PRAWO W DZIAŁANIU
SPRAWY KARNE
47/2021
DOI: 10.32041/pwd.4715

Tomasz Bojanowski, Klaudia Łuniewska, Bartłomiej Oręziak, Joanna Repeć, Iryna Prystenska*

Sprawozdanie z Międzynarodowej Konferencji Naukowej „V4CyberPower". Warszawa, 3–4 grudnia 2020 r.**

W dniach 3–4.12.2020 r. odbyła się międzynarodowa konferencja naukowa zatytułowana „V4CyberPower". Wydarzenie zostało zorganizowane przez Centrum Analiz Strategicznych Instytutu Wymiaru Sprawiedliwości (IWS), przy wsparciu Ministerstwa Sprawiedliwości (MS). Konferencja odbyła się w ramach projektu badawczego pt. „Cyberbezpieczeństwo Grupy Wyszehradzkiej na rzecz zapobiegania przyczynom przestępczości" współfinansowanego ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości.

V4CyberPower to pierwsza edycja międzynarodowego forum wymiany wiedzy i doświadczeń, na którym wybrzmiały najważniejsze głosy branży informatycznej krajów Grupy Wyszehradzkiej (V4). Dyskusje panelistów wytyczyły nowe kierunki rozwoju i pozwoliły znaleźć wspólne rozwiązania, które przyspieszą konieczne procesy informatyzacji państw członkowskich Grupy Wyszehradzkiej, a także zracjonalizują politykę tych państw dotyczącą sfery cyberbezpieczeństwa.

Konferencja została poświęcona tematyce cyberprzestępczości oraz sposobom jej zapobiegania w ujęciu międzynarodowym. Wydarzenie składało się z licznych podsekcji. Prelegenci w ramach wygłaszanych referatów wskazali w szczególności na metody walki z cyberprzestępczością czy wykorzystanie obecnej sytuacji panującej na świecie w atakach socjotechnicznych. Poruszone zostały kwestie związane z zagadnieniem spójności regulacji na poziomie unijnym, problematyki skutecznego zwalczania kradzieży tożsamości w aspekcie retencji danych, w tym

* Tomasz Bojanowski jest studentem na Wydziale Prawa i Administracji, Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie, Polska, ORCID: 0000-0001-8294-0968, e-mail: tomaszbojanovski@gmail.com; mgr Klaudia Łuniewska jest absolwentką Wydziału Prawa i Administracji, Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie, Polska, ORCID: 0000-0002-3546-3414, e-mail: klaudiakarolinaluniewska@gmail.com; mgr Bartłomiej Oręziak jest doktorantem w Katedrze Ochrony Praw Człowieka i Prawa Międzynarodowego Humanitarnego, Wydział Prawa i Administracji, Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie, Polska, ORCID: 0000-0001-8705-6880, e-mail: boreziak@gmail.com; mgr Joanna Repeć jest aplikantką adwokacką w Izbie Adwokackiej w Warszawie oraz absolwentką Wydziału Prawa i Administracji, Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie, Polska, ORCID: 0000-0002-9091-7888, e-mail: repecjoanna@gmail.com; mgr Iryna Prystenska jest absolwentką Wydziału Prawa i Administracji, Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie, Polska, e-mail: iprystenska@gmail.com

** Data zgłoszenia tekstu przez autorów: 2.04.2021 r.; data przyjęcia tekstu przez redakcję do publikacji: 7.07.2021 r.

również w kontekście rozstrzygnięć Trybunału Sprawiedliwości Unii Europejskiej (TSUE). W trakcie obrad omówione zostały istotne zagadnienia dotyczące tematyki cyberbezpieczeństwa oraz roli, jaką pełni ona jako kluczowy element w koncepcji bezpieczeństwa państwa.

Ponadto konferencja stworzyła możliwość zaprezentowania dotychczasowych rezultatów projektu oraz wymiany myśli i poglądów dotyczących problematyki cyberbezpieczeństwa oraz zapobiegania i przeciwdziałania zjawisku cyberprzestępczości.

Projekt badawczy pt. „Cyberbezpieczeństwo Grupy Wyszehradzkiej na rzecz zapobiegania przyczynom przestępczości" oraz organizowana w ramach niego konferencja „V4CyberPower" miały przede wszystkim na celu wymianę doświadczeń pomiędzy reprezentantami państw Grupy Wyszehradzkiej w zakresie cybersecurity, a także prezentację najnowszych technologii wytwarzanych w V4, jak również rozwój naukowy w Grupie Wyszehradzkiej.

Realizacja wyżej określonych działań projektowych stworzyła szansę na poprawę bezpieczeństwa państwa przed cyberatakami. Jest to prawdopodobne w szczególności z uwagi na możliwość wymiany wiedzy i doświadczeń międzynarodowych oraz edukację prawną w zakresie dotyczącym bezpieczeństwa sieci teleinformatycznych, a także wzmocnienie pozycji Polski w zakresie potencjału ludzkiego w branży IT na arenie międzynarodowej.

Pierwszy dzień konferencji otworzył swoim przemówieniem **Podsekretarz Stanu w Ministerstwie Sprawiedliwości dr Marcin Romanowski.** Minister powitał wszystkich gości, wskazał na wagę zagadnień poruszanych na konferencji dla funkcjonowania współczesnego państwa. Podkreślił także, że niezwykle istotna jest wymiana doświadczeń w zakresie walki z cyberprzestępczością oraz w celu poprawy cyberbezpieczeństwa w naszym obszarze geograficznym, ponieważ może to mieć przełożenie na zapobieganie i przeciwdziałanie przestępczości. Następnie głos zabrał **dr hab. Marcin Wielec – Dyrektor Instytutu Wymiaru Sprawiedliwości,** który także podziękował gościom za zainteresowanie tematyką konferencji oraz zaangażowanie wszystkich osób, które realizują projekt badawczy pt. „Cyberbezpieczeństwo Grupy Wyszehradzkiej na rzecz zapobiegania przyczynom przestępczości". Następnie Dyrektor IWS odniósł się do kwestii merytorycznych, ściśle powiązanych z przedmiotem projektu i dokonał prezentacji referatu poświęconego wpływowi regulacji międzynarodowych na zwalczanie przyczyn przestępczości w dobie nowoczesnych technologii, gdzie wskazał na szanse oraz zagrożenia płynące z coraz silniejszej pozycji prawa międzynarodowego na krajowe uregulowania w zakresie zwalczania cyberprzestępczości.

Pierwszy panel został poświęcony inicjatywom mającym na celu zwiększenie cyberbezpieczeństwa. Dyskusja podjęta w ramach tej części konferencji dotyczyła zagadnień fundamentalnych z perspektywy funkcjonowania państwa w realiach postępującej informatyzacji i cyfryzacji, a także silnej tendencji do ujednolicania mechanizmów prawnych i pozaprawnych w obszarze funkcjonowania Unii Europejskiej. W ramach pierwszego panelu głos zabrali: wspomniany **dr Marcin Romanowski, dr Ökrös Oszkár** (Podsekretarz Stanu w Ministerstwie Sprawiedliwości Węgier), **Jan Kostrzewa** (Dyrektor Biura Cyberbezpieczeństwa w MS), **dr hab. Szymon Pawelec, prof. UW** (kierownik Zakładu Międzynarodowego Postępowania

Karnego WPiA Uniwersytetu Warszawskiego) oraz **dr inż. Rafał Lizut** (Katolicki Uniwersytet Lubelski). W tym panelu omówione zostały inicjatywy, które miała na celu poprawę cyberbezpieczeństwa w państwach Grupy Wyszehradzkiej, ze szczególnym uwzględnieniem rozwiązań, które są wdrażane w Polsce i na Węgrzech. Zagadnienia zostały omówione zarówno z perspektywy decydentów, specjalistów, jak i naukowców.

Następnie głos zabrał **Koordynator Centrum Analiz Strategicznych Instytutu Wymiaru Sprawiedliwości oraz Kierownik Międzynarodowego Projektu Badawczego pt. „Cyberbezpieczeństwo Grupy Wyszehradzkiej na rzecz zapobiegania przyczynom przestępczości" mgr Bartłomiej Oręziak** (Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie), który w ramach swojego wystąpienia omówił główne założenia i cele projektu badawczego. Dalszą część swojej wypowiedzi poświęcił przedstawieniu referatu pt. **„Rozwój nowoczesnych technologii jako wyzwanie dla przeciwdziałania przyczynom przestępczości"**, gdzie wskazał, że rozwój nowoczesnych technologii nie jest jednowymiarowy i może mieć zarówno pozytywny, jak i negatywny wpływ na działalność organów administracji publicznej w zakresie dotyczącym przeciwdziałania przyczynom przestępczości.

Jako następna referat wygłosiła **mgr Agnieszka Karczmarz** (przedstawicielka Polski w Komitecie Obrony Cybernetycznej NATO, Komitecie Planowania Cywilnego i Komitecie Polityki Operacyjnej), która w swoim wystąpieniu zaprezentowała perspektywę NATO dotyczącą zjawiska cyberbezpieczeństwa. W przemówieniu odniesiono się do problematycznych kwestii, nad którymi współpracują sygnatariusze Paktu Północnoatlantyckiego.

Kolejny panel poświęcono metodom walki z cyberprzestępczością. Wzięli w nim udział funkcjonariusze Policji w osobie **nadkom. Tomasza Pawlickiego** (naczelnik Wydziału Rozpoznania Biura do Walki z Cyberprzestępczością Komendy Głównej Policji) oraz **kom. Agnieszki Stąpór** (ekspertka Wydziału Rozpoznania Biura do Walki z Cyberprzestępczością Komendy Głównej Policji). Prelegenci dokonali omówienia metod podejmowanych oraz wdrażanych przez polską Policję w zwalczaniu cyberprzestępczości.

Jako kolejna wystąpiła **dr hab. inż. Agnieszka Gryszczyńska** (Katedra Prawa Informatycznego WPiA UKSW, prokurator del. do Prokuratury Regionalnej w Warszawie), która zaprezentowała referat pt. **„Wykorzystanie COVID-19 w atakach socjotechnicznych".** W ramach wystąpienia dokonano omówienia zagadnień dotyczących całego społeczeństwa. Stwierdzono, że pandemia koronawirusa miała wpływ na życie każdej jednostki i wymusiła przeniesienie aktywności do internetu. Brak doświadczenia w zakresie informatyzacji i cyfryzacji sprawiło, że wiele osób stało się łatwym celem ataków socjotechnicznych.

W dalszej części konferencji głos zabrał **dr inż. Rafał Lizut**, który wygłosił przemówienie pt. **„Bezpieczeństwo państwa bezpieczeństwem obywateli? Wyzwania cyber (nie)bezpieczeństwa i obsługi danych"**. W trakcie wystąpienia poruszono aktualne zagadnienia wpływu sprawnego funkcjonowania instytucji publicznych na życie indywidualne jednostki w aspekcie cyberbezpieczeństwa. Prelegent wskazał, że mimo niechęci do obecności państwa w życiu prywatnym, w dzisiejszych okolicznościach państwo musi aktywnie dbać o bezpieczeństwa publiczne, bo tylko w ten sposób może zapewnić bezpieczeństwo wszystkim obywatelom.

Jako następny prelegent wystąpił **dr Blaža Markelja** (adiunkt Studiów nad Bezpieczeństwem na Wydziale Wymiaru Sprawiedliwości w Sprawach Karnych i Bezpieczeństwa, Uniwersytet w Mariborze, Słowenia). Podczas swojej prelekcji omówił problematykę urządzeń mobilnych, które są niezbędnym elementem dzisiejszego rozwoju technologii. W referacie wskazał, dlaczego tak ważna jest edukacja w zakresie przechowywania i wykorzystywania urządzeń mobilnych. Istotnym zagadnieniem, jakie zostało poruszone w ramach wystąpienia, było określenie zagrożeń oraz dokonanie oceny ryzyk płynących z korzystania z urządzeń mobilnych i przetwarzania na nich newralgicznych danych.

Jako ostatni głos zabrał **dr hab. inż. Teodor Buchner** (adiunkt na Wydziale Fizyki Politechniki Warszawskiej, ekspert narodowego operatora telekomunikacyjnego EXATEL S.A.), który przedstawił referat pt. **„Od czarnych i białych skrzynek do optyki kosmicznej i kwantowej: nowe wymiary bezpiecznej telekomunikacji"**. W trakcie swojego wystąpienia omówił on przykładowe kwestie związane z cyberbezpieczeństwem w sferze telekomunikacji w ujęciu fizycznym.

Na zakończenie pierwszego dnia konferencji odbyła się debata z uczestnikami wszystkich paneli, którzy mieli możliwość odniesienia się do zaprezentowanych inicjatyw mających na celu zwiększenie cyberbezpieczeństwa, a także przytoczonych metod zwalczania cyberprzestępczości.

Podsumowania pierwszego dnia konferencji dokonał **Jan Kostrzewa**, który podziękował wszystkim uczestnikom za udział w dyskusji i zaprosił do udziału w kolejnym dniu obrad.

W drugim dniu konferencji uroczystego powitania gości oraz prelegentów dokonał też **Jan Kostrzewa**.

Następnie głos zabrał **mgr Karol Wróbel** (dyrektor Departamentu Cyberbezpieczeństwa w EXATEL S.A., doświadczony architekt rozwiązań bezpieczeństwa, skupiony na tworzeniu i rozwoju kompleksowych usług cyberbezpieczeństwa), który wygłosił prelekcję pt. **„Rekonesans cyberbezpieczeństwa"**. Tematem przewodnim przemówienia była problematyka podejścia do bezpieczeństwa ofensywnego, jako efektywnego czasowo i kosztowo sposobu mającego na celu poprawę poziomu cyberbezpieczeństwa w podmiotach o różnym znaczeniu – zarówno tych działających jako podmioty prywatnego, jak i tych publicznych.

Kolejną prelegentką była **dr Aleksandra Komar-Nalepa** (adwokat w Izbie Adwokackiej w Warszawie, adiunkt w Zakładzie Międzynarodowego Postępowania Karnego WPiA UW). Poruszyła ona istotny temat z punktu widzenia procesu karnego, jakim jest charakter dowodów elektronicznych w postępowaniu karnym ze szczególnym uwzględnieniem ryzyka manipulacji. Dowody elektroniczne stały się integralną częścią procesu karnego, jednak organy procesowe muszą być uważne przy dopuszczaniu i przeprowadzaniu takich dowodów, co zostało wyraźnie podkreślone w przemówieniu.

Jako następny wystąpił **dr Rafał Kierzynka** (sędzia Sądu Okręgowego w Gorzowie Wielkopolskim, główny specjalista z zakresu europejskiego prawa karnego w MS i autor publikacji z tej dziedziny, przedstawiciel Polski w organach Unii Europejskiej i Rady Europy zajmujących się współpracą w sprawach karnych), który zaprezentował referat pt. **„Ewolucja kradzieży tożsamości jako efekt uboczny cyfryzacji usług"**. Przedstawił on skutki uboczne przyspieszonej cyfryzacji i informatyzacji, jakimi niewątpliwie może być kradzież tożsamości.

Kolejnym punktem konferencji „V4CybePower" był ekspercki panel dyskusyjny zatytułowany **„Spójność regulacji na poziomie unijnym, problematyka skutecznego zwalczania kradzieży tożsamości w aspekcie retencji danych, w kontekście rozstrzygnięć TSUE w sprawie w sprawach połączonych C-511/18, C-512/18, C-520/18 oraz współpraca z Facebookiem, Twitterem i innymi mediami społecznościowymi"**. Stanowił on rozwinięcie wystąpienia wygłoszonego przez dr. Rafała Kierzynkę. Uwagę skupiono na dostawcach usług w zakresie portali społecznościowych. Głos w dyskusji zabrali: **dr Gabor Jancso** (zastępca Sekretarza Stanu w Ministerstwie Sprawiedliwości Węgier), **dr inż. Tomasz Kisielewicz** (Kierownik Zespołu ds. Nowych Technologii MS) oraz **dr Rafał Kierzynka**. Prelegenci zwrócili szczególną uwagę na rolę dostawców usług portali społecznościowych w zakresie kradzieży danych. Takie media jak Facebook, Twitter, Linkedin posiadają ogromną bazę danych, w związku z tym konieczne jest podjęcie z nimi współpracy w zakresie przeciwdziałania kradzieży tożsamości, aby nie dochodziło do powtarzających się incydentów związanych z wyciekami danych.

Następnym prelegentem był **Piotr Sobczak** (dyrektor Biura Informacyjnego Krajowego Rejestru Sądowego), który wygłosił referat pt. **„Faktyczne implikacje wynikające z przetwarzania przez Krajowy Rejestr Karny danych o zagranicznym skazaniu obywatela polskiego w wyniku kradzieży tożsamości"**. Temat wystąpienia był ściśle powiązany z przestępstwem kradzieży tożsamości popełnionym za granicą przez polskiego obywatela.

Kolejny panel dyskusyjny nosił nazwę **„Gdzie uczą się cyberprzestępcy?"**. Głos w nim zabrali kolejno: **Jan Kostrzewa, dr inż. Tomasz Kisielewicz, dr Gabor Jancso** oraz **Paweł Wiszniewski** (ekspert Biura Bezpieczeństwa Narodowego). Celem panelu była próba odpowiedzi na zadane w tytule panelu pytanie o metody pozyskiwania wiedzy i rozwój cyberprzestępców. W ramach dyskusji istotnie zauważono, że cyberprzestępcy nie stoją w miejscu i wykorzystują nowe sposoby na popełnianie cyberprzestępstw. W związku z tym istotna jest analiza tego zjawiska oraz dalsze rozwijanie możliwości służb, które mają zapobiegać i wykrywać popełniane czyny zabronione.

Następnie **Paweł Wiszniewski** zaprezentował wystąpienie pt. **„Bądźmy odporni na cyberzagrożenia, cyberbezpieczeństwo – kluczowy element w koncepcji bezpieczeństwa państwa".** Wskazywał w nim na stale rosnące znaczenie cyberbezpieczeństwa w strategii bezpieczeństwa publicznego nowoczesnych państw.

Kolejny referat zaprezentował **mgr Dariusz Krzęcio (**doktorant na Wydziale Nauk o Bezpieczeństwie Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach), a nosił on tytuł **„Ryzyko cybernetyczne jako zjawisko naruszenia danych osobowych"**.

W dalszej części drugiego dnia konferencji głos zabrał również **dr inż. Tomasz Kisielewicz**, który omówił najważniejsze aspekty funkcjonowania Zespołu ds. Nowych Technologii działającego przy MS oraz wskazał na wagę zagadnień, które zostały podjęte w ramach Międzynarodowej Konferencji Naukowej pt. „V4CyberPower".

Ostatnie merytoryczne wystąpienie należało do **dr hab. Szymona Pawelca, prof. UW**, który odniósł się do zagadnienia dowodów elektronicznych. Wygłosił on prelekcję pt. **„Wybrane aspekty spraw karnych z udziałem dowodów elektronicznych"**. Podczas wystąpienia wskazano na doniosłość i zwiększającą się rolę

dowodów elektronicznych w sprawach karnych, ale jednocześnie ostrzeżono przed płynącymi z tego tytułu zagrożeniami.

Na koniec konferencji głos zabrał Podsekretarz Stanu MS **dr Marcin Romanowski**, który podziękował prelegentom za udział w konferencji oraz wskazał na potrzebę podejmowania debaty w zakresie cyberbezpieczeństwa. Podsekretarz Stanu wyraził nadzieję, że podejmowane w dyskusji problemy zostaną rozwinięte podczas kolejnej konferencji oraz w publikacji, która ma być rezultatem projektu badawczego pt. „Cyberbezpieczeństwo Grupy Wyszehradzkiej na rzecz zapobiegania przyczynom przestępczości".

Konferencja cieszyła się dużym zainteresowaniem, a przede wszystkim okazała się sukcesem z uwagi na to, że pozwoliła skonfrontować stanowiska wielu ekspertów z zakresu cyberbezpieczeństwa oraz cyberprzestępczości. Prelegentami byli zarówno teoretycy, praktycy, decydenci, funkcjonariusze publiczni oraz przedsiębiorcy, jak i naukowcy, co sprawiło, że konferencja przybrała przymiot wydarzenia interdyscyplinarnego poruszającego problematykę w sposób kompleksowy. Podjęte zagadnienia będą rozwijane w ramach dalszej realizacji projektu badawczego pt. **„Cyberbezpieczeństwo Grupy Wyszehradzkiej na rzecz zapobiegania przyczynom przestępczości"**, czego efektem będzie m.in. wspomniana wyżej monografia naukowa.