PROTOKÓŁ z XVII posiedzenia Rady do Spraw Cyfryzacji, które odbyło się 22 listopada 2019 roku, o godzinie 11:00 w siedzibie Ministerstwa Cyfryzacji.

Przedstawienie raportu ”Internet Rzeczy - Polska Przyszłości” przygotowanego przez Grupę ds. IoT – Pan Paweł Gora

Pan Paweł Gora swoje wystąpienie zaczął od przedstawienia twórców raportu - Grupy roboczej ds. Internetu Rzeczy (GRIOT). Wskazał, że Grupa zainaugurowała swoją działalność 24 sierpnia 2018r., a jej głównym celem jest[1] *wypracowanie rekomendacji działań, jakie rząd RP powinien podjąć dla zapewnienia warunków rozwoju i upowszechnienia wykorzystania technologii IoT, bazujących na polskiej myśli technicznej, służących poprawie jakości życia w Polsce oraz zagwarantowaniu przewagi konkurencyjnej polskiej gospodarki na rynkach międzynarodowych, ze szczególnym uwzględnieniem wsparcia promocji polskich innowacyjnych firm na świecie*. *Prace Grupy koncentrują się na następujących obszarach:*

- *analiza potrzeb polskiej gospodarki związanych z zastosowaniem IoT i wskazanie konkretnych rozwiązań, które powinny być wdrożone na szczeblu ministerstwa i rządu,*
- *wsparcie w wypracowaniu przez ministerstwo rozwiązań, mających stymulować rozwój firm, produktów i usług związanych z IoT,*
- *wskazanie barier prawnych, ograniczających rozwój IoT,*
- *zdefiniowanie obszarów wymagających wprowadzenia standardów i regulacji dla harmonizacji tej części rynku.*

W pracach Grupy uczestniczyło ponad 100 ekspertów *reprezentujących firmy inwestujące w produkty i usługi związane z IoT w Polsce oraz sektory gospodarki, których rozwój jest uzależniony od tych rozwiązań. W stale uzupełniany skład Grupy weszli też przedstawiciele branżowych izb gospodarczych, środowisk naukowych, związków i zrzeszeń pracodawców oraz organizacji społecznych*. Prace toczyły się w 10 podgrupach: Ogólna, Bezpieczeństwo i Certyfikacja, Finanse i Ubezpieczenia, Inteligentne Miasta i Budynki, Ochrona Zdrowia, Inteligentne Opomiarowanie, Przemysł, Rolnictwo i Ochrona Środowiska, Telekomunikacja, Transport, Logistyka i Pojazdy Autonomiczne

Efektem prac grupy jest raport, który został oficjalnie opublikowany 2 lipca 2019 r.

W raporcie omówione zostały perspektywy rozwoju branży IoT na świecie, warunki rozwoju IoT w Polsce (diagnoza sytuacji), kontekst strategiczny, branże o szczególnym potencjale rozwoju w Polsce w oparciu o IoT, analiza branż, kierunki dalszych działań.

Pan Paweł Gora podkreślił, że grupa zidentyfikowała ponad 110 barier związanych z wdrażaniem technologii IoT w danej branży i wskazała ok. 130 konkretnych propozycji działań rządu,

[1] Kursywą cytaty z raportu

aby usunąć te bariery. Postulowano konkretne zmiany prawne - np. zmiana ustawy Prawo o ruchu drogowym, umożliwiająca stosowanie narzędzi zautomatyzowanego nadzoru nad ruchem (w tym detekcji wykroczeń) przez zarządcę infrastruktury (miasto) w odniesieniu do obszaru objętego ustanowioną strefą czystego transportu. Wskazano również projekty badawczo-rozwojowe i rekomendacje ogólne:

- opracowanie zaleceń dla uczelni otwierających kierunki studiów związane z technologią IoT, w zakresie kształcenia ekspertów o adekwatnych do potrzeb rynku umiejętnościach,
- stworzenie przy Ministerstwie Cyfryzacji inkubatora projektów IoT,
- stworzenie Krajowego Zintegrowanego Systemu Wspierania Innowacji, który prowadziłby innowatorów „od pomysłu do przemysłu",
- stworzenie mechanizmu finansowania innowacji polegającego na dofinansowaniu wdrożeń pilotażowych i projektów PoC dla użytkowników końcowych, obejmującego innowacyjne produkty zarówno startupów, jak i firm dojrzałych,
- zapewnienie odpowiedniej infrastruktury do przesyłania danych między urządzeniami IoT oraz do przechowywania i przetwarzania danych.

Pomysły i propozycje wykroczyły znacznie poza wąsko rozumiany "Internet Rzeczy".

Obecnie prace w ramach grupy roboczej są kontynuowane. Prace toczą się w 3 podgrupach tematycznych: ds. legislacji, standaryzacji, projektów i finansowania. Przygotowywany jest wykaz projektów priorytetowych (głównie w obszarze Smart Cities), który zostanie skonsultowany z Ministrem Cyfryzacji.

Zaznaczone zostało, że warto zastanowić się nad rozwiązaniami systemowymi, które mogą pomóc w realizacji rekomendowanych działań i projektów. Wskazane zostało, że Rada mogłaby zająć się stworzeniem propozycji rozwiązań systemowych, które ułatwiłyby wdrażanie, zastosowanie tych rekomendacji, które zostały zawarte w raporcie.

Przewodniczący zauważył, że należy spojrzeć na Internet Rzeczy jako na nowy „przemysł usług" oraz pomyśleć czy nie powinna to być nowa struktura, nowy sposób zarządzania innowacjami. Wskazał, że być może należałoby znaleźć dla IoT odrębne rozwiązanie polityczne, organizacyjne, prawne oraz finansowe.

W toku dyskusji pojawiło się także pytanie o odbiorcę, do którego miałyby trafić rekomendacje grupy. Stwierdzono, że rekomendacje są skierowane do Rządu, ponieważ ten obszar dotyczy wielu branż i potrzebne są rozwiązania systemowe. Pomysły priorytetowe mają szansę zostać zrealizowane, a pozostałe kwestie czekają na swoich koordynatorów.

Przewodniczący zauważył, że potrzebny jest nie tyle inkubator usług Internetu Rzeczy przy Ministerstwie Cyfryzacji – gdyż Internet Rzeczy jest na tyle szeroką dziedziną, że wchodzi w branżowe, techniczne uwarunkowania, że MC musiałoby się stać „małym rządem eksperckim", żeby móc to rozwiązanie zbudować. Potrzebny jest inkubator rynku Internetu Rzeczy –

a kiedy ten rynek już będzie, to pojawi się konkurencja, metody finansowania oraz współpraca z zagranicą. IoT stanie się jedną z najszybciej rozwijających się dziedzin.

Zauważono, że kompetencją MC byłoby zapanowanie nad procesem certyfikacji cyberbezpieczeństwa dla Internetu Rzeczy - aby obywatele czuli się bezpiecznie korzystając z elementów IoT. Obecny na posiedzeniu Dyrektor Jacek Paziewski wskazał, że w kwestii Internetu Rzeczy MC szuka tych przestrzeni, gdzie konieczna jest ingerencja państwa i gdzie pojawiają się konieczne do usunięcia bariery.

Zwrócono uwagę na to, że mogą zaistnieć działania, które mogą zahamować, spowolnić lub uniemożliwić rozwój Internetu Rzeczy albo pewne jego elementy – mowa o działaniach legislacyjnych, które są obecnie prowadzone na poziomie UE (rozporządzenie ePrivacy).

Dyskusja na temat walki z cyberprzestępczością - wystąpienia:

- Panów insp. Mariusza Lenczewskiego, Dyrektora Biura do walki z cyberprzestępczością KGP oraz insp. Sławomira Szumilasa, Zastępcy Dyrektora Biura do walki z cyberprzestępczością KGP - „Główne problemy zwalczania cyberprzestępczości w Polsce”

  Pan Dyrektor Mariusz Lenczewski swoje wystąpienie zaczął od przestawienia rysu historycznego - w związku z tym, że przestępczość dużym krokiem weszła w cyberprzestrzeń (sieć teleinformatyczną) z wykorzystaniem różnego rodzaju technologii, Komendant Główny Policji w 2014 r. podjął decyzję o utworzeniu w każdej Komendzie Wojewódzkiej Policji wydziału do walki z cyberprzestępczością. Dokonano dużej selekcji i doboru osób, które posiadają wiedzę informatyczną i programistyczną w zakresie współpracy międzynarodowej. W czerwcu 2016 r. Komendant Główny Policji powołał Pełnomocnika do spraw utworzenia biura do walki z cyberprzestępczością, które to miało z pozycji KGP koordynować pracę i czynności podjęte przez wydziały do walki z cyberprzestępczością. Zajął się on współpracą międzynarodową z organami ścigania, z Prokuraturą Krajową, z Europolem, Interpolem, ze wszystkimi komórkami cyber w policji w Europie i na świecie.

  Biuro do walki z cyberprzestępczością powstało 1 grudnia 2016 r. Jak zaznaczył Pan Dyrektor Mariusz Lenczewski od tego czasu dużo spraw zostało zrealizowanych - zakończyły się ustaleniem wielu sprawców oraz pociągnięciem ich do odpowiedzialności. W trakcie prowadzonych czynności służbowych, nie tylko przez pion do walki z cyberprzestępczością, napotkano na wiele problemów. Sprawcy, którzy dokonują przestępstw w cyberprzestrzeni, monitorują sieć - internet pod kątem wyłapywania informacji o realizacjach, o tym w jaki sposób został zatrzymany sprawca, w jaki sposób popełnił błędy. Poprzez takie działania sprawcy uczą się, szukają nowych rozwiązań oraz możliwości. Problemy te dotyczą nie tylko organów polskich, także Europy i całego świata.

  Obecnie w ramach Biura do walki z cyberprzestępczością KGP podejmuje różnego rodzaju kroki, spotkania, konsultacje w sektorze prywatnym, prawnym, bankowym -

wszędzie tam, gdzie zagrożenie cyberprzestępczości jest obecne. Podejmowane są próby uzyskania jak największych możliwości, zwiększających efektywność działań Policji. Na bazie doświadczeń stwierdzono, że należałoby rozważyć dokonanie zmian w ustawie prawo telekomunikacyjne oraz ustawie o świadczeniu usług drogą elektroniczną.

W wystąpieniu zaznaczono, że cyberprzestępczość bardzo się rozwija i może dotyczyć każdego użytkownika w sieci. Wśród tych użytkowników są dzieci. Istnieje więc potrzeba podjęcia kroków, aby ograniczyć przestępstwa, a także zwiększyć możliwości organów ścigania w zakresie ustalania sprawców przestępstw. Pan Dyrektor zauważył, że przepisy dwóch w/w ustaw powodują, że w dużym zakresie niektóre dane techniczne towarzyszące ruchowi sieciowemu są niemożliwe do pozyskania i w rezultacie ustalenia użytkownika dopuszczającego się przestępstwa. Z tego względu, aby wymóc takie zadania na operatorach czy dostawcach usług elektronicznych muszą być dokonane zmiany prawne.

- Pani Agnieszki Gryszczyńskiej - „Kradzież tożsamości”

  Pani Agnieszka Gryszczyńska zaczęła od wyjaśnienia, że tożsamości nie da się ukraść, ponieważ nie jest rzeczą – można jedynie wykorzystać cudzą tożsamość. Omówiła art. 190 a § 2 Kodeksu karnego, stanowiący, że karze pozbawienia wolności do lat 3 *podlega, kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek lub inne jej dane osobowe w celu wyrządzenia jej szkody majątkowej lub osobistej*.

  Podkreślone zostało, że w wymienionym przepisie warto zwrócić uwagę na wielokrotne użycie słowa „jej”. Oznacza to, że żeby podlegać odpowiedzialności karnej ktoś musi wykorzystać dane (bądź wizerunek) konkretnej osoby i jednocześnie chcieć wyrządzić tej konkretnej osobie szkodę. Co więcej, wymagany jest zamiar bezpośredni kierunkowy, czyli że sprawca musi działać w kierunku wyrządzenia szkody tej osobie, której tożsamość wykorzystuje. Zaznaczone zostało, że taka interpretacja art. 190 a § 2 kk zgodna jest z orzecznictwem sądowym.

  Pani A. Gryszczyńska omówiła problemy praktyczne. Wskazała, że istnieje możliwość kupienia wielu danych - osobowych, haseł, przejętych kont. Dane osobowe są tanie i są sprzedawane masowo, zarówno na forach w DarkWeb jak również na portalach internetowych powszechnie dostępnych. Oferowane są zarówno bazy danych, dane do logowania do kont poczty elektronicznej czy portali społecznościowych jak również rachunki bankowe założone na dane innych osób. Omówiony został także problem rejestracji kart SIM - wspomniano, że brak jest odpowiedzialności za nieprzerejestrowanie karty SIM czy ich rejestrację z podaniem innych danych niż dane rejestrującego. Często też do rejestracji wykorzystywane są dane przypadkowych osób. Wiele jest przy tym obserwowanych metod pozyskiwania danych oraz ich monetyzacji.

  Wykorzystywanie cudzej tożsamości obserwowane jest w prawie każdej kategorii spraw karnych – w tym w szczególności w sprawach z zakresu cyberprzestępczości.

Podszywanie się pod inne osoby jest mechanizmem wykorzystywanym przez sprawców, mającym na celu ukrycie własnej tożsamości czy skierowanie działań ze strony organów ściągania na inne osoby. Żeby wyeliminować problemy należałoby dokonać zmian legislacyjnych – w szczególności karnoprawnej odpowiedzialności za kradzież tożsamości, czy obowiązków podmiotów świadczących usługi drogą elektroniczną – w szczególności w zakresie gromadzenia i przekazywania uprawnionym organom logów i danych osób korzystających z usług (ustalenie zakresu przechowanych danych, standaryzacja udostępnianych organom ścigania danych, okres retencji danych).

Podkreślone zostało, że należy walczyć z cyberprzestępczością wieloaspektowo, ponieważ jest to skomplikowane i złożone zjawisko.

W toku dyskusji po w/w wystąpieniach pojawiła się sugestia wprowadzenia takich zmian w przepisach, które określałyby, jakiego rodzaju dane powinny być wprowadzane w systemach tak, aby łatwiej było ustalić tożsamość sprawcy czynu.

Zauważono, że potrzebny jest dialog z przedsiębiorcami, przedstawicielami operatorów na temat procesów uzyskiwania od nich danych niezbędnych do obsługi incydentu i ustalenia sprawców czynów zabronionych. Istnieją duże koszty w związku z obsługą zapytań od organów ścigania. Problem, który zgłaszają przedsiębiorcy jest taki, że otrzymują zapytania dotyczące tej samej sprawy z różnych miejsc, każde dotyczy innego zakresu danych, każde musi być obsługiwane niezależnie od siebie. Gdyby wprowadzono ustrukturyzowanie tych zapytań tak, aby było wiadomo, jaki zakres danych jest wymagany, to taki przedsiębiorca może wysłać jedną odpowiedź w kilka miejsc, co obecnie jest niemożliwe. Takie rozwiązanie ograniczyłoby koszty i zwiększyły chęć do współpracy ze strony przedsiębiorców. Pojawiła się propozycja zaproszenia do rozmów małych i dużych przedsiębiorców, którzy są proszeni o udostępnianie danych retencyjnych.

Cyberprzestępczość rozwija się w szybkim tempie, powinna więc powstać instytucja, która analizowałaby problemy prawne, techniczne i organizacyjne w tym zakresie. Rozwijająca się międzynarodowa cyberprzestępczość będzie coraz groźniejsza.

Przedstawienie stanu badań nad AI w Polsce (raport OPI) – Pan Sebastian Szymański

Pan Sebastian Szymański na wstępie odniósł się do raportu „Rozwój sztucznej inteligencji w sektorze nauki w Polsce", przygotowanego przez Ośrodek Przetwarzania Informacji. Raport zgodnie z deklaracjami autorów obejmuje okres lat 2013-2018 i przedstawia stan przygotowania uczelni i ośrodków naukowych w Polsce do prowadzenia badań nad sztuczną inteligencją oraz ich oferty edukacyjne w zakresie kształcenia specjalistów.

Wskazane zostało, że obraz stanu badań przedstawiony w raporcie przedstawia skalę zainteresowania problematyką sztucznej inteligencji w społeczności badaczy w różnych dyscyplinach, jednak nie daje informacji w jakim stopniu przytoczona w raporcie liczba publikacji dot. AI odzwierciedla realnie prowadzone badania w Polsce oraz w jakim stopniu publikacje te

funkcjonują w naukowym obiegu światowym. Podkreślono, że w statystykach w skali światowej zaobserwować można gwałtowny wzrost liczby badaczy zajmujących się tą dziedziną oraz liczby publikacji na ten temat. W Polsce pozostaje ona od 5 lat na stałym poziomie, co oznacza, że w Polsce niewiele się w tym zakresie dzieje.

Pan Sebastian Szymański zaznaczył, że wydaje się, że przedstawione w raporcie informacje są zbyt optymistyczne. Wskazał, że w Narodowym Centrum Nauki od 2011 r. zrealizowano łącznie 229 projektów zawierających w opisie słowo kluczowe „sztuczna Inteligencja/AI". Struktura finansowania ww. projektów, która w NCN odbywa się w panelach, przedstawia się następująco:

- Panel HS (nauki humanistyczne): 108 projektów,
- Panel NZ (nauki o życiu): 5 projektów
- Panel ST (nauki techniczne): 116 projektów, w tym ST6 (informatyka i technologie informacyjne): 98 projektów.

Podkreślone zostało, że jedynie 4 dofinansowane projekty dotyczą społecznych konsekwencji sztucznej inteligencji.

Pan Sebastian Szymański szacuje, że wysokość wszystkich nakładów na wszystkie projekty związane z AI od 2011 roku to ok. 120 mln zł. Natomiast szacunkowa średnia wysokość rocznych nakładów na wszystkie projekty związane z AI od 2011 roku to ok. 13 mln zł.

Analizując raporty roczne Narodowego Centrum Badań i Rozwoju zidentyfikowano 2 projekty związane ze sztuczną inteligencją dofinansowane przez NCBiR:

- 2017: Projekt Airly – dotyczący opracowania i implementacji efektywnej prognozy i monitoringu zanieczyszczeń powietrza w oparciu o techniki AI przy użyciu danych z rozległej sieci pomiarowej,
- 2019: Platforma GPW Data jako innowacyjny system wykorzystujący techniki sztucznej inteligencji celem wspierania decyzji inwestycyjnych na rynku kapitałowym - stworzenie bazujących na nowoczesnych technologiach, w tym AI, usług wspierających emitentów i inwestorów giełdowych

Poruszony został również temat nakładów na doktoraty dotyczące AI. W Polsce jest przewidzianych 30 doktoratów wdrożeniowych, co oznacza przyznanie stypendiów w wysokości 3,5/4,5 tys. zł./mies.

Wymieniono również główne przeszkody w rozwoju badań nad AI, jakimi są niski poziom finansowania i brak finansowania dedykowanego, rozproszenie badaczy i zespołów badawczych, brak dedykowanych programów studiów, brak dedykowanych programów doktoranckich, utrudnienia w pozyskiwaniu środków na projekty interdyscyplinarne, brak wiedzy o aktualnym stanie badań nad AI.

Podkreślone zostało, że dobrze byłoby np. zwrócić się do NCBiR o podanie solidnych statystyk dotyczących tego, jakie działania związane z AI są podejmowane – Przewodniczący poprosił o określenie pytań i tematów do poruszenia podczas rozmowy z NCBiR.

Uczestnicy posiedzenia:

Członkowie Rady:

1. Joanna Adamczyk
2. Jacek Czarnecki
3. Paweł Gora
4. Agnieszka Gryszczyńska
5. Anna Beata Kwiatkowska
6. Tomasz Łukawski
7. Dariusz Milka
8. Józef Orzeł - Przewodniczący
9. Włodzimierz Schmidt
10. Sebastian Szymański

Zaproszeni goście:

11. Insp. Mariusz Lenczewski, Dyrektor Biura do walki z cyberprzestępczością KGP
12. Insp. Sławomir Szumilas, Zastępca Dyrektora Biura do walki z cyberprzestępczością KGP
13. Tomasz Iwanowski, Prokurator Prokuratury Krajowej
14. Jan Kostrzewa, Dyrektor Biura Cyberbezpieczeństwa w Ministerstwie Sprawiedliwości
15. Robert Kośla, Dyrektor Departamentu Cyberbezpieczeństwa w MC
16. Wiesław Paluszyński, ekspert
17. Jarosław Mojsiejuk, ekspert
18. Krzysztof Komorowski, ekspert
19. AndrzejRęgowski, ekspert

Sekretariat Rady i pracownicy Ministerstwa Cyfryzacji:

20. Jacek Paziewski, Dyrektor Biura Analiz i Projektów Strategicznych w MC
21. Katarzyna Stopińska MC
22. Joanna Laskowska MC