Andrzej Adamski

Cyberprzestępczość – rozwój regulacji prawnej w Europie. Doświadczenia krajowe na tle implementacji prawnych instrumentów zwalczania cyberprzestępczości (Londyn, 11–12 listopada 2010 r.)

Organizatorem konferencji była Akademia Prawa Europejskiego (*Academy of European Law*) w Trewirze, gospodarzem – Instytut Zaawansowanych Studiów Prawniczych Uniwersytetu Londyńskiego. Ok. 60 uczestników z 20 państw miało okazję wysłuchać 14 referatów składających się na półtoradniowy program konferencji, a także zabrać głos w dyskusji nad wieloma zagadnieniami związanymi ze zjawiskiem cyberprzestępczości, które poruszono w ramach czterech sesji.

W sesji pierwszej („Cyberprzestępczość – rozwój regulacji prawnej w Europie i poza nią") wystąpiło czterech mówców. Henrik Kaspersen[1] scharakteryzował aktualny stan implementacji konwencji Rady Europy o cyberprzestępczości[2] na świecie i ocenił przyjęte w niej rozwiązania prawne na tle postępu technicznego i ewolucji przestępczości związanej z technologią informacyjną. Uznał, że w obu tych aspektach Konwencja wytrzymała próbę czasu i stanowi jeden z najbardziej udanych i użytecznych instrumentów prawnych Rady Europy, o czym wymownie świadczy jej ratyfikacja przez 30 państw członkowskich Rady Europy i USA w ciągu ostatnich ośmiu lat.

Gillian Murray[3] w pierwszej części swojego wystąpienia skupiła się na analizie dokumentów ONZ związanych z problematyką cyberprzestępczości, w tym Konwencji NZ przeciwko międzynarodowej przestępczości zorganizowanej (UNTOC) oraz Rezolucji Zgromadzenia Ogólnego NZ z dnia 17 marca 2010 r. w sprawie globalnej kultury cyberbezpieczeństwa i ochrony

[1] Przewodniczący Komitetu ekspertów Rady Europy ds. przestępczości w cyberprzestrzeni w latach 1997–2001, emerytowany profesor prawa komputerowego Wolnego Uniwersytetu w Amsterdamie.

[2] Council of Europe Convention on Cybercirme, Budapest 21 listopada 2001 r. (ETS No.185); http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm.

[3] Centralny Punkt ds. Cyberprzestępczości, Wydział Przestępczości Zorganizowanej i Nielegalnego Handlu, Biuro ds. Narkotyków i Przestępczości NZ (UNODC) w Wiedniu.

krytycznych infrastruktur informacyjnych[4]. Nawiązując do art. 29(h) UNTOC, zwróciła uwagę na obowiązek szkolenia przez państwa–strony funkcjonariuszy organów ścigania, w tym prokuratorów i sędziów śledczych w dziedzinie metod zwalczania międzynarodowej przestępczości zorganizowanej i wykorzystywania do celów przestępczych komputerów, sieci telekomunikacyjnych i innych rodzajów nowoczesnych technologii. Przywołując Rezolucję Zgromadzenie Ogólnego NZ z dnia 17 marca 2010 r., przypomniała, że wzywa ona (art. 13) państwa członkowskie do systematycznego nowelizowania przepisów prawnych dotyczących cyberprzestępstw, prywatności, danych osobowych, prawa handlowego, podpisów cyfrowych i kryptografii oraz wykorzystywania w tym celu regionalnych i międzynarodowych instrumentów i standardów prawnych.

Druga część wystąpienia przedstawicielki ONZ dotyczyła problematyki cyberprzestępczości na XII Kongresie NZ na temat Zapobiegania Przestępczości i Wymiaru Sprawiedliwości Karnej (Salvador, Brazylia, 12–19 kwietnia 2010 r.). Przedmiotem szczegółowych uwag był dokument końcowy Kongresu – tzw. „Deklaracja Salwadorska", która wzywa członków społeczności międzynarodowej do podejmowania wysiłków na rzecz zapobiegania, wykrywania i ścigania wszelkich form cyberprzestępczości oraz apeluje do Komisji Zapobiegania Przestępczości i Wymiaru Sprawiedliwości o powołanie pod auspicjami ONZ międzyrządowej grupy ekspertów w celu podjęcia studiów nad tym problemem[5].

Ian Walden[6] dokonał przeglądu zagadnień związanych z jurysdykcją w sprawach cyberprzestepstępstw o charakterze transgranicznymi i poruszył kwestię międzynarodowej pomocy prawnej w tej dziedzinie. Na tle ogólnych zasad jurysdykcji terytorialnej i pozaterytorialnej przedstawił aktualne rozwiązania prawne w prawie karnym międzynarodowym (konwencja Rady Europy o cyberprzestępczości), instrumentach Unii Europejskiej (decyzje ramowe) oraz w prawie porównawczym wybranych państw (USA, Anglia i Walia). W tym ostatnim aspekcie, na tle wyroków w sprawach Waddon (2000) i Sheppard (2010), wskazał na rysującą się w orzecznictwie Sądu Apelacyjnego JKM tendencję do „terytorializacji" *locus delicti* w sprawach przestępstw transgranicznych polegających na rozpowszechnianiu niedozwolonych treści przy pomocy serwerów zlokalizowanych za granicą.

---

[4] Resolution adopted by the General Assembly [on the report of the Second Committee (A/64/422/Add.3)] 64/211. Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures.

[5] Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World http://www.unodc.org/ documents/ crime–congress/12th–Crime–Congress/Documents/ A_CONF.213_18/V1053828e.pdf.

[6] Profesor prawa, Instytut Prawa Komputerowego i Komunikacji Elektronicznej w Centrum Badań Prawa Handlowego na Uniwersytecie Londyńskim Queen Mary.

Achim Schmitz[7] przedstawił problem współpracy międzynarodowej organów policji w dziedzinie ścigania cyberprzestępstw popełnianych przez członków sieci kryminalnych operujących w Internecie na skalę globalną. Zwrócił uwagę na kontrowersje związane z kwalifikacją prawną udziału osób zaangażowanych w *phishing*[8] i *pharming*[9] jako formy uczestnictwa w zorganizowanej grupie przestępczej. Na przykładzie prowadzonych przez policję niemiecką dochodzeń omówił *modus operandi* sprawców zamachów na bankowość internetową oraz scharakteryzował mechanizm współdziałania policji niemieckiej z policją brytyjską, ukraińską i estońską w ramach jednego z takich postępowań prowadzonych przy pomocy Europolu. Mówca krytycznie ocenił decyzję ramową o wspólnych zespołach śledczych, która jego zdaniem nadmiernie formalizuje współpracę międzynarodową i nie rozwiązuje problemu jej kosztów. Instruktywnie brzmiały natomiast uwagi referenta na temat organizacji postępowań karnych w sprawach „przestępczych operacji internetowych" na szczeblu krajowym, w szczególności, gdy chodzi o zasadę jednoosobowego kierownictwa zespołem śledczym i ścisłą współpracę stojącego na jego czele prokuratora z sędzią śledczym. Pierwszy niemiecki zespół śledczy ds. cyberprzestępstw pod kierunkiem prokuratora krajowego ze Stuttgartu zdołał w ciągu jedenastu miesięcy doprowadzić do likwidacji ośmioosobowej grupy *phisherów*, korzystających z usług 470 pośredników (tzw. „agentów finansowych"), ponad 100 botnetów i 2,5 mln komputerów *zombi* na świecie, a w konsekwencji uchronić klientów e-banków od utraty kilku milionów euro.

Przedmiotem drugiej sesji konferencji („Doświadczenia krajowe związane z implementacją instrumentów prawnych zwalczania cyberprzestępczości") były dwa zagadnienia: praktyka prokuratorska i sądowa w zakresie ścigania i sądzenia cyberprzestępstw oraz doświadczenia państw członkowskich Unii Europejskiej związane z filtrowaniem i blokowaniem dostępu do nielegalnych treści w Internecie. Referaty wygłoszone w pierwszej części sesji miały charakter studiów przypadków a ich autorami byli przedstawiciele głównych zawodów prawniczych: prokurator, sędzia i adwokat.

Pedro Verdelho[10] w wystąpieniu zatytułowanym „Nielegalne działania w sieci – doświadczenia portugalskie" przedstawił efekty transpozycji przepisów konwencji Rady Europy o cyberprzestępczości do ustawodawstwa karnego Portugalii. Omawiając uchwaloną w tym celu ustawę nr 109 z dnia 15 września 2009 r., podkreślił jej kompleksowy (materialno-procesowy) charakter. Wskazał, że zawiera ona wszystkie przewidziane konwencją instrumenty karnoprocesowe, co powinno ułatwić policji portugalskiej ściganie

[7] Przedstawiciel Krajowego Urzędu Kryminalnego Północnej Nadrenii–Westfalii.
[8] Zob. http://pl.wikipedia.org/wiki/Phishing.
[9] Zob. http://pl.wikipedia.org/wiki/Pharming.
[10] Prokurator, wykładowca Portugalskiej Szkoły Sądownictwa w Lizbonie.

sprawców przestępstw, nie tylko komputerowych, lecz również tradycyjnych. Dla zilustrowania tej tezy posłużył się przykładem zbiegłego za granicę sprawcy zabójstwa, który dzięki współpracy międzynarodowej opartej na konwencyjnych instrumentach prawnych został zlokalizowany i ujęty tylko dlatego, że używał poczty elektronicznej.

Christiaan Baardman[11] rozpoczął wystąpienie od przedstawienia informacji o działającym od 2009 r. przy sądzie apelacyjnym w Hadze ośrodku badawczym nad cyberprzestępczością, którego głównym zadaniem jest upowszechnianie wśród sędziów holenderskich wiedzy o technicznych i prawnych problemach Internetu i związanej z nim przestępczości. Rozwinięciem tego ostatniego wątku były studia przypadków wybranych kategorii cyberprzestępstw (skimming, wirtualna pornografia dziecięca, grooming, zniesławienie, kradzież wirtualnych przedmiotów i atak DDoS), które zostały zaprezentowane przez autora referatu w aspekcie prawnym na tle orzeczeń sądowych. Największe zainteresowanie słuchaczy wywołały orzeczenia dotyczące „kradzieży" wirtualnych rekwizytów uczestników gier internetowych typu MMORPG[12]. Przedmiotem ożywionej dyskusji, toczącej się również w kuluarach konferencji, był wyrok sądu apelacyjnego w Leeuwarden, który w 2009 r. uznał, że dokonanie *on-line* zaboru w celu przywłaszczenia wirtualnej maski i amuletu należących do uczestnika gry „RuneScape" wyczerpuje znamiona przestępstwa kradzieży, mimo że wg art. 310 holenderskiego kodeksu karnego przedmiotem wykonawczym tego czynu może być rzecz.

Stephen Mason[13] przedstawił specyficzny dla prawodawstwa Anglii i Walii problem dostępu obrońcy oskarżonego do materiału dowodowego w sprawach związanych z pornografią dziecięcą. Zagadnienie to jest szczegółowo unormowane w kilku aktach prawnych oraz wytycznych ACPO[14] dla funkcjonariuszy policji. Jednakże w praktyce – wobec restrykcyjnych zakazów prawnomaterialnych – stosowanie przepisów proceduralnych wywołuje komplikacje. Autor referatu omówił je na przykładzie jednego z postępowań karnych, w którym prokurator wbrew zarządzeniu sędziego o wykonaniu kopii zdjęć dla sądu i oskarżonego domagał się, by oskarżony i jego obrońca zapoznali się z oryginalnym materiałem dowodowym w sądowym pokoju przesłuchań w asyście funkcjonariusza policji. Sąd Apelacyjny w wyroku z dnia 28 kwietnia 2010 r. (sprawa Regina v R (L)) rozstrzygnął ten spór na rzecz sądu I instancji i, powołując się na zasadę uczciwego procesu, orzekł, że oskarżony i jego obrońca mają prawo do zapoznania się z materiałem

[11] Sędzia sądu apelacyjnego, Centrum badań i ekspertyz cyberprzestępczości w Hadze.
[12] Zob. http://pl.wikipedia.org/wiki/MMORPG.
[13] Adwokat i współpracownik Instytutu Zaawansowanych Studiów Prawniczych Uniwersytetu Londyńskiego.
[14] The ACPO Good Practice Guide for Computer–Based Electronic Evidence – http://www.acpo. police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf.

dowodowym w warunkach zapewniających im swobodną i poufną wymianę zdań podczas tej czynności, bez jakiejkolwiek obserwacji i kontroli ze strony osób trzecich.

Drugą część sesji wypełniła problematyka blokowania dostępu do stron internetowych zawierających pornografię dziecięcą. Jest to projekt popierany przez Komisję Europejską[15], lecz wywołujący zastrzeżenia Europejskiego Inspektora Ochrony Danych i dezaprobatę organizacji pozarządowych. Krytycznie o blokowaniu dostępu do stron internetowych wypowiedział się pierwszy z mówców – Richard Clayton[16], który w kwestii podstawowej („czy blokowanie jest skuteczne?") udzielił następujących odpowiedzi: „tak, ponieważ utrudnia dostęp przypadkowy, choć to nie on jest istotą problemu", „nie, gdyż blokadę łatwo można obejść", „tak, bo daje politykom poczucie, że rozwiązali problem", „nie, gdyż nielegalne strony działają nadal i udostępniają pornografię". Drugi z mówców – Peter Robbins[17], jako przedstawiciel organizacji, która na użytek dostawców usług internetowych kompiluje „czarne listy" stron internetowych z pornografią dziecięcą, prezentował w kwestii ich blokowania bardziej umiarkowane stanowisko. Nie wykluczał, że w pewnych okolicznościach blokowanie może być uzasadnione, generalnie jednak opowiadał się za stosowaniem procedury „powiadamiania i usuwania" *(*ang. *notice and take down*) i eliminowaniem tą drogą z Internetu zdjęć przedstawiających seksualne wykorzystywanie dzieci. W zakończeniu podkreślił, że blokowanie dostępu do pornografii dziecięcej nie ograniczy skali zjawiska seksualnego wykorzystywania małoletnich ani nie zniechęci dewiantów seksualnych do poszukiwania tego rodzaju materiałów w sieci.

W ramach trzeciej sesji („Współpraca sektora publicznego i prywatnego w zwalczaniu cyberprzestępczości") wygłoszono trzy referaty.

Nicola Dileone[18] scharakteryzował fenomen cyberprzestępczości opartej na modelu biznesowym (*cybercrime business model*) oraz problemy, na jakie napotyka zwalczanie przestępstw internetowych o charakterze transgranicznym przez policję. Wskazywał, że skuteczne rozwiązywanie tych problemów leży zarówno w interesie sektora gospodarczego, który jest celem ataków cyberprzestępców, jak i organów powołanych do ich ścigania. Na tym tle przedstawił szereg postulatów dotyczących współdziałania sektora prywatnego z policją. Jej przedmiotem powinno być m.in. ustalenie *modus*

[15] Komisja Europejska, Wniosek – Dyrektywa Parlamentu Europejskiego i Rady w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, uchylająca decyzję ramową 2004/68/WSiSW, Bruksela, dnia 29 marca 2010 r., KOM(2010)94, wersja ostateczna.

[16] Pracownik naukowy Uniwersytetu Cambridge, specjalista w dziedzinie bezpieczeństwa informatycznego.

[17] Dyrektor generalny Internet Watch Foundation.

[18] Pierwszy oficer Centrum przestępczości zawansowanych technologii w Europolu.

vivendi w zakresie godzenia interesu gospodarczego pokrzywdzonego (przywrócenie funkcjonowania systemu po ataku) z interesem wymiaru sprawiedliwości (zabezpieczenie dowodów przestępstwa), jak i ściślejsza współpraca instytucji finansowych z organami ścigania w celu uniemożliwienia transferu i legalizacji korzyści majątkowych pochodzących z nielegalnych źródeł.

W dalszej części wystąpienia omówione zostały aktualnie realizowane przez Europol projekty związane z przeciwdziałaniem cyberprzestępczości, w szczególności Europejska Platforma Cyberprzestępczości (*European Cyber Crime Platform*) – główne repozytorium danych oraz miejsce wymiany informacji na temat przestępstw internetowych ujawnianych w krajach UE.

Wolfgang Schreiber[19] rozpoczął swoje wystąpienie pt. „Rola Interpolu w zwalczaniu cyberprzestępczości oraz sieć 24/7 G8" od przedstawienia historii powstania i zakresu prac podgrupy roboczej państw Grupy Ośmiu (G8) zajmującej się problematyką cyberprzestępczości (*Subgroup on High-Tech Crime*). Omówił też cele i zasady funkcjonowania sieci punktów kontaktowych 24/7 Grupy Ośmiu, do której należy obecnie 58 państw. Druga część referatu dotyczyła Interpolu i realizowanych w ramach tej organizacji inicjatyw i projektów o charakterze badawczo-edukacyjnym, których rezultaty włączane są sukcesywnie do wydawanego w formie elektronicznej podręcznika dla policjantów zajmujących się ściganiem cyberprzestępstw[20]. Na marginesie tego wystąpienia można odnotować, że Polska stanowi „białą plamę" na mapie sieci 24/7 G8, nie jest też wymieniana wśród członków grupy roboczej Interpolu ds. przestępczości teleinformatycznej.

W imieniu sektora prywatnego wstąpił Stephen Deadman[21], który jako przedstawiciel globalnego operatora telekomunikacyjnego (385 mln klientów na świecie) zaprezentował podejście marketingowe do tematu i położył większy akcent na polityce ochrony prywatności i bezpieczeństwa klientów Vodafone niż na partnerstwie publiczno-prywatnym w znaczeniu współpracy z organami ścigania. Obszernie wypowiadał się o filtrowaniu dostępu do stron internetowych przy pomocy list Internet Watch Foundation oraz obsłudze zgłoszeń użytkowników sieci o popełnianych w niej nadużyciach. Wskazywał, że w przypadku hostingu stosowanie procedury „powiadamiania I usuwania" szkodliwych lub nielegalnych treści przebiega sprawnie i trwa bardzo krótko (decyzja o ewentualnym usunięciu kwestionowanego materiału zapada w ciągu 48 godzin od chwili zgłoszenia incydentu).

---

[19] Przewodniczący Grupy Roboczej Interpolu ds. przestępczości komputerowej w Europie, funkcjonariusz Bundeskriminalamt, Wiesbaden.

[20] Zob. https://www.interpol.int/Public/Icpo/Publications/default.asp.

[21] Kierownik zespołu Grupy Vodafone ds. spraw prawnych, ochrony prywatności i bezpieczeństwa.

Ostatnią sesję konferencji („Perspektywy na przyszłość i uwagi końcowe związane z pracami prowadzonymi w ramach Unii Europejskiej") wypełnił referat przedstawiciela Dyrekcji Generalnej Spraw Wewnętrznych Komisji Europejskiej.

Radomir Jansky[22] w wystąpieniu zatytułowanym „Unijne instrumenty przeciwdziałania cyberprzestępczości" scharakteryzował zadania UE I państw członkowskich w tej dziedzinie wynikające z przyjętych przez Komisję Europejską dokumentów programowych (Strategii sztokholmskiej oraz Europejskiej agendy cyfrowej), komunikatów (Strategia bezpieczeństwa wewnętrznego UE) oraz inicjatyw legislacyjnych w postaci wniosków dwóch dyrektyw Parlamentu Europejskiego i Rady (w sprawie ataków na systemy informacyjne[23] oraz w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej[24]). Zdaniem mówcy, bezpieczeństwo użytkowników Internetu I skuteczne zwalczanie cyberprzestępczości należą obecnie do priorytetów polityki bezpieczeństwa Unii Europejskiej. Wskazuje na to wyraźnie treść powołanych wyżej dokumentów oraz sformułowane w nich cele i zamierzenia, w tym w szczególności plany utworzenia do 2013 r. europejskiego centrum przeciwdziałania cyberprzestępczości, które ma umożliwić państwom członkowskim i instytucjom UE budowanie zdolności operacyjnych i analitycznych do prowadzenia dochodzeń oraz pogłębienia współpracy z partnerami międzynarodowymi.

Mimo napiętego, lecz interesującego programu i trafnego doboru merytorycznie kompetentnych mówców, konferencję uznać można za sukces jej organizatorów oraz źródło satysfakcji intelektualnej uczestników.

[22] Pracownik zespołu ds. Zwalczania Przestępczości Zorganizowanej, Dyrekcja Ogólna Spraw Wewnętrznych Komisji Europejskiej

[23] Komisja Europejska, Wniosek – Dyrektywa Parlamentu Europejskiego i Rady dotycząca ataków na systemy informatyczne i uchylająca decyzję ramową Rady 2005/222/WSiSW, Bruksela, dnia 30 września 2010 r., KOM(2010) 517, wersja ostateczna.

[24] Zob. przyp. 15.