Zeszyty Prawnicze
17.1 / 2017

SPRAWOZDANIA

STRATEGIA CYBERBEZPIECZEŃSTWA DLA POLSKI. ASPEKTY INSTYTUCJONALNE I PRAWNE. SPRAWOZDANIE Z VIII KONFERENCJI NAUKOWEJ Z CYKLU BEZPIECZEŃSTWO W INTERNECIE

W dniach 19-20 maja 2016 roku odbyła się w Warszawie VIII edycja konferencji z cyklu „Bezpieczeństwo w Internecie". Tematem była „Strategia cyberbezpieczeństwa dla Polski. Aspekty instytucjonalne i prawne". Organizatorami konferencji byli Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie, Generalny Inspektor Ochrony Danych Osobowych, Ministerstwo Spraw Wewnętrznych i Administracji oraz Naukowe Centrum Prawno-Informatyczne.

Konferencja miała szczególny charakter nie tylko ze względu na poruszane zagadnienia, ale także ze względu na udział wybitnych ekspertów, zarówno teoretyków, jak i przedstawicieli praktyki. W skład Komitetu Naukowego VIII edycji konferencji weszli: Prof. Andrzej Adamski – UMK; Prof. Tomasz Bąkowski – UG; Min. Edyta Bielak-Jomaa – GIODO; Ks. prof. Stanisław Dziekoński – Rektor UKSW; Prof. Jerzy Cytowski – Prorektor UKSW; Prof. Paweł Fajgielski – KUL; Mec. Tomasz Grzegory – Google Polska; dr inż. Wacław Iszkowski – Prezes PIIT; Prof. Jerzy Kosiński – WSPol; Prof. C. Martysz – UŚ, Kolegium NIK; Gen. bryg. Włodzimierz Nowak – Pełnomocnik Ministra Cyfryzacji ds.Cyberbezpieczeństwa; Prof. Stanisław Piątek – UW; Prezes Krzysztof Pietraszkiewicz – ZBP; Prof. Bolesław Szafrański – WAT; prof. Grażyna Szpor – UKSW; Dr Wojciech Wiewiórowski – UG, Z-ca EIOD, Tomasz Zdzikot – Wiceminister Spraw Wewnętrznych i Administracji.

Członkowie Komitetu Naukowego i zaproszeni goście uczestniczyli w dniu 19 maja w sesji eksperckiej poświęconej podsumowaniu kończącego się projektu „Model regulacji jawności i jej ograniczeń w demokratycznym państwie prawnym", zainicjowanego i współfinansowanego przez Narodowe Centrum Badań i Rozwoju.

Uroczystego otwarcia obrad plenarnych w dniu 20 maja dokonał Jego Magnificencja ks. prof. Stanisław Dziekoński, Rektor UKSW. Ksiądz Rektor podziękował za tworzenie środowiska osób zajmujących się cyberbezpieczeństwem i scharakteryzował zagrożenia związane z obecną rewolucją informacyjną oraz rolę Uniwersytetu w stwarzaniu przyjaznej przestrzeni do debaty, pozwalającej na wyrażanie rozmaitych poglądów i proponowanie śmiałych rozwiązań.

Pani dr Edyta Bielak-Jomaa, Generalny Inspektor Ochrony Danych Osobowych, podkreśliła coraz większą rolę danych osobowych w rozwijaniu innowacyjnych usług dla społeczeństwa oraz wiążące się z tym niebezpieczeństwa w cyberprzestrzeni. Pani Minister zwróciła uwagę na działalność Komisji Europejskiej, której celem jest budowanie zaufania obywateli do usług cyfrowych, a także na zmiany, jakie wprowadzają nowe przepisy z zakresu ochrony danych osobowych. Omówiła ponadto możliwe konflikty pomiędzy ochroną danych osobowych a działaniami na rzecz cyberbezpieczeństwa.

Minister Tomasz Zdzikot, Podsekretarz Stanu w Ministerstwie Spraw Wewnętrznych i Administracji, przedstawił działalność resortu na rzecz ochrony cyberprzestrzeni, w tym realizację zaleceń zawartych w raporcie Najwyższej Izby Kontroli oraz udział Ministerstwa w tworzeniu założeń strategii cyberbezpieczeństwa. Pan Minister podkreślił wagę współpracy między sektorem publicznym i prywatnym oraz konieczność współpracy między gestorami państwowej infrastruktury krytycznej.

Zastępca Europejskiego Inspektora Ochrony Danych, dr Wojciech Wiewiórowski, zwrócił uwagę, że kwestia bezpieczeństwa informacyjnego wymaga ciągłej przebudowy, gdyż bardzo szybko traci na aktualności. Wskazał, że kolejną wielką rewolucją, która nas czeka, jest Internet rzeczy. Organizacja dorocznych konferencji „Bezpieczeństwo w Internecie" przyczyniła się do tworzenia środowiska osób zajmujących się kwestiami bezpieczeństwa informacyjnego, co jest szczególnie

istotne dla Polski, która musi przeciwdziałać zagrożeniom płynącym z cyberberprzestrzeni.

Prof. Marek Michalski, Dziekan Wydziału Prawa i Administracji UKSW, zauważył, że dziewiętnastowieczny aksjomat prywatności, który nakazywał wierzyć, że żyjemy w zamkniętym otoczeniu, nagle został przełamany przez to, co dzieje się dookoła nas i wkracza w życie prywatne. Dodał, że działalność Wydziału, a w szczególności Pani prof. Grażyny Szpor i Katedry Prawa Informatycznego, nakierowana jest na badanie tej rzeczywistości, nie tylko normatywnej. Organizowane tu konferencje mają wymiar interdyscyplinarny, co stanowi wartość dla przedsięwzięć naukowych, dlatego że w efekcie zmierzają do usystematyzowania złożonej rzeczywistości, która zaskakuje nas swą dynamiką.

Po wystąpieniach organizatorów konferencji rozpoczęła się część merytoryczna. Obrady plenarne podzielono na pięć sesji, obejmujących zagadnienia: organizacji ochrony cyberprzestrzeni RP, prawnych aspektów ochrony sieci i informacji, metod i technik zwalczania cyberprzestępczości, stanu i perspektyw ochrony publicznej infrastruktury informacyjnej, terroryzmu i cyberterroryzmu.

Sesję pierwszą „Organizacja ochrony cyberprzestrzeni RP" wystąpieniem na temat systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej" rozpoczął dyr. Piotr Januszewicz z Ministerstwa Cyfryzacji, przedstawiając działania z zakresu cyberbezpieczeństwa realizowane przez Ministerstwo Cyfryzacji. Prezentacja odnosiła się do celu budowy narodowego systemu bezpieczeństwa cyberprzestrzeni, filozofii budowy oraz funkcjonowania tego systemu w różnych stanach zagrożenia państwa. Pan dyrektor podkreślił, że dla zapewnienia bezpieczeństwa konieczne jest osadzenie zasad dotyczących bezpieczeństwa w systemie prawnym i w Ministerstwie Cyfryzacji trwają prace nad projektem ustawy o cyberbezpieczeństwie. Zwrócił również uwagę na konieczność zmiany spojrzenia na budowę systemów, które powinny być zorientowane na bezpieczeństwo i usługi. Prelegent wskazał, że obecnie istnieje konieczność stworzenia systemu, który będzie mógł reagować na materializację zagrożeń w cyberprzestrzeni. Wyjaśniając poszczególne fazy materializacji zagrożeń i tak zwaną czasową skuteczność systemów bezpieczeństwa, omówił rozwiązania strukturalne narodowego systemu

bezpieczeństwa cyberprzestrzeni oraz rolę Ministerstwa Cyfryzacji jako koordynatora przedsięwzięcia.

Wystąpienie prof. Zbigniewa Cieślaka z UKSW, „Bezpieczna administracja", odnosiło się do spojrzenia na administrację publiczną już po wprowadzeniu skutecznego systemu obrony cyberprzestrzeni. Celem wystąpienia było wskazanie, co wynika ze struktury administracji, a także omówienie problemów związanych z informacją jako narzędziem oraz informacją będącą przedmiotem działań administracji publicznej. Prof. Zbigniew Cieślak scharakteryzował pojęcie administracji w znaczeniu przedmiotowym jako funkcję państwa polegającą na realizowaniu przez podmioty administrujące wskazanych ustawowo wartości, oraz w znaczeniu podmiotowym, jako usystematyzowany zbiór podmiotów administrujących o różnym statusie prawnym realizującym wartości ustawowe. Wskazał, że powyższy podział identyfikuje różne wymiary stanu bezpieczeństwa informacyjnego administracji, rozumianej jako państwo i obywatele. Prof. Zbigniew Cieślak podsumował, że wspólnym mianownikiem dla obu spojrzeń na administrację jest stabilność, pewność, płynność, brak zakłóceń w jej funkcjonowaniu oraz skuteczność.

Temat „Cztery filary dopuszczalnej ingerencji w prawo do prywatności w ramach działań cyberobronnych" prezentował pan doktor Wojciech Wiewiórowski, Zastępca Europejskiego Inspektora Ochrony Danych. Zwrócił on uwagę na istniejący w Europie konflikt między wartościami, które chcielibyśmy chronić: bezpieczeństwem oraz prywatnością i możliwością samodzielnego decydowania o tym, co nas dotyczy, bez wpływu i ingerencji oraz dyskryminacji, którą miałaby wprowadzić jakakolwiek instytucja publiczna. Wskazał na znaczenie art. 31 i 49 Konstytucji dla dyskusji o ochronie bezpieczeństwa w cyberprzestrzeni oraz istnienie w Europie schematu zachowania, umożliwiającego ingerencję państwa w prywatność obywateli w celu ochrony ich bezpieczeństwa, a zarazem zachowanie wartości konstytucyjnych. Odniósł się do ingerencji państwa w prawo do prywatności, w oparciu o cztery filary: przetwarzanie danych osobowych w celu zapewnienia bezpieczeństwa osób (I), przetwarzanie danych osobowych, które jest niezbędne i proporcjonalne dla uzasadnionych potrzeb (II), istnienie

organu nadzorczego, będącego w stanie panować nad tym, w jaki sposób przetwarzanie danych osobowych następuje (III), istnienie efektywnej możliwości zaskarżenia działań, z której może korzystać indywidualna osoba fizyczna (IV).

Pierwszą sesję zakończył referatem „Rola organizacji pozarządowych w budowaniu cyberbezpieczeństwa państwa." dr inż. Wacław Iszkowski, Prezes Polskiej Izby Informatyki i Telekomunikacji. Omawiając zagadnienia doktryny bezpieczeństwa teleinformatycznego, za istotną uznał odpowiedź na pytanie, czy z prawnego punktu widzenia dozwolone jest podejmowanie przez państwo środków zapobiegawczych, tzn. dokonywanie ataków na sieci komputerowe w celu niszczenia infrastruktury potencjalnego przestępcy. Prelegent podkreślił wagę tworzenia przez państwa centrów zapasowych dla głównych systemów teleinformatycznych i zapewnienie bezpieczeństwa osobom pracującym przy systemach.

Drugą sesję, „Prawne aspekty ochrony sieci i informacji", rozpoczął pan prof. Bolesław Szafrański z Wojskowej Akademii Technicznej w Warszawie. W wystąpieniu „Zwalczanie cyberprzestępczości a statystyczne zastosowania baz danych" wskazał, że istotą bezpieczeństwa w statystyce publicznej jest takie skonstruowanie państwowego systemu, żeby dostęp do informacji w ramach prawa był zapewniony. Podkreślił znaczenie zapewnienia Głównemu Urzędowi Statystycznemu wpływu na porządkowanie infrastruktury informacyjnej państwa, bez czego nie będzie można prowadzić wiarygodnych analiz porównawczych zarówno krajowych jak i międzynarodowych. Zwrócił też uwagę na potrzebę wprowadzenia jednolitej regulacji odnoszącej się do cyberbezpieczeństwa.

Kolejne wystąpienie dotyczyło „Europejskich standardów ochrony sieci i informacji oraz ich implementacji do prawa polskiego". Pan prof. Andrzej Adamski z Uniwersytetu Mikołaja Kopernika w Toruniu podkreślił, że w polskim kodeksie postępowania karnego brakuje przepisów, które realizowałyby postanowienia Konwencji Rady Europy w zakresie walki z cyberprzestępczością. Zauważył również, że w Kodeksie postępowania karnego nie ma podstawy prawnej do żądania przez sądy czy prokuratury danych internetowych, co powoduje, że trzydzieści procent zapytań dotyczących tych danych spotyka się z odmową ich

udostępnienia z uwagi na to, że organy nie podają podstawy prawnej albo podają błędną. Prof. Andrzej Adamski wyjaśnił też cele wprowadzenia dyrektywy z 2013 roku dotyczącej ataków na systemy informatyczne oraz problemy jej transpozycji do prawa polskiego.

Profesor Czesław Martysz z Uniwersytetu Śląskiego w Katowicach podjął problem „Dostosowania regulacji informatyzacji wykonywania zadań publicznych do nowych zagrożeń." Wskazał, że dla uporządkowania regulacji dotyczących informatyzacji konieczne byłoby albo stworzenie kodeksu informacyjnego (model idealny) albo należałoby uchwalić akty wiodące, dotyczące prawa informatycznego i ochrony tajemnic (model realny). Pan Profesor Martysz wymienił również najistotniejsze zmiany, jakie są konieczne do wprowadzenia w obecnych przepisach dotyczących informatyzacji.

Pan Jacek Kowalski z BEREC *(The Office of the Body of European Regulators for Electronic Communications)*, prezentował „Regulację rozwoju Internetu rzeczy w prawie telekomunikacyjnym". Odniósł się do tego prawa w kontekście obowiązków regulacyjnych i oceny ich zastosowania wobec użytkowników Internetu rzeczy. Rozważając, czy wobec podmiotów świadczących usługi Internetu rzeczy rozporządzenie roamingowe znajdzie zastosowanie, jako przykład podał sytuację, w której urządzenie korzysta z mobilnej usługi dostępu do sieci lub usług telekomunikacyjnych. Omówił też mechanizmy zastosowane w rozporządzeniu: możliwość zablokowania przez operatorów telekomunikacyjnych dostępu do usług, gdy roaming jest wykorzystywany w sposób niestandardowy i wprowadzenie „Polityki Uczciwego Korzystania". Podkreślił, że obowiązki nakładane na Internet rzeczy powinny być szacowane finansowo, aby nie powodować blokady usług.

Temat „Prawo a etos cyberprzestrzeni" został przedstawiony przez pana doktora Karola Dobrzenieckiego z Uniwersytetu Mikołaja Kopernika w Toruniu. Celem było wyjaśnienie fenomenu cyberprzestrzeni, na który składa się między innymi rozwój technologiczny, wzmocnienie sieci społecznej oraz tak zwany „bezczasowy czas". Referent opisał zjawisko stanów odmiennej świadomości. Podkreślił, że technologia informacyjna zmienia sposób postrzegania rzeczywistości, co przejawia się chociażby w przyzwyczajaniu się do braku kontaktu fizycznego

w relacjach międzyludzkich. Zwrócił też uwagę, że powinniśmy badać, w jaki sposób zmiany prawa w zakresie nowych technologi wpływają na etos społeczeństwa.

Sesję trzecią rozpoczęła pani doktor Maria Podolska z Urzędu Komunikacji Elektronicznej referatem „Neutralność sieci w kontekście bezpieczeństwa." Na początku omówiła rozporządzenie o neutralności sieci i jego relację do bezpieczeństwa. Zwróciła uwagę na wagę pojęcia definicji otwartości Internetu oraz na obowiązek traktowania dostawców usług ruchu jednakowo, bez dyskryminacji i ograniczeń. Wskazała na istniejące w tym zakresie akceptowalne i nieakceptowalne naruszenia neutralności sieci (samozarządzanie ruchem, priorytetyzacja ruchu). Odniosła się również do sposobów zarządzania ruchem celem zapewnienia integralności i bezpieczeństwa sieci oraz przedstawiła obowiązki Urzędu Komunikacji Elektronicznej w związku z wprowadzonym rozporządzeniem.

Pan dr Kamil Czaplicki z UKSW podjął temat „Kradzież tożsamości a metody jej identyfikacji.". Odnosząc się do wirtualnej kradzieży tożsamości, podkreślił, że narażony na kradzież tożsamości jest każdy użytkownik Internetu, a przestępstwo to jest zjawiskiem powszechnym, występującym m.in. w portalach społecznościowych, e-handlu, e-bankowości. Scharakteryzował trzy metody identyfikacji: opartą na tym, co wiemy (hasła, loginy, piny), na tym, co posiadamy (smart phony, karty zdrapki), na tym, kim jesteśmy (metoda biometryczna). Wyraził pogląd, że najbardziej skuteczną metodą jest wielopoziomowa metoda biometryczna.

Tematem prezentacji pani doktor inżynier Agnieszki Gryszczyńskiej z UKSW były „Publiczne rejestry a cyberprzestępczość". Prelegentka, będąca też prokuratorem, podkreśliła, że istnieje problem braku definicji przestępstwa komputerowego, a w kodeksie karnym zostały uregulowane tylko takie cyberprzestępstwa, jak hacking czy naruszenie tajemnicy korespondencji. Wskazała, że przy udostępnianiu danych rejestrowych on-line i innych zasobów danych nie wzięto pod uwagę zagrożeń związanych z wykorzystaniem danych w innym celu niż cel, dla którego pierwotnie zostały zebrane. Zwróciła uwagę na potrzebę weryfikacji zakresu i szczegółowości danych podlegających publikacji

on-line, redefinicji pojęcia jawności formalnej rejestrów i rozważenia modeli dostępu.

Zamykający sesję referat „Próba oceny zwalczania cyberprzestępczości w Polsce" wygłosił pan profesor Jerzy Kosiński z Wyższej Szkoły Policji w Szczytnie. Omówił sukcesy policji w zakresie wykrywania cyberprzestępstw na przykładzie portalu internetowego „zaufana trzecia strona". W oparciu o przeprowadzone badania wskazał, że ogólna liczba cyberprzestępstw rośnie, a wykrywalność przestępstw przeciwko poufności, integralności i dostępności danych maleje. Podkreślił też, że sukcesy w policji w zakresie rozpracowywania cyberprzestępstw wiążą się z powstałą w Komendzie Głównej Policji komórką prowadzącą prace analityczne. Pan profesor odniósł się do sukcesów w zwalczeniu cyberprzestępczości Komendy Głównej Policji oraz Wyższej Szkoły Policji, dzięki której powstało Centrum Analityczno–Wywiadowcze Doskonalenia Zwalczania Cyberprzestępczości.

Sesję czwartą, „Stan i perspektywy ochrony publicznej infrastruktury informacyjnej", rozpoczęło wystąpienie pana doktora Macieja Szmita oraz pani doktor inżynier Dominiki Lisiak-Felickiej z Uniwersytetu Łódzkiego: „Zarządzanie bezpieczeństwem informacji w urzędach." Przedstawiono wyniki badań przeprowadzonych w latach 2012-2015, które wykazały brak spójnego systemu zgłaszania incydentów związanych z bezpieczeństwem informacji, niejednorodność standardów, w oparciu o które budowane są systemy zarządzania bezpieczeństwem informacji oraz niejednorodność dokumentacji. Podkreślono, że problemy w urzędach wiążą się też z niedostateczną świadomością cyberzagrożeń, brakiem jednolitej procedury zgłaszania incydentów i jednolitego systemu obrony.

Kolejny temat, „Przeciwdziałanie cyberatakom przez przedsiębiorstwa", prezentowała pani doktor Jowita Sobczak ze Społecznej Akademii Nauk w Warszawie. Omówiła ochronę infrastruktury krytycznej i jej wpływ na wizerunek przedsiębiorców. Wymieniła istniejące problemy przedsiębiorstw, takie jak brak wystarczającej świadomości w obszarze wprowadzenia systemu bezpieczeństwa informacji, podejmowanie działań po wystąpieniu incydentu, przeświadczenie, że cyberzagrożenia dotyczą wyłącznie dużych korporacji. Podkreśliła, że zagrożenia, będące

największym wyzwaniem, jeśli chodzi o złośliwe oprogramowanie, z którymi będą mierzyć się przedsiębiorstwa, to ataki typu ATP. Pani doktor stwierdziła, że dla bezpieczeństwa informacji niezbędne jest podnoszenie świadomości pracowników, zapobieganie incydentom, regularny monitoring i przegląd bezpieczeństwa.

Pan doktor Piotr Sitniewski z Krajowej Szkoły Administracji Publicznej w wystąpieniu „Dostęp do informacji publicznej a cyberbezpieczeństwo" skupił się na analizie przepisów ustawy o dostępie do informacji publicznej. Wyjaśnił, co w praktyce oznacza ustanowiony w art. 8 ust. 4 sposób dostępu do informacji publicznej, oraz podkreślił, że celem przepisu jest „ucywilizowanie" składania wniosków o dostęp do informacji publicznej, które byłoby możliwe poprzez wprowadzenie wyłącznie obowiązującego formularza. Odniósł się też do art. 12 ust. 2 ustawy, wskazując na problemy dotyczące interpretacji poszczególnych form udostępniania informacji publiczej. Postulował zmianę przepisów, która pozwoliłaby na odciążenie sądów od udzielania odpowiedzi, czy dany wniosek został skutecznie złożony.

Następnie pan Piotr Trąbiński z Narodowego Centrum Studiów Strategicznych omawiał „Nowe trendy w ochronie cyberprzestrzeni". Cechą charakterystyczną cyberprzestrzeni jest to, że podmioty przenoszą swoje „życie" do sieci, a zagrożenia w niej występujące nie należą jednej kategorii, a szczególnie specyficzne niebezpieczeństwa wiążą się z Internetem rzeczy. W Polsce rozpoczeły się działania na rzecz wdrażania strategii cyberbezpieczeństwa, w tym implementacji dyrektywy NIS. Prelegent wskazał, że *big data* może być środkiem służącym ochronie cyberprzestrzeni oraz że konieczna jest zmiana sppjrzenia państwa na cyberbezpieczeństwo z defensywnego na ofensywny.

Sesję zamykał pan profesor Giovanni Bianco z Uniwersytetu w Bari prezentacją „Cyberprzestępstwa we Włoszech". Po wyjaśnieniu etymologii słowa „cyber" podkreślił, że wielką wartością w dzisiejszym świecie jest informacja. Wskazał, że największym zagrożeniem dla cyberbezpieczeństwa są ludzie oraz że firmy zatrudniają hakerów po to, żeby sprawdzać skuteczność działania swoich systemów. Cyberprzestępczość we Włoszech została także ukazana na przykładzie przestępstwa dokonanego przez firmę Telekom.

Ostatnią, piątą sesję konferencji rozpoczął pan magister inżynier Krzysztof Świtała referatem „Terroryzm i cyberterroryzm". Scharakteryzował pojęcia terroru i cyberterroryzmu, wskazał kraje najbardziej dotknięte przez terroryzm i najważniejsze ataki terrorystyczne w ostatnim dziesięcioleciu (zamach w Monachium podczas igrzysk olimpijskich, zamach nad Lockerbie, zamach w Madrycie, wybuchy w Londynie, zamachy w Oslo, ataki w Paryżu oraz zestrzelenie malezyjskiego samolotu na terytorium Ukrainy)m a także poziomy ataków (logiczne, socjotechniczne oraz ataki na fizyczną infrastrukturę informatyczną). Omówił również najważniejsze ataki cyberterrorystyczne ostatnich lat (m.in. w Estonii i w Gruzji oraz atak stuxnet).

Temat „Walka z terroryzmem w kontekście ochrony konstytucyjnych praw i wolności jednostki" został zaprezentowany przez pana magistra Kamila Stępniaka. Referent podkreślił, że ochrona życia, prawo do prywatności, wolność wyznawania swoich poglądów, wolność zrzeszania się, prawo do ochrony zdrowia to prawa najbardziej zagrożone przez działania ograniczające terroryzm. Omówił również wprowadzone zmiany do francuskiej konstytucji po zamachach w Paryżu w listopadzie 2015 roku.

Pani Katarzyna Beśka z Koła Naukowego „Forum Prawa Publicznego" referowała „Co zmieni ustawa antyterrorystyczna". Omówiła kompetencje poszczególnych organów administracji. Scharakteryzowała przepisy uprawniające władze publiczne do inwigilacji cudzoziemców i możliwości ich wydalenia z Polski. Przedstawiła kontrowersje związane z wymogiem podania swych danych przy wykupie karty pre-paid i możliwością zablokowania na okres do 30 dni przez szefa Agencji Bezpieczeństwa Wewnętrznego strony internetowej w celu wykrywania i zapobiegania przestępstwom o charakterze terrorystycznym.

Pan magister inżynier Piotr Kolmann z Wojskowej Akademii Technicznej referował problemy „Edukacji społeczeństwa wobec zagrożenia terrorystycznego". Wskazał sposoby prowadzenia edukacji na temat zagrożeń terrorystycznych w społeczeństwie oraz miejsca, w których można znaleźć informacje na temat działań zapobiegawczym takim atakom. Wnioskował, że celem edukacji jest oswojenie się z zagrożeniem oraz zapewnienie gotowości do racjonalnego działania w sytuacji jego

wystąpienia. Zdaniem referenta edukacja terrorystyczna jest równie istotna jak środki organizacyjno-techniczne.

Temat „Polityka cyberbezpieczeństwa w świetle zagrożenia cyberterroryzmem" prezentował pan magister Marcin Skolimowski. Odnosząc się do penalizacji terroryzmu i cyberterroryzmu, wskazał, że polskie prawo nie przewiduje jednego aktu stanowiącego o tych zagadnieniach. Podkreślił, że kluczowe znaczenie dla ochrony przed cyberterroryzmem ma zabezpieczenie infrastruktury krytycznej. Omówił również działalność Ministerstwa Obrony Narodowej w zakresie przeciwdziałania cyberterroryzmowi oraz przedstawił działalność Agencji Bezpieczeństwa Wewnętrznego i Służby Kontrwywiadu Wojskowego w ramach ochrony informacji niejawnych i bezpieczeństwa systemów teleinformatycznych.

Pan Dawid Durak z Uniwersytetu Jagielońskiego wygłosił referat „Czy cyberterroryzm jest realnym zagrożeniem?". Wskazał na charakterystyczne cechy cyberterroryzmu, takie jak relatywnie niskie koszty materialne, anonimowość, specyficzne cechy środowiska informatycznego, psychologię i socjologię, czynnik ludzki oraz globalność. Podał także miejsca najbardziej zagrożone atakami. Podkreślił, że dotychczas większość zaistniałych zdarzeń nie wypełniła nawet w osiemdziesięciu procentach definicji cyberterroryzmu.

Temat „Regulacje prawne dotyczące zwalczania cyberprzestępczości w Polsce oraz Unii Europejskiej", prezentowany był przez panią Izabelę Wilk z FPP, która wskazała na znaczenie dyrektyw 97/66 z 2007 roku i 2002/58 z 2002 roku. Zwróciła też uwagę na decyzję ramową Rady w sprawie ataków na systemy teleinformatyczne z 2005 roku oraz na dyrektywę 2006/24. Prelegentka odniosła się również do przedstawionej przez Komisję Europejską w dniu 28 kwietnia 2015 roku agendy bezpieczeństwa na lata 2015-2020.

Pani Klara Dygaszewicz z FPP w referacie "Kradzież tożsamości" przedstawiła definicje kradzieży tożsamości. Wymieniła zagrożenia wiążące się z kradzieżą tożsamości w działaności bankowej i administracji (np. zameldowania cudzoziemców pod fałszywym adresem) oraz zaznaczyła, że istnieje konieczność skoordynowanych działań na poziomie krajowym, które angażowałyby do przeciwdziałania kradzieży

tożsamości administrację publiczną i podmioty gospodarcze w różnych sektorach.

Dr Michał Leciak z Uniwersytetu Mikołaja Kopernika w Toruniu omówił „Spójność karnoprawnej ochrony informacji istotnych dla bezpieczeństwa państwa". Wskazał na mankamenty krajowych regulacji polegające na tym, że zagrożenia określonych dóbr, w szczególności związanych z dawną tajemnicą państwową, mogą być różnie klasyfikowane przez obecne przepisy karne. W odniesieniu do tej niespójności omówione zostały problemy: podmiotu (sprawcy), znamion, kary i ścigania oraz zadane zostało pytanie o zasadność uzależniania ochrony prawnokarnej od faktu nadania odpowiedniej klauzuli tajności.

Referat "Profilowanie a cyberbezpieczeństwo" przedstawiła pani magister Elżbieta Niezgódka. Po wyjaśnieniu pojęcia cyberbezpieczeństwa (*sensu stricto* i *sensu largo*) omówiła ostatnie zmiany w przepisach dotyczących ochrony danych osobowych w kontekście profilowania (rozporządzenie 679/2016 oraz dyrektywa 680/2016). Referentka podjęła także kwestię, czy profilowanie może opierać się na danych anonimowych.

Konferencję zakończył referat „Polski model regulacji jawności i jej ograniczeń a obronność i bezpieczeństwo państwa." Pani prof. Grażyna Szpor zwróciła uwagę, że następuje jurydyzacja jawności i jej ograniczeń, podkreślając jednocześnie, że skoro mamy społeczeństwo informacyjne, gospodarkę informacyjną, to coraz więcej aktów prawnych odnosi się do tych zagadnień. Dla rozwiązania wielu problemów stosuje się zarówno instrumenty publicznoprawne jak i prywatnoprawne. Regulacje tworzone na potrzeby zasobów analogowych w coraz większym stopniu odnoszą się do zasobów cyfrowych, a dominację w dysponowaniu tymi zasobami straciła już administracja na rzecz biznesu. Istotne jest też przejście od regulacji jednopoziomowej, krajowej, w kierunku wielopoziomowej. Transgraniczność stosunków informacyjnych także wiąże się z potrzebą zmian regulacji. Mieliśmy prawo dobrze osadzone w przestrzeni realnej, ale obecnie przenoszenie danych w Chmurę [cloud computing], oznacza, że nie wiemy, gdzie nasze dane się znajdują i jakiej jurysdykcji są poddane. Nasilają się konflikty informacyjne i związane z cyberprzestrzenią zagrożenia bezpieczeństwa a skuteczność prawa w ich rozwiązywaniu maleje, do czego przyczynia się pogłębianie

rozproszenia krajowej regulacji. W przezwyciężaniu tych trudności może być użyteczne zapoznanie się z wynikami projektu badawczo–rozwojowego „Model regulacji jawności i jej ograniczeń w demokratycznym państwie prawnym", pod adresem internetowym www.mrj.uksw.edu.pl, w tym z bibliografią obejmującą blisko 4000 publikacji, prezentacjami wybitnych specjalistów oraz przejściem do pełnotekstowych opracowań dotyczących wszystkich obowiązujących tajemnic prawnie chronionych.

Na zakończenie prof. Grażyna Szpor podkreśliła, że udział około 400 osób w konferencji potwierdza znaczenie podjętych problemów i podziękowała władzom publicznym za współorganizację, a uczestnikom za przyjęcie zaproszenia.

Elżbieta Niezgódka*

* Uniwersytet Kardynała Stefana Wyszyńskiego.