego wpływu na zdrowie fizyczne.

Dominujący przekaz obciąża odpowiedzialnością za negatywne skutki używania ekranów wyłącznie ich użytkowników. Regulacje i wymagania wobec twórców i współtwórców są niewystarczające. Gdyby biznes nowo technologiczny był odpowiedzialny społecznie, to Deklaracja Praw Dziecka czy Konwencja Praw Dziecka zawiera wystarczające zapisy dotyczące sposobu tworzenia produktów internetowych sprzyjających dziecku. Społeczeństwo informacyjne funkcjonuje w pewnym środowisku cyfrowym, składającym się z twórców, współtwórców i użytkowników, z czego tworzy się wspólne dobro, które jest wspólną odpowiedzialnością dla wszystkich kształtujących przestrzeń cyfrową.

Pani Prezes wspomniała, że ideą w której upatruje przyszłość w zakresie uregulowania globalnie wskazanej sytuacji jest cyfrowe obywatelstwo, stawiające w centrum rozwoju technologii człowieka a nie biznes, nakazujące postrzeganie oraz ocenianie sposobu projektowania produktów przez pryzmat sprzyjania zdrowiu człowieka. Cyfrowe obywatelstwo to postawa świadomego i odpowiedzialnego tworzenia oraz używania nowych technologii z korzyścią dla siebie i społeczeństwa.

W dalszej części wypowiedzi przytoczona została definicja higieny cyfrowej stworzonej na podstawie materiału i dorobku naukowego - higiena cyfrowa to korzystne dla zdrowia zachowania związane z używaniem technologii informacyjno-komunikacyjnych, zwłaszcza Internetu i urządzeń ekranowych. W Instytucie Cyfrowego Obywatelstwa stworzono narzędzie pomiarowe, tj. Test Higieny Cyfrowej. To narzędzie certyfikowane naukowo z pozytywną opinią Komisji Etyki Badań Naukowych Warszawskiego Uniwersytetu Medycznego, które zostanie zaprezentowane wraz z wynikami badań Ogólnopolskiego Badania Higieny Cyfrowej na początku marca br. Wymieniono także trzy wymiary cyfrowego obywatelstwa, tj. indywidualny, społeczny i systemowy.

Pan Konrad Ciesiońkiewicz zapytał Pana mec. Tomasza Darkowskiego czy w Biurze Rzecznika Praw Dziecka ma miejsce koordynacja działań dot. praw człowieka w rozumieniu praw dziecka w środowisku cyfrowym, bądź czy jest próba objęcia koordynacją tego obszaru przez działalność Biura.

Pan mec. Tomasz Darkowski odpowiedział, że Biuro Rzecznika Praw Dziecka od kilku lat jest aktywne na forach także związanych z cyfryzacją i z ochroną praw dziecka. Kilka projektów legislacyjnych było konsultowanych z Biurem. Przede wszystkim prawa dziecka są w Polsce chronione konstytucją. W ramach działalności BRPD skupia się na wszystkich aspektach praw dziecka, a kwestia cyfryzacji przestała być wyodrębnionym tworem. Podstawowym odbiorcą wszystkich technologicznych nowinek są dzieci. Rodzice są w stanie bardziej się kontrolować, natomiast dzieci poświęcają praktycznie całe swoje życie technologiom informatycznym. Ta technologia staje się wypełnieniem każdego aspektu, łącznie z aspektem dojrzwania. BRPD skupia się również na sprawach indywidualnych, gdzie zauważalne są coraz częściej pojawiające się problemy związane z wykorzystaniem Internetu. Interweniuje zarówno przed sądami jak i instytucjami administracyjnymi. W Biurze powstaje raport jakości życia dzieci, gdzie zbierany jest szereg informacji o potencjalnych zagrożeniach i od momentu wprowadzenia edukacji zdalnej pojawiły się w raportach sygnały, że kwestia nadmiernego korzystania z technologii powoduje bardzo znaczący spadek jakości życia psychicznego dzieci. Z tego m.in. powodu powołano telefon zaufania, który lawino zwiększył liczbę interwencji po wprowadzeniu zdalnej edukacji. Korzystając z tych dwóch źródeł zauważono kwestię problemu higieny cyfrowej, ale także kwestię realizacji podstawowych uprawnień dziecka. W obrocie cyfrowym mamy do czynienia z ludźmi, którzy są niepełnoletni, ale są identyfikowani jako pełnoletni. Jest to bardzo duże narażenie na niebezpieczeństwo. Pan mec. nawiązał do wypowiedzi Pani Prezes w kwestii nastawienia dużych koncernów na czerpanie zysków. To dzieci są najczęściej ofiarami prostych gier nastawionych na szybkie bodźcowanie, a następnie na niewielkie wydatki rzędu kilku złotych na elementy powodujące natychmiastowe pozytywne bodźcowanie takiego dziecka. Kolejnym poruszonym problemem był seksting. Jest to zjawisko pozostające poza świadomością większości społeczeństwa, natomiast dzieci nie widzą w nim zagrożenia.

Pan mec. odpowiadając na pytanie o koordynacje wskazał, że BRPD stara się działać, ale nie dostrzega konieczności wyodrębnienia osobnego biura do spraw informatyzacji, z uwagi na pojawianie się tych aspektów w odniesieniu do każdego elementu działania BRPD.

Pan mec. wspomniał, że BRPD jest otwarte na współpracę z Radą.

Jeden z członków Rady zwrócił uwagę, że warto zastanowić się z jakiego powodu Internet tak bardzo przyciąga młodzież i dzieci. Pojawia się pytanie, czy dla tych treści w Internecie, dla ich możliwości i współczesnych rozwiązań jest alternatywa w postaci wartościowych materiałów, które równie mocno angażowałyby w naukę, rozwijanie zainteresowań i zdolności. Zwrócono uwagę, że było wiele projektów, np. Program Rozwoju Talentów Informatycznych, gdzie wytworzone zostały wspaniałe materiały informatyczne. Projekt obecnie nie jest kontynuowany.

Wskazane zostało, że powstają inicjatywy w kontekście tworzenia alternatywnej przestrzeni bezpiecznego i spokojnego środowiska dla dzieci i młodzieży. Warto wprowadzić pewne rozwiązania i zastanowić się, jak skonsolidować różne aktywności, słuszne działania i wszelkiego typu inwencje twórcze w tym obszarze.



## Uczestnicy posiedzenia:

### Członkowie Rady:

1. Izabela Albrycht
2. Katarzyna Chałubińska-Jentkiewicz
3. Konrad Ciesiołkiewicz
4. Andrzej Dulka
5. Agnieszka Gryszczyńska
6. Janusz Kosiński
7. Anna Beata Kwiatkowska
8. Mirosław Maj
9. Dariusz Milka - Wiceprzewodniczący
10. Aleksandra Musielak
11. Józef Orzeł - Przewodniczący
12. Bolesław Piasecki
13. Robert Trętowski
14. Mateusz Tykierko

### Zaproszeni goście:

15. Krzysztof Zieliński, Dyrektor Departamentu Cyberbezpieczeństwa w Urzędzie Komisji Nadzoru Finansowego
16. Anna Wojczakowska, Zastępca Dyrektora Departamentu Bankowości Komercyjnej w Urzędzie Komisji Nadzoru Finansowego
17. Paweł Jaskulski, BNP Paribas Bank Polska SA, CSIRT – Digital Fraud
18. Maciej Górski, Dyrektor Departamentu Zarządzania Systemami w KPRM
19. Katarzyna Kopytowska, Zastępca Dyrektora Departamentu Zarządzania Systemami w KPRM
20. Przemysław Chiluta, Naczelnik Wydziału Zarządzania Danymi i Jakości Usług Departamentu Zarządzania Systemami w KPRM
21. Magdalena Bigaj, Prezeska Fundacji Instytut Cyfrowego Obywatelstwa
22. Mecenas Tomasz Darkowski, przedstawiciel Biura Rzecznika Praw Dziecka
23. Jarosław Mojsiejuk, ekspert Rady

Sekretariat Rady i pracownicy Kancelarii Prezesa Rady Ministrów:

24. Natalia Matyba, Zastępca Dyrektora Departamentu Polityki Cyfrowej w KPRM
25. Michał Sołek, Radca Prawny, Departament Zarządzania Danymi w KPRM
26. Katarzyna Stopińska, KPRM
27. Joanna Laskowska, KPRM