Cyberbezpieczeństwo na rzecz zapobiegania przyczynom przestępczości

CYBER SECURITY TO PREVENT CRIME CAUSES

Redakcja Marcin Wielec

Cyberbezpieczeństwo na rzecz zapobiegania przyczynom przestępczości

CYBER SECURITY TO PREVENT CRIME CAUSES

Cyberbezpieczeństwo na rzecz zapobiegania przyczynom przestępczości

CYBER SECURITY TO PREVENT CRIME CAUSES

Redakcja Marcin Wielec

WYDAWNICTWO INSTYTUTU WYMIARU SPRAWIEDLIWOŚCI | **Warszawa 2023**

MINISTERSTWO SPRAWIEDLIWOŚCI

FUNDUSZ SPRAWIEDLIWOŚCI

Współfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

RECENZENCI *prof. zw. dr hab. Ewa M. Guzik-Makaruk*
dr Klara Dygaszewicz

KOREKTA *studioformat.pl*
SKŁAD, ŁAMANIE *Wiaczesław Krysztal*
PROJEKT OKŁADKI *Tomasz Smołka*
W projekcie wykorzystano zdjęcie autorstwa Matthew Henry'ego

ISBN 978-83-67149-30-3

WYDAWNICTWO INSTYTUTU WYMIARU SPRAWIEDLIWOŚCI
ul. Krakowskie Przedmieście 25, 00-071 Warszawa
SEKRETARIAT tel.: (22) 630-94-53, e-mail: wydawnictwo@iws.gov.pl

DRUK, OPRAWA *„Elpil", ul. Artyleryjska 11, 08-110 Siedlce*

Spis treści

Przedmowa

Rozwój technologii i Internetu znacząco poprawił jakość naszego życia, ponieważ usprawnił komunikację, skrócił dystans między ludźmi i umożliwił powstawanie zupełnie nowych form biznesu. Proces ten spowodował jednocześnie pojawienie się ogromnych zagrożeń. Szybkość wymiany informacji, pozorna anonimowość i beztroska użytkowników to czynniki, które sprawiają, że cyberprzestępczość jest jedną z najszybciej rozwijających się działalności przestępczych. Cyberprzestępczość, obok ataków terrorystycznych i zmian klimatycznych, jest jednym z największych wyzwań XXI w. Rosnąca liczba przestępstw związanych z bankowością internetową na świecie sprawiła, że Światowe Forum Ekonomiczne w swoim badaniu „Global Risks Report" uznało cyberprzestępczość za największe ryzyko biznesowe w 2020 r. Analiza powyższych zagadnień prowadzi do wniosku, że cyberprzestrzeń stała się narzędziem, które może bezpośrednio i pośrednio powodować naruszenia podstawowych wolności i praw człowieka. Obecnie Internet jest nieodłączną częścią naszego życia, ale jak pokazują statystyki, może być również strefą zagrożenia dla wolności i praw człowieka. Przejawia się to na różne sposoby – m.in. przez kierowanie i udostępnianie treści odbiorcom, do których nie powinny one trafić.

Publikacja, którą oddajemy do rąk Czytelnika, jest wynikiem analiz przeprowadzonych w ramach projektu „Cyberbezpieczeństwo Grupy Wyszehradzkiej na rzecz zapobiegania przyczynom przestępczości" realizowanego w ramach środków Funduszu Pomocy Pokrzywdzonym oraz Pomocy Postpenitencjarnej – Funduszu Sprawiedliwości. Projekt prowadzony był pod kierunkiem Centrum Analiz Strategicznych, będącego jednostką Instytutu Wymiaru Sprawiedliwości w Warszawie.

Monografia zawiera opracowania dotyczące szeroko rozumianego problemu cyberbezpieczeństwa i zapobiegania przestępstwom w cyberprzestrzeni poprzez analizę i diagnozę najpopularniejszych zjawisk z zakresu cyberbezpieczeństwa. Z powyższych względów w publikacji znalazły się m.in.: analiza ochrony dzieci przed szkodliwym wpływem treści publikowanych w Internecie, analiza roli i zadań wybranych służb specjalnych w zakresie zwalczania i przeciwdziałania cyberprzestępczości, wybrane zagadnienia związane ze zjawiskiem cyberprzestępczości popełnianej z wykorzystaniem mediów społecznościowych i platform cyfrowych czy też ekspertyza dotycząca definicji samej cyberprzestrzeni i cyberprzestępczości, a także komentarze koncepcyjne do tych definicji wraz z elementami badań prawnoporównawczych. Zwrócono również uwagę na regulacje polskiego prawa rodzinnego, kształtujące omawiane zagadnienie poprzez konstrukcję instytucji władzy rodzicielskiej, a także przeanalizowano polskie regulacje związane z zagrożeniami i perspektywami telemedycyny. W monografii poruszono także problem cyberprzestępczości w sferze prawa bankowego. Tematyka publikacji jest więc bardzo szeroka i ukazuje powiązania zagadnienia cyberbezpieczeństwa z wieloma dziedzinami prawa, odnosząc się przy tym do regulacji obowiązujących w tym zakresie w różnych państwach.

Mamy nadzieję, że publikacja ta będzie dla Czytelnika ważną poznawczo lekturą, zachęcającą do samodzielnej analizy przedstawionych przez Autorów zjawisk. Jednocześnie wierzymy, że wnioski zawarte w publikacji będą stanowiły istotny element oceny stanu regulacji obowiązujących w analizowanym zakresie i rzucą nowe światło na pewne rozwiązania występujące w różnych dziedzinach życia, wskazując na ciągłą potrzebę doskonalenia rozwiązań sprzyjających cyberbezpieczeństwu.

Marcin Wielec, Bartłomiej Oręziak

Cyberprzestrzeń i cyberprzestępczość: uwagi dotyczące definicji z elementami analizy prawnoporównawczej

1. Cyberprzestrzeń

1.1. Wprowadzenie

Za mający istotne znaczenie należy uznać fakt, że definicji pojęcia „cyberprzestrzeni" w literaturze przedmiotu jest wiele. Ukazanie, jak rozumiane jest to pojęcie, ma doniosłe oraz kreatywne znaczenie dla dalej idących wniosków. Potwierdza to dość szeroki dorobek doktryny w zakresie korelacji nowoczesnych technologii z prawem i postępowaniem karnym[1]. Wypada zauważyć,

[1] Zob.: L. Lessig, P. Resnick, *Zoning Speech on the Internet: A Legal and Technical Model*, „Michigan Law Review" 1999, nr 98(2), s. 395–431; L. Speer, *Redefining Borders: The Challenges of Cybercrime*, „Crime, Law and Social Change" 2000, nr 34, s. 259–273; M. Gercke, *Europe's Legal Approaches to Cybercrime*, „ERA Forum" 2009, nr 10, s. 409–420; M. Nuth, *Taking Advantage of New Technologies: For and Against Crime Computer Law and Security Report*, „Computer Law & Security Review" 2008, nr 24, s. 437–446; N. Katyal, *Criminal Law in Cyberspace*, „University of Pennsylvania Law Review" 2001, nr 149(4), s. 1003–1114; N. Marion, *Symbolic Policies in Clinton's Crime Control Agenda*, „Buffalo Criminal Law Review" 1997, nr 1, s. 67–108; O. Silver, *European Cybercrime Proposal Released*, „Computer Fraud and Security" 2001, nr 5, s. 5; P. Berman, *The Globalization of Jurisdiction*, „University of Pennsylvania Law Review" 2002, nr 151(2), s. 311–545; P. Swire, *Elephants and Mice Revisited: Law and Choice of Law on the Internet*, „University of Pennsylvania Law Review" 2005, nr 153(6), s. 1975–2001; S. Brenner, J. Schwerha, *Introduction-Cybercrime: A Note on International Issues*, „Information Systems Frontiers" 2004, nr 6(2), s. 111–114; S. Hilley, *Pressure Mounts on US Senate to Pass Cybercrime Treaty*, „Digital Investigation" 2005, nr 2, s. 171–174; S. Moitra, *Developing Policies for Cybercrime*, „European Journal of Crime, Criminal Law and Criminal Justice" 2005, nr 13(3), s. 435–464; A. Kigerl, *CAN SPAM Act: An Empirical analysis*, „International Journal of Cyber Criminology" 2009, nr 3(2), s. 566–589; A. Shapiro, *The Internet*, „Foreign Policy" 1999, nr 115, s. 14–27; A. Stolz, *Congress and Capital Punishment: An Exercise in Symbolic Politics*, „ Law and Policy Quarterly" 1983, nr 5(2), s. 157–180; B. Hancock, *US and Europe Cybercrime Agreement Problems*, „Computers and Security" 2000, nr 19(4), s. 306–307; B. Wible, *A Site Where Hackers are Welcome: Using Hack-In Contests to Shape Preferences and Deter Computer Crime*, „The Yale Law Journal" 2003, nr 112(6), s. 1577–1623; C. Coleman, *Security Cyberspace – New Laws and Developing Strategies*, „Computer Law and Security Report"

że w literaturze przedstawia się różne definicje. Wypracowanie właściwego znaczenia pojęcia „cyberprzestrzeni" jest aktualnym zagadnieniem od wielu już lat, podczas gdy okres ten głównie był przeznaczony na prace związane z wypracowaniem jasnych, precyzyjnych i bezwarunkowych definicji „cyberprzestrzeni" zarówno w nauce, jak i w działalności współczesnych państw. Wydaje się, że jest to warunek konieczny prawidłowej legislacji dotyczącej tej, ciągle rozwijającej się, materii normatywnej. W tym momencie warto podkreślić, że kluczową cechą cyberprzestrzeni jest zmienność i jednoczesna innowacyjność. Bogata – jak się wydaje – historia pojęcia „cyberprzestrzeni" nie neguje tego twierdzenia pod warunkiem, że przyjmiemy założenie o stałej i postępującej ewolucji cyberprzestrzeni. Warunek ten nie wydaje się trudny do przyjęcia.

2003, nr 19(2), s. 131–136; E. Simon, *Cyberporn and Censorship: Constitutional Barriers to Preventing Access to Internet Pornography by Minors*, „The Journal of Criminal Law and Criminology" 1998, nr 88(3), s. 1015–1048; I. Walden, *Harmonising Computer Crime Laws in Europe*, „European Journal of Crime, Criminal Law and Criminal Justice" 2004, nr 12(4), s. 321–336; J. Reidenberg, *Technology and Internet Jurisdiction*, „University of Pennsylvania Law Review" 2005, nr 153(6), s. 1951–1974; J. Sinrod, W. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, „Santa Clara Computer and High Technology Law Journal" 2000, nr 16(2), s. 1–53; S. Wang, *Measures of Retaining Digital Evidence to Prosecute Computer-based Cyber-crimes*, „Computer Standards and Interfaces" 2007, nr 29, s. 216–223; U. Kohl, *Eggs, Jurisdiction and the Internet*, „The International and Comparative Law Quarterly" 2002, nr 51(3), s. 555–582; W. Chung, H. Chen, W. Chang, S. Chou, *Fighting cybercrime: a review and the Taiwan Experience*, „Decision Support Systems" 2006, nr 41, s. 669–682; M. Cieślak, *Proces karny* (*skrypt*), Kraków 1952, s. 9; *idem*, *Środki przymusu na tle bodźców prawnych w procesie karnym*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace Prawnicze" 1960, z. 7, s. 101–102; B. Boni, *Creating a Global Consensus Against Cybercrime*, „Network Security" 2001, nr 9, s. 18–19; J. Clough, *A world of difference: The Budapest Convention on Cybercrime and the challenges of harmonization*, „Monash University Law Review" 2014, nr 40(3), s. 698–736; M. Gercke, *The Convention on Cybercrime*, „Multimedia und Recht" 2004, nr 20, s. 802; R. Winick, *Searches and seizures of computers and computer data*, „Harvard Journal of Law & Technology" 1994, nr 8(1), s. 75–128; D. Resseguie, *Computer Searches and Seizure*, „Cleveland State Law Review" 2000, nr 48(185), s. 185–214; J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9, s. 225–234; T. Aleksandrowicz, *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, nr 15, s. 11–12; M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – Zarys problemu*, „Bezpieczeństwo Narodowe" 2012, nr 22 s. 125–139; A. Nowak, *Cyberprzestrzeń jako nowa jakość zagrożeń*, „Zeszyty Naukowe Akademii Obrony Narodowej" 2013, z. 3(92) s. 5–46; J. Kulesza, *Międzynarodowe prawo Internetu*, Poznań 2010, s. 57; J. Bednarek, A. Andrzejewska, *Cyberświat – możliwości i zagrożenia*, Warszawa 2009, s. 29–32; H. Babis, *Internet*, [w:] *Encyklopedia zagadnień międzynarodowych*, red. E. Cała-Wacinkiewicz, R. Podgórzański, Warszawa 2011, s. 540–541.

1.2. Propozycje definicji cyberprzestrzeni

Po analizie literatury związanej z tytułowym zagadnieniem można dojść do wniosku, iż często sugeruje się, że cyberprzestrzeń to płaszczyzna złożonych i wielowarstwowych powiązań cyfrowych o charakterze niematerialnym oraz funkcjonująca za pomocą odpowiednio dostosowanej i przygotowanej infrastruktury[2]. Zauważa się też, że:

> mianem cyberprzestrzeni (*cyberspace*) określa się sieć łączącą systemy komputerowe obejmujące jednostki centralne i ich oprogramowanie, ale także dane, sposoby i środki ich przesyłania. Cyberprzestrzeń obejmuje systemy powiązań internetowych, usługi teleinformatyczne oraz systemy zapewniające prawidłowe funkcjonowanie kraju, tj. systemy transportu, łączności, systemy infrastruktury energetycznej, wodociągowej i gazowej czy ochrony zdrowia[3].

W innym miejscu można przeczytać, że cyberprzestrzeń to „przestrzeń otwartego komunikowania się za pośrednictwem połączonych komputerów i pamięci informatycznych pracujących na całym świecie"[4]. Ciekawą definicją jest ta zaproponowana przez estońskie Centrum Doskonalenia Cyberobrony Organizacji Traktatu Północnoatlantyckiego w Tallinie, zgodnie z którą:

> cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems. They describe the background of the definition and show why this approach may be preferable over others[5].

---

[2] M. Madej, *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*, [w:] *Bezpieczeństwo teleinformatyczne państwa*, red. M. Madej, M. Terlikowski, Warszawa 2009, s. 28; T. Aleksandrowicz, *op. cit.*, s. 11.

[3] P. Tekielska, Ł. Czekaj, *Działania służb w Unii Europejskiej realizujących zadania na rzecz bezpieczeństwa cybernetycznego*, [w:] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, red. M. Górka, Warszawa 2014, s. 163; T. Aleksandrowicz, *op. cit.*, s. 11.

[4] P. Levy, *Drugi potop*, [w:] *Nowe media w komunikacji społecznej w XX wieku. Antologia*, red. M. Hopfinger, Warszawa 2002, s. 380.

[5] *Cyberspace: Definition and Implications*, https://ccdcoe.org/library/publications/cyberspace-definition-and-implications/ (dostęp: 29.08.2022 r.).

Dodatkowo pojęcie „cyberprzestrzeni" jest ujmowane także z psychologicznego i socjologicznego punktu widzenia[6] i w tym wymiarze określane jest jako „każda przestrzeń, w której ludzie mogą gromadzić swoje umysły bez zabierania tam swoich ciał"[7]. Zauważa się również, że cyberprzestrzeń to nowa Wieża Babel, miejsce, w którym można dzielić się kulturami świata, pomysłami i informacjami oraz je rozpowszechniać w czasie rzeczywistym, natomiast wykluczenie z tego świata cyfrowego skazuje ludzi na izolację, firmy na upadek, a narody na uzależnienie[8].

1.3. Analiza prawnoporównawcza

W Stanach Zjednoczonych Ameryki uznanym określeniem cyberprzestrzeni jest definicja, zgodnie z którą cyberprzestrzeń to:

> A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers[9].

Zastanawiające tutaj jest jednak pominięcie w cytowanym rozwiązaniu elementów osobowych i skupienie się wyłącznie na technicznych aspektach funkcjonowania cyberprzestrzeni. Wydaje się, że nie jest to rozwiązanie trafne[10],

---

[6] R. Tadeusiewicz, *Wychowywanie dla cyberprzestrzeni jednym z warunków zapobiegania cyberuzależnieniom*, [w:] *Cyberuzależnienia: przeciwdziałanie uzależnieniom od komputera i Internetu*, red. E. Mastalerz, K. Pytel, H. Noga, Kraków 2007, s. 23.

[7] K. Dobrzeniecki, *Prawo a etos cyberprzestrzeni*, Toruń 2004, s. 18.

[8] Stanowisko takie zostało przedstawione przez francuskiego Generalnego Sekretarza Agencji i Bezpieczeństwa Sieci oraz Informacji w dokumencie „Obrona oraz bezpieczeństwo systemów informacyjnych. Strategia dla Francji" z 2011 r., https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf (dostęp: 29.08.2022 r.).

[9] *National Institute of Standards and Technology*, https://csrc.nist.gov/glossary/term/cyberspace (dostęp: 29.08.2022 r.).

[10] W aspekcie pominięcia w stworzonej przez Departament Obrony USA definicji „cyberprzestrzeni" aspektu programowego zobacz: R. Ottis, P. Lorents, *Cyberspace: Definition*

gdyż nawet intuicyjnie można stwierdzić, że prawidłowe działanie cyberprzestrzeni bez ludzkiego udziału nie jest możliwe. Człowiek jako istota wyposażona w cnotę rozumu[11] zawsze powinna stanowić jądro wszystkich nowych rozwiązań, stanowić jej rozwinięcie i sens, stanowić jej warunek *sine qua non*. Rozwiązania przyjmowane w USA wydają się nie zauważać powyższego warunku, co starała się zmienić definicja, zgodnie z którą

> Cyberspace is their nervous system–the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security[12].

Fakt, że w ramach procesów definicyjnych występujących w administracji USA zauważono potrzebę zwrócenia, choćby pośrednio, uwagi na człowieka, który jest kluczowym desygnatem definicyjnym pojęcia „cyberprzestrzeni", należy ocenić pozytywnie.

W Republice Francuskiej powszechnie funkcjonującą definicję „cyberprzestrzeni" stworzył organ administracji publicznej odpowiedzialny za cyberbezpieczeństwo. W dokumencie Agencji i Bezpieczeństwa Sieci oraz Informacji „Obrona oraz bezpieczeństwo systemów informacyjnych. Strategia dla Francji" z 2011 r. zawarto twierdzenie, zgodnie z którym cyberprzestrzeń oznacza: „The communication space created by the worldwide interconnection of automated digital data processing equipment"[13]. Należy zauważyć, że powyżej przedstawiona francuska definicja skupia się przede wszystkim na aspekcie

---

and Implications. In Proceedings of the 5th International Conference on Information Warfare and Security, Dayton 2010, s. 2.

[11] H. Buczyńska-Garewicz, *O pojęciu cnoty: czy cnota jest przeżytkiem?*, „Teksty: teoria literatury, krytyka, interpretacje" 1981, nr 1(55), s. 9–30.

[12] *NATIONAL STRATEGY TO SECURE CYBERSPACE*, https://www.cisa.gov/national-strategy-secure-cyberspace (dostęp: 29.08.2022 r.).

[13] *Information system defence and security. France's strategy*, https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf (dostęp: 29.08.2022 r.).

międzyludzkich połączeń zachodzących w cyberprzestrzeni oraz ich technicznym zapleczu. Mowa tutaj przede wszystkim o ogólnoświatowym scaleniu komputerów[14] w jedną sieć i przetwarzaniu danych umieszczanych przez użytkowników. Oprócz wskazanego powyżej dokumentu został opracowany jeszcze jeden. Mianowicie „Francuska Narodowa Strategia Bezpieczeństwa Cyfrowego"[15] wydana w 2015 r. Choć w tym dokumencie nie znajdziemy innych jakościowo definicji „cyberprzestrzeni", to warto, choćby w formie sygnalizacji, o nim wspomnieć, gdyż dotyczy opisywanej problematyki w sposób bezpośredni oraz zawiera wiele ciekawych wskazówek i uwag.

W Rzeczypospolitej Polskiej także zostały podjęte działania zmierzające do właściwego określenia omawianego pojęcia. W związku z powyższym została przyjęta definicja „cyberprzestrzeni" przedstawiona w dokumencie stworzonym w 2015 r. przez Biuro Bezpieczeństwa Narodowego „Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej"[16]. Można w nim przeczytać, że „cyberprzestrzeń" oznacza

> przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci) wraz z powiązaniami między nimi oraz relacjami z użytkownikami[17].

Warty odnotowania jest także fakt istnienia definicji legalnej „cyberprzestrzeni" w Polsce, co stanowi ewenement na skalę światową, gdyż w większości

---

[14] G. Paul, *Foundations of Digital Evidence*, Chicago 2008, s. 129.

[15] *French National Digital Security Strategy*, https://www.ssi.gouv.fr/en/actualite/the-french-national-digital-security-strategy-meeting-the-security-challenges-of-the-digital-world/ (dostęp: 29.08.2022 r.).

[16] Dokument stworzony przez Biuro Bezpieczeństwa Narodowego w 2015 r. „Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej", https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf (dostęp: 29.08.2022 r.).

[17] *Ibidem*.

przypadków funkcjonujące definicje „cyberprzestrzeni" w ramach różnych porządków państwowych są tworzone w dokumentach o charakterze rządowym, nie zaś w ustawie, która stanowi źródło powszechnie obowiązującego prawa. Dnia 2 listopada 2011 r. weszła w życie[18] ustawa nowelizująca ustawę z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych[19], która wdrażając do polskiego systemu normatywnego problematykę cyberbezpieczeństwa, jednocześnie wprowadziła definicję legalną „cyberprzestrzeni". Zgodnie z tą ostatnią

> Przez cyberprzestrzeń, o której mowa w ust. 1, rozumie się przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2017 r. poz. 570), wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami[20].

Ze względu na umieszczenie w powyższej definicji odesłania ustawowego konieczne jest dokonanie jej pełnej rekonstrukcji. W tym celu należy zbadać, jaka treść kryje się pod pojęciem „systemów teleinformatycznych", które określone są w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[21]. Okazuje się, że w omawianym przypadku chodzi o zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniających przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo

[18] Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz.U. Nr 222, poz. 1323).

[19] Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (t.j. Dz.U. z 2017 r. poz. 1932 z późn. zm.).

[20] *Ibidem*.

[21] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2021 r. poz. 2070 z późn. zm.).

telekomunikacyjne[22]. W związku z powyższym, właściwe wydaje się być twierdzenie, że w ramach dokumentu „Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej" dokonano poprawnego odtworzenia pełnej zawartości normatywnej definicji legalnej „cyberprzestrzeni". Niemniej jednak cały powyższy proces interpretacyjny nie byłby w ogóle potrzebny, gdyby polski ustawodawca zdecydował się na etapie legislacyjnym nie umieszczać w definicji legalnej „cyberprzestrzeni" odesłania ustawowego. Przedmiotowe odesłanie wydaje się być całkowicie zbędne oraz zaburzające możliwość prawidłowego zrozumienia powszechnie obowiązującego prawa, z całą pewnością nie sprzyja ono postulatowi przejrzystości prawa. W związku z powyższą uwagą *de lege ferenda* treść definicji legalnej „cyberprzestrzeni" powinna mieć takie samo brzmienie jak w dokumencie „Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej", stanowiłoby to wypełnienie zasady poprawnej legislacji[23], gdyż nie do przyjęcia jest sztuczne komplikowanie prawa. Dodatkowo wydaje się, że to ostatnie stanowi naruszenie zasady określoności przepisów prawa[24]. Jednakże odnosząc się do samej treści normatywnej dyskutowanej definicji, należy zauważyć, że zwraca ona uwagę, podobnie jak opisywane powyżej, na wieloskładnikowość cyberprzestrzeni. Użycie sformułowania „systemy teleinformatyczne" w liczbie mnogiej *expressis verbis* przesądza o tym, że Internet, w świetle polskiego rozwiązania, stanowi jedynie jedną z wielu części składowych cyberprzestrzeni, gdyż składają się na nią także inne systemy teleinformatyczne oraz odpowiednie urządzenia końcowe. W związku z tym mamy tutaj do czynienia z aspektem materialnym (fizycznym) oraz niematerialnym (niefizycznym) cyberprzestrzeni. Co więcej, z owej definicji można także wyinterpretować dwa specyficzne

[22] Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz.U. z 2022 r. poz. 1648).

[23] K. Działocha, T. Zalasiński, *Zasada prawidłowej legislacji jako podstawa kontroli konstytucyjności prawa*, „Przegląd Legislacyjny" 2006, nr 3, s. 5–6; S. Wronkowska, *Zasady przyzwoitej legislacji w orzecznictwie Trybunału Konstytucyjnego*, [w:] *Księga XX-lecia orzecznictwa Trybunału Konstytucyjnego*, red. M. Zubik, Warszawa 2006, s. 673; J. Nowacki, *Rządy prawa. Dwa problemy*, Katowice 1995, s. 98; wyrok TK z dnia 12 września 2005 r., SK 13/05, LEX nr 165330; wyrok TK z dnia 30 października 2001 r., K 33/00, LEX nr 49538; wyrok TK z dnia 17 maja 2005 r., P 6/04, LEX nr 155504; Wyrok TK z dnia 25 listopada 1997 r., K 26/97, LEX nr 31034; wyrok TK z dnia 20 listopada 2002 r., K 41/02, LEX nr 57092.

[24] Wyrok TK z dnia 21 marca 2001 r., K 24/00, LEX nr 46863; wyrok TK z dnia 22 maja 2002 r., K 6/02, LEX nr 54067; wyrok TK z dnia 20 listopada 2002 r., K 41/02, LEX nr 57092.

wymiary omawianego pojęcia: wymiar horyzontalny oraz wymiar wertykalny. Pierwszy z nich polega na funkcjonowaniu w ramach cyberprzestrzeni wzajemnych oddziaływań systemów teleinformatycznych, zaś drugi z nich na korelacji systemu teleinformatycznego z użytkownikiem. W związku z tym rozwiązanie polskie, poza wskazaną powyżej wadą natury prawidłowej legislacji, zasługuje na duże uznanie, jeżeli chodzi zarówno o treść, jak i o formę aktu prawnego, która stanowi wyjątek w skali światowej.

2. Cyberprzestępczość

2.1. Wprowadzenie

Rzecz ujmując konkretnie, „cyberprzestępczość" to przestępczość w cyberprzestrzeni. Przedstawione twierdzenie wydaje się poprawne z merytorycznego punktu widzenia, choć z pewnością nie ma większej wartości naukowej czy praktycznej. Faktem jest, że ze względu na aktualny proces postępu technologicznego przestępczość w jej tradycyjnej formie została poddana daleko idącej modyfikacji. Z momentem pojawienia się cyberprzestrzeni podmioty dopuszczające się czynów zabronionych zyskały nową i atrakcyjną płaszczyznę działania. Wspomniana „atrakcyjność" cyberprzestrzeni dla przestępczości przejawia się głównie w tym, że, co do zasady, można w niej działać anonimowo, szybko, dochodowo, bezpiecznie oraz transgranicznie. Wspomniane wybrane atrybuty cyberprzestrzeni stanowiły asumpt do powstania i doskonalenia się[25] zjawiska cyberprzestępczości, co następczo implikowało pojawienie się wyspecjalizowanych form jej zwalczania[26]. Na wszystkie powyższe właściwości cyberprzestępczości uwagę zwróciła Komisja Europejska w swoim Komunikacie z dnia 7 lutego 2013 r.[27], w którym możemy przeczytać, że:

[25] K. Peretti, *Data Breaches: What the Underground World of "Carding" Reveals*, „Santa Clara Computer and High Technology Journal" 2008, nr 25(2), s. 375–413.

[26] T. Brown, E. Murphy, *Through a Scanner Darkly: Functional Neuroimaging as Evidence of Criminal Defendant's Mental States*, „Stanford Law Review" 2010, nr 62(4), s. 1119–1208.

[27] *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of The Regions. Cybersecurity Strategy of the European Union.*

> The more we live in a digital world, the more opportunities for cyber criminals to exploit. Cybercrime is one of the fastest growing forms of crime, with more than one million people worldwide becoming victims each day. Cybercriminals and cybercrime networks are becoming increasingly sophisticated and we need to have the right operational tools and capabilities to tackle them. Cybercrimes are high-profit and low-risk, and criminals often exploit the anonymity of website domains. Cybercrime knows no borders – the global reach of the Internet means that law enforcement must adopt a coordinated and collaborative cross- border approach to respond to this growing threat[28].

2.2. Propozycje definicji cyberprzestępczości

Wypracowanie prawidłowej definicji „cyberprzestępczości" to zagadnienie dyskutowane w literaturze[29]. Cyberprzestępczość można definiować jako popełnienie czynu zabronionego z użyciem Internetu lub innej sieci teleinformatycznej albo jako specyficzny rodzaj przestępczości gospodarczej, gdzie elektroniczna maszyna cyfrowa (komputer) stanowi przedmiot czynu zabronionego albo jest jego narzędziem[30]. W tym kontekście Internet, inna sieć teleinformatyczna lub komputer mogą zostać użyte poprzez zastosowanie

An Open, Safe and Secure Cyberspace, https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (dostęp: 29.08.2022 r.).

[28] *Ibidem*.

[29] J. Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Washington 2002, s. 1–12; A. Golonka, *Cyberprzestępczość – międzynarodowe standardy zwalczania zjawiska a polskie regulacje karne*, „Studia Prawnicze, Rozprawy i Materiały" 2016, nr 1(18), s. 63–84; J. Wasilewski, *Przestępczość w cyberprzestrzeni – zagadnienia definicyjne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, nr 15, s. 149–173; J. Stańczyk, *Współczesne pojmowanie bezpieczeństwa*, Warszawa 1996, *passim*; M. Karatysz, *Zjawisko cyberprzestępczości a polityka cyberbezpieczeństwa w regulacjach prawnych Rady Europy, Unii Europejskiej i Polski*, „Refleksje" 2013, nr 7, s. 139–151; B. Hołyst, J. Pomykała, *Cyberprzestępczość, ochrona informacji i kryptologia*, „Prokuratura i Prawo" 2011, nr 1, s. 5–34; U. Sieber, *Przestępczość komputerowa a prawo karne informatyczne w międzynarodowym społeczeństwie informacji i ryzyka*, „Przegląd Policyjny" 1995, nr 3, s. 6.

[30] A. Borsdorff, *Computerkriminalität*, [w:] *Wörterbuch zur Inneren Sicherheit*, red. H. Lange, Heidelberg 2006, s. 46 i n.; B. Hołyst, J. Pomykała, *op. cit.*, s. 17.

kilku wariantów możliwości[31], gdzie Internet, inna sieć teleinformatyczna lub komputer jest: przedmiotem czynności wykonawczej[32]; narzędziem głównym, za pomocą którego popełniane jest przestępstwo; narzędziem pomocniczym, które w procesie dokonywania czynu zabronionego odgrywa drugoplanową rolę (np. do przechowywania skradzionych fizycznie danych). Przedstawiane określenia cyberprzestępczości częstokroć zwracają uwagę na dwa charakterystyczne aspekty funkcjonowania przestępców działających w cyberprzestrzeni. Pierwszy, aspekt oddziaływania wewnętrznego, polega na tym, że działalność przestępcza popełniana jest w ramach płaszczyzny sieci komputerowych, a przedmiotem czynności wykonawczej jest dokładnie ta sama płaszczyzna. Podczas gdy drugi, aspekt oddziaływania zewnętrznego, polega na tym, że, tak samo jak w aspekcie oddziaływania wewnętrznego, działalność przestępcza popełniana jest w ramach płaszczyzny sieci komputerowych, ale przedmiotem czynności wykonawczej jest już inne dobro prawnie chronione. Z łatwością można zauważyć, że różnice pomiędzy aspektem oddziaływania wewnętrznego a aspektem oddziaływania zewnętrznego w tym ujęciu, swoistą linię demarkacyjną, stanowi wyłącznie przedmiot czynności wykonawczej. Kończąc rozważania czysto doktrynalne, można przywołać definicję „cyberprzestępczości", która, jak się wydaje, bierze pod uwagę większość powyższych spostrzeżeń:

> Podsumowując, cyberprzestępczość należy rozumieć jako przestępczość mającą miejsce w cyberprzestrzeni – przestrzeni przechowywania, przetwarzania oraz obrotu informacji tworzonej przez systemy elektroniczne,

[31] *Ibidem*.

[32] Co do pojęcia „przedmiotu czynności wykonawczej": M. Filar, *Pokrzywdzony* (*ofiara przestępstwa*) *w polskim prawie karnym materialnym*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2002, z. 2, s. 25, cyt. za: S. Tarapata, *Przedmiot czynności wykonawczej a przedmiot służący do popełnienia przestępstwa. Uwagi na marginesie uchwały Sądu Najwyższego z 30 października 2008 r.* (*sygn. akt I KZP 20/08*), „Czasopismo Prawa Karnego i Nauk Penalnych" 2009, z. 3, s. 131–148. Można tam przeczytać, że przedmiot czynności wykonawczej oznacza „takie dobro chronione przepisami prawa karnego, na którym czyn przestępczy jest dokonywany, tj. zgodnie z zamiarem sprawcy jest bezpośrednio atakowane lub (w przypadku nieumyślności) w relacji do którego naruszane zostają zasady bezpiecznego obchodzenia się z danym dobrem, a nie także i takie, które tylko pośrednio doznają uszczerbku przy okazji takiego ataku, lub są nim pośrednio zagrożone".

> a przede wszystkim Internet. W wąskim rozumieniu obejmuje jedynie takie zamachy, których zrealizowanie nie będzie możliwe poza cyberprzestrzenią, podczas gdy w szerokim ujęciu będzie to ogół zachowań przestępczych dokonanych z wykorzystaniem urządzeń teleinformatycznych. Komputer może być zarówno celem przestępstwa, kluczowym elementem, czy po prostu narzędziem koniecznym do jego popełniania. Niezależnie od zastosowania, użycie komputera umożliwia działanie z dużej odległości, często bez świadomości, gdzie faktycznie jest zlokalizowane urządzenie. Sprawca nie musi znajdować się w miejscu popełnienia przestępstwa, a dowody jego działania często mieszczą się w geograficznie odległej przestrzeni[33].

Przechodząc do definicji uznawanych przez wybrane organizacje międzynarodowe i zaczynając od Unii Europejskiej, należy zauważyć, że Komisja Europejska w swoim Komunikacie do Parlamentu Europejskiego, Rady oraz Komitetu Regionów w kierunku ogólnej strategii zwalczania cyberprzestępczości[34] zauważa, że ze względu na brak wypracowania jednolitej definicji „cyberprzestępczości" pojęcia takie jak „przestępczość komputerowa", „cyberprzestępczość", „przestępczość związana z komputerami" czy „przestępczość przy użyciu zaawansowanych technologii" stosowane są zamiennie. W związku z powyższym Komisja Europejska przyjęła, że dla celów swojego Komunikatu pod pojęciem „cyberprzestępczości" powinno się rozumieć „czyny przestępcze dokonane przy użyciu sieci łączności elektronicznej i systemów informatycznych lub skierowane przeciwko takich sieciom i systemom"[35]. W tym samym dokumencie możemy przeczytać, że pojęcia „cyberprzestępczości", co do zasady, używa się w odniesieniu do trzech kategorii przestępstw. Pierwsza dotyczy

---

[33] A. Jaroszewska, *Wybrane aspekty cyberprzestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne*, Olsztyn 2017, s. 11–12 (w cytowanym fragmencie powoływani są następujący przedstawiciele literatury przedmiotu: J. Kosiński, *Paradygmaty cyberprzestępczości*, Warszawa 2015, s. 88; J. Kulesza, *op. cit.*, s. 152–153).

[34] *Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów z dnia 25 maja 2007 roku w kierunku ogólnej strategii zwalczania cyberprzestępczości*, http://eur-lex.europa.eu/legal-content/PL/TXT /HTML/?uri=CELEX:52007DC0267&from=PL (dostęp: 29.08.2022 r.).

[35] *Ibidem*.

tradycyjnych form przestępstw (np. oszustwo czy fałszerstwo), które popełniane są przy użyciu elektronicznych sieci informatycznych oraz systemów informatycznych. Druga jest utożsamiana z publikacją nielegalnych treści w mediach elektronicznych (np. treści związane z seksualnym wykorzystywaniem dzieci czy nawoływaniem do nienawiści rasowej). Trzecia składa się z przestępstw charakterystycznych dla elektronicznych sieci informatycznych oraz systemów informatycznych (ataki przeciwko systemom informatycznym, ataki typu *denial of service* czy hakerstwo). Wszystkie powyższe kategorie, pomimo oczywistych różnic, posiadają wspólne przymioty, mianowicie: mogą być one popełniane na masową skalę[36] oraz odległość geograficzna pomiędzy miejscem popełnienia przestępstwa a jego skutkami może być znaczna. Natomiast Rada Europy w dokumencie zatytułowanym „Raport Wyjaśniający do Konwencji o cyberprzestępczości"[37] i przyjętym 23 listopada 2001 r. w Budapeszcie zauważa, że:

> These „cyber-space offences" are either committed against the integrity, availability, and confidentiality of computer systems and telecommunication networks or they consist of the use of such networks of their services to commit traditional offences. The transborder character of such offences, e.g. when committed through the Internet, is in conflict with the territoriality of national law enforcement authorities[38].

Po tym wstępnym zarysie problemu autorzy powołanego dokumentu proponują, aby przez pojęcie „cyberprzestępstwa" rozumieć

> cyberspace offences, in particular those committed through the use of telecommunication networks, e.g. the Internet, such as illegal money transactions,

[36] M. Gruchoła, *Polityka Unii Europejskiej w zakresie cyberprzestępczości*, [w:] *Patologie w cyberświecie*, red. S. Bębas, J. Plis, J. Bednarek, Radom 2012, s. 149.

[37] Raport Wyjaśniający do Konwencji o cyberprzestępczości (ang. *Explanatory Report to the Convention on Cybercrime*) przyjęty 23 listopada 2001 r. w Budapeszcie, https://rm.coe.int/16800cce5b (dostęp: 29.08.2022 r.).

[38] *Ibidem*.

> offering illegal services, violation of copyright, as well as those which violate human dignity and the protection of minors[39].

Z kolei Organizacja Narodów Zjednoczonych proponuje, aby pojęcie „cyberprzestępczości" rozumieć zarówno w sposób ścisły, jak i szeroki. Pierwszy z nich kryje szereg działań uderzających bezpośrednio w bezpieczeństwo systemów komputerowych oraz procesowanych przez nie danych, zaś pod drugim wariantem znajdują się wszelkie nielegalne działania popełniane z użyciem lub dotyczące systemów i sieci komputerowych[40].

2.3. Analiza prawnoporównawcza

W USA w dokumencie znajdującym się na oficjalnej stronie internetowej Senackiego Komitetu Polityki Demokratycznej (ang. *Senate Democratic Policy Committee*) „Słowniczek Najważniejszych Terminów z zakresu Bezpieczeństwa Informacji"[41] możemy przeczytać, że:

> Cybercrime is criminal activity conducted using computers and the Internet, often financially motivated. Cybercrime includes identity theft, fraud, and internet scams, among other activities. Cybercrime is distinguished from other forms of malicious cyber activity, which have political, military, or espionage motivations[42].

Z powołanej definicji wynika, że cyberprzestępczość w USA rozumiana jest jako działanie, co do zasady, motywowane finansowo i popełniane przy użyciu komputera oraz Internetu. Należy zauważyć, że przy zastosowaniu tak

---

[39] *Ibidem*.

[40] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia terroryzmem*, Warszawa 2010, s. 152.

[41] *Glossary of Cyber Related Terms* (*Słowniczek Najważniejszych Terminów z zakresu Bezpieczeństwa Informacji*), https://www.dpc.senate.gov/docs/fs-112-2-183.pdf (dostęp: 29.08.2022 r.).

[42] *Ibidem*.

rozumianej terminologii samo używanie komputera, choćby prowadziło do dokonania czynu zabronionego, nie jest wystarczające do zakwalifikowania takiego czynu jako cyberprzestępstwa. Uwaga ta ma także zastosowanie do używania Internetu bez komputera. Jednakże wydaje się, że użycie pojęcia „komputery" (ang. *computers*) przez autorów omawianej definicji ma w tym przypadku szersze znaczenie niż intuicyjnie można mu przypisywać. W związku z powyższym, sprawia wrażenie zasadności twierdzenie, że przez pojęcie to powinno się rozumieć wszelkie narzędzia do obsługi Internetu. W takim przypadku powołana definicja „cyberprzestępstwa" zawiera warunek koincydencji[43] działania w Internecie oraz używania narzędzia do obsługi Internetu. Warunek taki zdaje się być spójny logicznie, gdyż każda działalność znajdująca swój obraz w Internecie powodowana jest w rezultacie przez urządzenie końcowe sterowane przez użytkownika, któremu, właśnie na tej podstawie, można przypisać takie, a nie inne zachowanie. Poza powyższym komentarzem definicja „cyberprzestępstwa" stworzona przez SKPD jest w pełni zrozumiała i należy ją ocenić pozytywnie.

We Francji, w odróżnieniu od USA, funkcjonują przynajmniej dwie różne definicje „cyberprzestępstwa". W powoływanym już dokumencie Agencji i Bezpieczeństwa Sieci oraz Informacji „Obrona oraz bezpieczeństwo systemów informacyjnych. Strategia dla Francji"[44] z 2011 r. zawarto twierdzenie, że cyberprzestępstwami są:

> Acts contravening international treaties and national laws, targeting networks and information systems, or using them to commit an offence or crime[45].

Na oficjalnej stronie internetowej estońskiego Centrum Doskonalenia Cyberobrony Organizacji Traktatu Północnoatlantyckiego w Tallinie[46] widniała

---

[43] Słownikowo koincydencja to jednoczesne występowanie czegoś, współistnienie pewnych związków bądź zjawisk, czy po prostu zbieżność sytuacji (S. Skorupka, H. Auderska, Z. Łempicka, *Mały słownik języka polskiego*, Warszawa 1968, s. 283).

[44] *NATIONAL STRATEGY TO SECURE CYBERSPACE*, https://www.cisa.gov/national-strategy-secure-cyberspace (dostęp: 29.08.2022 r.).

[45] *Ibidem*.

[46] *Cyber-Definitions*, https://ccdcoe.org/cyber-definitions.html (dostęp: 29.08.2022 r.).

definicja „cyberprzestępstwa" przypisywana Francji, zgodnie z którą cyberprzestępstwem jest:

> The process of decrypt Acts contravening international treaties and national laws, targeting networks or information systems, or using them to commit an offence or crime e.g. encrypted data, without the encryption keys[47].

Obie powyższe propozycje posiadają wspólne cechy oraz pewne różnice. Zaczynając od przymiotów tożsamych, należy zauważyć, że zarówno w pierwszej, jak i w drugiej definicji podany jest ten sam zakres przedmiotowy przepisów możliwych do naruszenia, czyli przepisy prawa krajowego oraz międzynarodowego prawa traktatów. Rozwiązanie takie nie powinno dziwić, gdyż każde państwo dba o poszanowanie swojego porządku prawnego, a częścią składową takiego porządku są także umowy międzynarodowe. To ostatnie dodatkowo potwierdza art. 55 Konstytucji Republiki Francuskiej[48], zgodnie z którym traktaty lub umowy międzynarodowe należycie ratyfikowane bądź zatwierdzone, zyskują z chwilą ich ogłoszenia moc wyższą niż ustawy, o ile zasada ta jest stosowana przez drugą stronę wobec tych umów lub traktatów[49]. Przechodząc zaś do różnic, to pierwsza z nich polega na określeniu, jaka czynność jest kwalifikowana jako cyberprzestępstwo, w pierwszej definicji są to „czyny" (ang. *acts*), zaś w drugiej jest to „proces odszyfrowywania" (ang. *The process of decrypt Acts*). Wydaje się, że jest to znacząca dysproporcja, gdyż nie każdy czyn będzie procesem odszyfrowywania, jednakże zależność ta będzie zachodzić w drugą stronę, ponieważ każdy proces odszyfrowywania będzie czynem. W związku z powyższym zakres znaczeniowy terminu „czyn" jest o wiele szerszy niż terminu „proces odszyfrowywania". Druga i zarazem ostatnia różnica bazuje na

---

[47] *Ibidem*.

[48] Konstytucja Republiki Francuskiej z dnia 4 października 1958 r. ogłoszona w Dzienniku Urzędowym Republiki Francuskiej (fr. *Journal Officiel de la Republique Française*) nr 234 z dnia 5 października 1958 r., dostępna na oficjalnej stronie internetowej Zgromadzenia Narodowego Francji, https://www.assemblee-nationale.fr/connaissance/constitution.asp (dostęp: 29.08.2022 r.).

[49] *Ibidem*; Oryginalna treść art. 55 Konstytucji Republiki Francuskiej: *Les traités ou accords régulièrement ratifiés ou approuvés ont, dès leur publication, une autorité supérieure à celle des lois, sous réserve, pour chaque accord ou traité, de son application par l'autre partie*.

tym, że wspomniana powyżej czynność kwalifikująca dane zachowanie jako cyberprzestępstwo ma na celu, w pierwszej definicji „dokonanie działalności przestępczej w sieci i systemach informacyjnych lub wykorzystanie ich do popełnienia przestępstwa". Natomiast w drugiej definicji cel ten został określony jako „dokonanie działalności przestępczej w sieci lub systemach informacyjnych, lub wykorzystanie ich do popełnienia przestępstwa". Dysharmonia polega na zastosowaniu odmiennych funktorów logicznych w cytowanych fragmentach definicji. Zarówno w pierwszej, jak i drugiej został wykorzystany funktor zdaniotwórczy o charakterze ekstencjonalnym (tzw. funktor prawdziwości), jednakże rozdźwiękiem jest forma ich użycia[50]. W pierwszym przypadku jest to użycie koniunkcyjne „i" (ang. *and*), które zakłada koincydencję łączonych argumentów, podczas gdy w drugim wariancie jest to użycie alternatywne zwykłe „lub" (ang. *or*), które zakłada możliwość występowania tylko jednego argumentu albo dwóch naraz. Wynika z tego, że zgodnie z pierwszą definicją, żeby można było mówić o cyberprzestępstwie, musi zostać spełniony warunek jednoczesnego dokonania działalności w sieci i systemach informacyjnych. W związku z powyższymi rozważaniami żadna z zaprezentowanych definicji nie jest idealna, jednakże połączenie rozwiązań zastosowanych w nich może prowadzić do wyeliminowania spostrzeżonych niedoskonałości. Z tego powodu *de lege ferenda* przedmiotowe połączenie mogłoby polegać na zastąpieniu, w drugiej definicji, terminu „proces odszyfrowywania" terminem „czyn" tak, żeby powstała definicja o następującej treści: „Cyberprzestępstwem jest czyn niezgodny z międzynarodowymi traktatami i przepisami krajowymi, którego celem jest działalność przestępcza w sieci lub systemie informatycznym, lub wykorzystywanie ich do popełnienia przestępstwa".

W Polsce w dokumencie stworzonym przez Ministerstwo Administracji i Cyfryzacji we współpracy z Agencją Bezpieczeństwa Wewnętrznego „Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej"[51] można przeczytać,

[50] S. Lewandowski, H. Machińska, A. Malinowski, J. Petzel, *Logika dla prawników*, Warszawa 2003, s. 31–33, 100–101.

[51] *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, http://www.cert.gov.pl/download/3/161/PolitykaOchronyCyberprzestrzeniRP148x210wersjapl.pdf (dostęp: 29.08.2022 r.).

że cyberprzestępstwo to „czyn zabroniony popełniony w obszarze cyberprzestrzeni”[52]. Dokonując odszyfrowania cytowanej definicji „cyberprzestępstwa”, w pierwszej kolejności należy przypomnieć ustanowioną w Polsce definicję legalną „cyberprzestrzeni” i dokonać podmiany użytego w cytowanej definicji cyberprzestępstwa terminu „cyberprzestrzeni” na jego ustalone znaczenie. Po przeprowadzeniu zapowiedzianego procesu dekodowania można uzyskać definicję „cyberprzestępstwa” o następującej treści:

> cyberprzestępstwo to czyn zabroniony popełniony w przestrzeni przetwarzania i wymiany informacji tworzonej przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci) wraz z powiązaniami między nimi oraz relacjami z użytkownikami.

Kolejnym krokiem, w celu poprawnej interpretacji definicji stworzonej przez MAC i ABW, jest ustalenie znaczenia terminu „czyn zabroniony” i dokonanie takiego samego zabiegu jak powyżej. Okazuje się, że w polskim Kodeksie karnym[53], dokładnie w art. 115 § 1, znajduje się definicja legalna omawianego pojęcia, zgodnie z którą „Czynem zabronionym jest zachowanie o znamionach określonych w ustawie karnej”. Oczywistym jest, że nie jest to tylko zachowanie przewidziane w ustawie karnej, ale także przewidziane w prawie międzynarodowym wiążącym Polskę. Wniosek taki *expressis verbis* wynika z art. 9 Konstytucji Rzeczypospolitej Polskiej[54], który stanowi, że Polska przestrzega wiążącego ją prawa międzynarodowego. W związku z powyższymi rozważaniami i po zastosowaniu zaprezentowanych technik interpretacyjnych uzyskujemy definicję

[52] *Ibidem*.

[53] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. Dz.U. z 2022 r. poz. 1138).

[54] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. Nr 78, poz. 483 z późn. zm.).

cyberprzestępstwa zaproponowaną w dokumencie stworzonym przez MAC i ABW o następującej treści:

> cyberprzestępstwo to zachowanie o znamionach określonych w ustawie karnej, w tym w prawie międzynarodowym, popełnione w przestrzeni przetwarzania i wymiany informacji tworzonej przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci) wraz z powiązaniami między nimi oraz relacjami z użytkownikami.

Reasumując, *de lege ferenda* polski legislator powinien rozważyć wprowadzenie definicji „cyberprzestępstwa" o wskazanej treści do swojego systemu prawnego, innymi słowy winien stworzyć definicję legalną „cyberprzestępstwa", tak jak ma to miejsce z pojęciem „cyberprzestrzeni".

3. Wnioski

Prezentowane podsumowanie zawiera dwa postulaty *de lege ferenda*, których wdrożenie usprawni dyskusję nad zagadnieniami związanymi z cyberprzestrzenią oraz cyberprzestępczością.

Po pierwsze, konieczne jest stworzenie na forum międzynarodowym jednej i powszechnie akceptowanej definicji cyberprzestrzeni, która brałaby pod uwagę większość pozytywnych aspektów występujących w propozycjach znaczeniowych przedstawianych na płaszczyźnie dogmatycznej i przez wybrane organizacje międzynarodowe i pozarządowe oraz współczesne państwa. Postulowanym byłoby wypracowanie jej i przyjęcie na forum Organizacji Narodów Zjednoczonych, gdyż zyskałaby ona wtedy przymiot uniwersalności i powszechności. Jednakże do tego czasu należy skupić się na polskim ustawodawstwie, gdyż, w tym zakresie, nie jest ono trafne ze względu na brak przejrzystości. Z tego powodu

treść polskiej definicji legalnej „cyberprzestrzeni" powinna mieć takie samo brzmienie jak w dokumencie „Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej", stanowiłoby to wypełnienie zasady poprawnej legislacji, gdyż nie do przyjęcia jest sztuczne komplikowanie prawa. Dodatkowo wydaje się, że to ostatnie stanowi naruszenie zasady określoności przepisów prawa. Wynikiem spełnienia tego postulatu byłoby zamienienie enigmatycznego sformułowania:

> Przez cyberprzestrzeń, o której mowa w ust. 1, rozumie się przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2017 r. poz. 570), wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami

sformułowaniem:

> Cyberprzestrzeń oznacza przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci) wraz z powiązaniami między nimi oraz relacjami z użytkownikami.

Po drugie, podobnie jak miało to miejsce przy definicji „cyberprzestrzeni" także w przypadku cyberprzestępczości nieuniknione jest stworzenie jednej i powszechnie akceptowanej definicji, która brałaby pod uwagę większość pozytywnych aspektów występujących w propozycjach znaczeniowych przedstawianych na płaszczyźnie dogmatycznej i przez wybrane organizacje międzynarodowe i pozarządowe oraz współczesne państwa. Rekomendowane jest zawarcie jej w tym samym akcie prawa międzynarodowego Organizacji Narodów Zjednoczonych co definicji „cyberprzestrzeni". Tylko i wyłącznie za pomocą postulowanego rozwiązania możliwe będzie przypisanie jej cechy

uniwersalności i powszechności. Jednakże, przechodząc na grunt krajowych systemów prawnych, wypada wnioskować za przyjęciem definicji „cyberprzestępczości" o następującej formie:

> cyberprzestępstwo to zachowanie o znamionach określonych w ustawie karnej, w tym w prawie międzynarodowym, popełnione w przestrzeni przetwarzania i wymiany informacji tworzonej przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci) wraz z powiązaniami między nimi oraz relacjami z użytkownikami.

Dodatkowo *de lege ferenda* polski legislator powinien rozważyć wprowadzenie definicji „cyberprzestępstwa" o wskazanej treści do swojego systemu prawnego, innymi słowy winien stworzyć definicję legalną „cyberprzestępstwa", tak jak ma to miejsce z pojęciem „cyberprzestrzeni".

Bibliografia

Aleksandrowicz T., *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, nr 15.

Babis H., *Internet*, [w:] *Encyklopedia zagadnień międzynarodowych*, red. E. Cała-Wacinkiewicz, R. Podgórzański, Warszawa 2011.

Bednarek J., Andrzejewska A., *Cyberświat – możliwości i zagrożenia*, Warszawa 2009.

Berman P., *The Globalization of Jurisdiction*, „University of Pennsylvania Law Review" 2002, nr 151(2).

Boni B., *Creating a Global Consensus Against Cybercrime*, „Network Security" 2001, nr 9.

Borsdorff A., *Computerkriminalität*, [w:] *Wörterbuch zur Inneren Sicherheit*, red. H. Lange, Heidelberg 2006.

Brenner S., Schwerha J., *Introduction-Cybercrime: A Note on International Issues*, „Information Systems Frontiers" 2004, nr 6(2).

Brown T., Murphy E., *Through a Scanner Darkly: Functional Neuroimaging as Evidence of Criminal Defendant's Mental States*, „Stanford Law Review" 2010, nr 62(4).
Buczyńska-Garewicz H., *O pojęciu cnoty: czy cnota jest przeżytkiem?*, „Teksty: teoria literatury, krytyka, interpretacje" 1981, nr 1(55).
Chung W., Chen H., Chang W., Chou S., *Fighting cybercrime: a review and the Taiwan Experience*, „Decision Support Systems" 2006, nr 41.
Cieślak M., *Proces karny* (*skrypt*), Kraków 1952.
Cieślak M., Środki przymusu na tle bodźców prawnych w procesie karnym, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace Prawnicze" 1960, z. 7.
Clough J., *A world of difference: The Budapest Convention on Cybercrime and the challenges of harmonization*, „Monash University Law Review" 2014, nr 40(3).
Coleman C., *Security Cyberspace – New Laws and Developing Strategies*, „Computer Law and Security Report" 2003, nr 19(2).
Dobrzeniecki K., *Prawo a etos cyberprzestrzeni*, Toruń 2004.
Działocha K., Zalasiński T., *Zasada prawidłowej legislacji jako podstawa kontroli konstytucyjności prawa*, „Przegląd Legislacyjny" 2006, nr 3.
Filar M., *Pokrzywdzony* (*ofiara przestępstwa*) *w polskim prawie karnym materialnym*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2002, nr 2.
Gercke M., *Europe's Legal Approaches to Cybercrime*, „ERA Forum", 2009, nr 10.
Gercke M., *The Convention on Cybercrime*, „Multimedia und Recht" 2004, nr 20.
Golonka A., *Cyberprzestępczość – międzynarodowe standardy zwalczania zjawiska a polskie regulacje karne*, „Studia Prawnicze, Rozprawy i Materiały" 2016, nr 1(18).
Gruchoła M., *Polityka Unii Europejskiej w zakresie cyberprzestępczości*, [w:] *Patologie w cyberświecie*, red. S. Bębas, J. Plis, J. Bednarek, Radom 2012.
Grzelak M., Liedel K., *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – Zarys problemu*, „Bezpieczeństwo Narodowe" 2012, nr 22.
Hancock B., *US and Europe Cybercrime Agreement Problems*, „Computers and Security" 2000, nr 19(4).
Hilley S., *Pressure Mounts on US Senate to Pass Cybercrime Treaty*, „Digital Investigation" 2005, nr 2.
Hołyst B., Pomykała J., *Cyberprzestępczość, ochrona informacji i kryptologia*, „Prokuratura i Prawo" 2011, nr 1.
Jaroszewska A., *Wybrane aspekty cyberprzestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne*, Olsztyn 2017.
Karatysz M., *Zjawisko cyberprzestępczości a polityka cyberbezpieczeństwa w regulacjach prawnych Rady Europy, Unii Europejskiej i Polski*, „Refleksje" 2013, nr 7.
Katyal N., *Criminal Law in Cyberspace*, „University of Pennsylvania Law Review" 2001, nr 149(4).
Kigerl A., *CAN SPAM Act: An Empirical analysis*, „International Journal of Cyber Criminology" 2009, nr 3(2).

Kohl U., *Eggs, Jurisdiction and the Internet*, „The International and Comparative Law Quarterly" 2002, nr 51(3).
Kosiński J., *Paradygmaty cyberprzestępczości*, Warszawa 2015.
Kulesza J., *Międzynarodowe Prawo Internetu*, Poznań 2010.
Lessig L., Resnick P., *Zoning Speech on the Internet: A Legal and Technical Model*, „Michigan Law Review" 1999, nr 98(2).
Lewandowski S., Machińska H., Malinowski A., Petzel J., *Logika dla prawników*, Warszawa 2003.
Lewis J., *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Washington 2002.
Levy P., *Drugi potop*, [w:] *Nowe media w komunikacji społecznej w XX wieku. Antologia*, red. M. Hopfinger, Warszawa 2002.
Madej M., *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*, [w:] *Bezpieczeństwo teleinformatyczne państwa*, red. M. Madej, M. Terlikowski, Warszawa 2009.
Marion N., *Symbolic Policies in Clinton's Crime Control Agenda*, „Buffalo Criminal Law Review" 1997, nr 1.
Moitra S., *Developing Policies for Cybercrime*, „European Journal of Crime, Criminal Law and Criminal Justice" 20005, nr 13(3.
Nowacki J., *Rządy prawa. Dwa problemy*, Katowice 1995.
Nowak A., *Cyberprzestrzeń jako nowa jakość zagrożeń*, „Zeszyty Naukowe Akademii Obrony Narodowej" 2013, z. 3(92).
Nuth M., *Taking Advantage of New Technologies: For and Against Crime Computer Law and Security Report*, „Computer Law & Security Review" 2008, nr 24.
Ottis R., Lorents P., *Cyberspace: Definition and Implications. In Proceedings of the 5th International Conference on Information Warfare and Security*, Dayton 2010.
Paul G., *Foundations of Digital Evidence*, Chicago 2008.
Peretti K., *Data Breaches: What the Underground World of "Carding" Reveals*, „Santa Clara Computer and High Technology Journal" 2008, nr 25(2).
Reidenberg J., *Technology and Internet Jurisdiction*, „University of Pennsylvania Law Review" 2005, nr 153(6).
Resseguie D., *Computer Searches and Seizure*, „Cleveland State Law Review" 2000, nr 48(185).
Shapiro A., *The Internet*, „Foreign Policy" 1999, nr 115.
Sieber U., *Przestępczość komputerowa a prawo karne informatyczne w międzynarodowym społeczeństwie informacji i ryzyka*, „Przegląd Policyjny" 1995, nr 3.
Silver O., *European Cybercrime Proposal Released*, „Computer Fraud and Security" 2001, nr 5.
Simon E., *Cyberporn and Censorship: Constitutional Barriers to Preventing Access to Internet Pornography by Minors*, „The Journal of Criminal Law and Criminology" 1998, nr 88(3).

Sinrod J., Reilly W., *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, „Santa Clara Computer and High Technology Law Journal" 2000, nr 16(2).

Skorupka S., Auderska H., Łempicka Z., *Mały słownik języka polskiego*, Warszawa 1968.

Speer L., *Redefining Borders: The Challenges of Cybercrime*, „Crime, Law and Social Change" 2000, nr 34.

Stańczyk J., *Współczesne pojmowanie bezpieczeństwa*, Warszawa 1996.

Stolz A., *Congress and Capital Punishment: An Exercise in Symbolic Politics*, „Law and Policy Quarterly" 1983, nr 5(2).

Suchorzewska A., *Ochrona prawna systemów informatycznych wobec zagrożenia terroryzmem*, Warszawa 2010.

Swire P., *Elephants and Mice Revisited: Law and Choice of Law on the Internet*, „University of Pennsylvania Law Review" 2005, nr 153(6).

Tadeusiewicz R., *Wychowywanie dla cyberprzestrzeni jednym z warunków zapobiegania cyberuzależnieniom*, [w:] *Cyberuzależnienia: przeciwdziałanie uzależnieniom od komputera i Internetu*, red. E. Mastalerz, K. Pytel, H. Noga, Kraków 2007.

Tarapata S., *Przedmiot czynności wykonawczej a przedmiot służący do popełnienia przestępstwa. Uwagi na marginesie uchwały Sądu Najwyższego z 30 października 2008 r.* (*sygn. akt I KZP 20/08*), „Czasopismo Prawa Karnego i Nauk Penalnych" 2009, z. 3.

Tekielska P., Czekaj Ł., *Działania służb w Unii Europejskiej realizujących zadania na rzecz bezpieczeństwa cybernetycznego*, [w:] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, red. M. Górka, Warszawa 2014.

Walden I., *Harmonising Computer Crime Laws in Europe*, „European Journal of Crime, Criminal Law and Criminal Justice" 2004, nr 12(4).

Wang S., *Measures of Retaining Digital Evidence to Prosecute Computer-based Cyber--crimes*, „Computer Standards and Interfaces" 2007, nr 29.

Wasilewski J., *Przestępczość w cyberprzestrzeni – zagadnienia definicyjne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, nr 15.

Wasilewski J., *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9.

Wible B., *A Site Where Hackers are Welcome: Using Hack-In Contests to Shape Preferences and Deter Computer Crime*, „The Yale Law Journal" 2003, nr 112(6).

Winick R., *Searches and seizures of computers and computer data*, „Harvard Journal of Law & Technology" 1994, nr 8(1).

Wronkowska S., *Zasady przyzwoitej legislacji w orzecznictwie Trybunału Konstytucyjnego*, [w:] *Księga XX-lecia orzecznictwa Trybunału Konstytucyjnego*, red. M. Zubik, Warszawa 2006.

Akty prawne

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. Nr 78, poz. 483 z późn. zm.).

Konstytucja Republiki Francuskiej z dnia 4 października 1958 roku ogłoszona w Dzienniku Urzędowym Republiki Francuskiej (fr. *Journal Officiel de la Republique Française*) nr 234 z dnia 5 października 1958 roku. Dostępna na oficjalnej stronie internetowej Zgromadzenia Narodowego Francji (https://www.assemblee-nationale.fr/connaissance/constitution.asp, dostęp: 29.08.2022 r.).

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz.U. z 2022 r. poz. 1138).

Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (t.j. Dz.U. z 2017 r. poz. 1932 z późn. zm.).

Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz.U. z 2022 r. poz. 1648).

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2021 r. poz. 2070 z późn. zm.).

Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz.U. Nr 222 poz. 1323).

Orzecznictwo

Wyrok Trybunału Konstytucyjnego z dnia 25 listopada 1997 r., K 26/97, LEX nr 31034.

Wyrok Trybunału Konstytucyjnego z dnia 21 marca 2001 r., K 24/00, LEX nr 46863.

Wyrok Trybunału Konstytucyjnego z dnia 30 października 2001 r., K 33/00, LEX nr 49538.

Wyrok Trybunału Konstytucyjnego z dnia 22 maja 2002 r., K 6/02, LEX nr 54067.

Wyrok Trybunału Konstytucyjnego z dnia 20 listopada 2002 r., K 41/02, LEX nr 57092.

Wyrok Trybunału Konstytucyjnego z dnia 17 maja 2005 r., P 6/04, LEX nr 155504.

Wyrok Trybunału Konstytucyjnego z dnia 12 września 2005 r., SK 13/05, LEX nr 165330.

Netografia

Cyber-Definitions, https://ccdcoe.org/cyber-definitions.html (dostęp: 29.08.2022 r.).

Cyberspace: Definition and Implications, https://ccdcoe.org/library/publications/cyberspace-definition-and-implications/ (dostęp: 29.08.2022 r.).

Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej, https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf (dostęp: 29.08.2022 r.).

French National Digital Security Strategy, https://www.ssi.gouv.fr/en/actualite/the-french-national-digital-security-strategy-meeting-the-security-challenges-of-the-digital-world/ (dostęp: 29.08.2022 r.).

Glossary of Cyber Related Terms (*Słowniczek Najważniejszych Terminów z zakresu Bezpieczeństwa Informacji*), https://www.dpc.senate.gov/docs/fs-112-2-183.pdf (dostęp: 29.08.2022 r.).

Information system defence and security. France's strategy, https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf (dostęp: 29.08.2022 r.).

Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of The Regions. Cybersecurity Strategy of the European Union. An Open, Safe and Secure Cyberspace, https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (dostęp: 29.08.2022 r.).

Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów z dnia 25 maja 2007 roku w kierunku ogólnej strategii zwalczania cyberprzestępczości, http://eur-lex.europa.eu/legal-content/PL/TXT /HTML/?uri=CELEX:52007DC0267&from=PL (dostęp: 29.08.2022 r.).

National Institute of Standards and Technology, https://csrc.nist.gov/glossary/term/cyberspace (dostęp: 29.08.2022 r.).

NATIONAL STRATEGY TO SECURE CYBERSPACE, https://www.cisa.gov/national-strategy-secure-cyberspace (dostęp: 29.08.2022 r.).

Obrona oraz bezpieczeństwo systemów informacyjnych. Strategia dla Francji, https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf (dostęp: 29.08.2022 r.).

Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, http://www.cert.gov.pl/download/3/161/PolitykaOchronyCyberprzestrzeniRP148x210wersjapl.pdf (dostęp: 29.08.2022 r.).

Raport Wyjaśniający do Konwencji o cyberprzestępczości („*Explanatory Report to the Convention on Cybercrime*"), przyjęty 23 listopada 2001 r. w Budapeszcie, https://rm.coe.int/16800cce5b (dostęp: 29.08.2022 r.).

Łukasz Pohl

Miejsce popełnienia cyberprzestępstwa z perspektywy polskiego kodeksu karnego z 1997 r.

Rozpocząć należy od tego, że zagadnienie miejsca popełnienia cyberprzestępstwa jest problematyczne już z tego powodu, że centralnemu w jego ramach pojęciu „cyberprzestępstwa" nadaje się w literaturze przedmiotu różne znaczenia. Bez wątpienia okolicznością sprzyjającą rozwojowi występującej tu wieloznaczności jest fakt braku stosownej wypowiedzi polskiego kodyfikatora. Nie ulega bowiem wątpliwości, że kodeksowe zdefiniowanie rzeczonego pojęcia istotnie ograniczyłoby rejestrowaną tu polisemię i ukierunkowałoby ewentualne spory interpretacyjne już li tylko na detaliczne kwestie związane z wykładnią składników użytych w części definiującej definicji owego pojęcia. Z drugiej jednak strony nie można tracić z pola widzenia i tych głosów doktryny prawniczej, które wyrażają daleko idący sceptycyzm wobec zasadności pomysłu zdefiniowania pojęcia „cyberprzestępstwa" w kodeksie karnym – sceptycyzm najczęściej uzasadniany brakiem potrzeby takiej definicji, a także obawą, że ewentualne jej sformułowanie mogłoby w sposób merytorycznie niezasadny spłaszczyć wielowymiarowość zjawiska obejmowanego mianem naukowo ujmowanej cyberprzestępczości. Nie wchodząc w tym miejscu w rozstrzyganie, którą z naszkicowanych opcji należałoby poprzeć, nie sposób jednak nie odnotować, że w obecnym stanie prawnym, wyznaczonym kształtem słownym aktualnie obowiązujących przepisów polskiego kodeksu karnego z 1997 r., niewątpliwie nie jest spełniony warunek konieczny wprowadzenia rozważanej definicji do wskazanego kodeksu, gdyż wyraz „cyberprzestępstwo", jako niepojawiający się w jego przepisach, nie jest wyrazem języka tego kodeksu. Tym samym nie ma tu potrzeby jego objaśniania na użytek wykładni statuujących ten kodeks przepisów.

Ażeby powyższego wywodu nie zawieszać w teoretycznej próżni, potwierdźmy krótko, iż pojęcie „cyberprzestępstwa" nacechowane jest daleko idącą wieloznacznością. I tak, jak rejestruje to w szczególności Mariusz Nawrocki[1], opierając się w tym względzie na sprawozdaniu Brunona Hołysta[2], już na zjeździe *Forensic Science Society* w Huntingdon w 2001 r. podjęto próbę sprecyzowania pojęcia „cyberprzestępstwa", obejmując nim kilka charakterystycznych typów zachowań. Jak podnosi B. Hołyst, wyodrębniono tamże 6 kategorii przestępstw cybernetycznych (ang. *cyber–crimes*):

1/ przestępstwa ułatwiane przez komputer (ang. *computer assisted*),
2/ przestępstwa, których popełnienie komputer umożliwia (ang. *computer enabled*),
3/ przestępstwa, których nie da się popełnić bez komputerowej techniki (ang. *computer only*),
4/ przestępstwa możliwe do popełnienia w sposób konwencjonalny, ale też z wykorzystaniem Internetu (ang. *Internet assisted*),
5/ przestępstwa, które łatwiej popełnić, wykorzystując Internet (ang. *Internet enabled*),
6/ oraz przestępstwa, których popełnienie możliwe jest wyłącznie przy wykorzystaniu Internetu (ang. *Internet only*)[3].

Dodajmy także, że widoczne wobec powyższego zróżnicowanie zachowań obejmowanych pojęciem „cyberprzestępstwa" pogłębiane jest przez okoliczność, iż w literaturze przedmiotu nader często rzeczone pojęcie uznaje się za równoznaczne względem pojęcia „przestępstwa komputerowego", któremu – niestety – także towarzyszą dyskusje ujawniające brak zgody co do jego znaczeniowego zakresu.

Nadto – co również istotne – w ramach owych dyskusji zwraca się jeszcze uwagę na okoliczność, że pojęcie „przestępstwa komputerowego" może być różnie rozumiane ze względu na przyjmowany jurydyczny cel jego analizy. Za szczególnie reprezentatywne uchodzą tu zwłaszcza interesujące spostrzeżenia Andrzeja Adamskiego, który wskazuje na materialnoprawne ujęcie przestępstwa

[1] Zob. M. Nawrocki, *Miejsce popełnienia czynu zabronionego*, Warszawa 2016, s. 98.
[2] B. Hołyst, *Internet jako miejsce zdarzenia*, „Prokuratura i Prawo" 2009, nr 4, s. 19–20.
[3] *Ibidem*, s. 19–20.

komputerowego i formalnoprawne (procesowe) ujęcie tego przestępstwa[4]. W ujęciu materialnoprawnym – zdaniem przywołanego autora – chodzić ma z jednej strony o przestępstwa polegające na ataku sprawcy na system komputerowy, program komputerowy lub dane komputerowe, a z drugiej strony – o przestępstwa charakteryzujące się zamachem na tradycyjne dobra prawnie chronione realizowanym poprzez użycie elektronicznego systemu przetwarzania informacji[5]. W ujęciu zaś procesowym za przestępstwa komputerowe uchodzić mają te przestępstwa, których – jak ujmuje to w ślad za A. Adamskim M. Nawrocki:

> […] ściganie wymaga od organów wymiaru sprawiedliwości uzyskania dostępu do informacji przetwarzanej w systemach komputerowych lub teleinformatycznych[6].

Mając w polu widzenia uwidocznioną niejednorodność zachowań obejmowanych mianem cyberprzestępstwa, za naukowo odważne uznać przeto należy poglądy starające się respektować tę ich właściwość. Zwolennikiem takiego podejścia jest w polskiej literaturze przedmiotu w szczególności przywoływany już M. Nawrocki, który w swoich monograficznych rozważaniach na temat miejsca popełnienia czynu zabronionego przyjął, że mianem cyberprzestępstw obejmował będzie:

> […] wszelkie przejawy przestępnej działalności z użyciem komputera (lub innego podobnie działającego urządzenia) oraz Internetu bądź innej sieci, np. intranetu, które charakteryzują się m.in. działaniem na odległość (np. oddziaływaniem na inny komputer czy serwer)[7].

---

[4] A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 30 i n. Nadmieńmy, że rzeczone rozróżnienie odnotowuje także m.in. M. Nawrocki – zob. M. Nawrocki, *op. cit.*, s. 99.

[5] Zob. A. Adamski, *op. cit.*, s. 30 i n.

[6] M. Nawrocki, *op. cit.*, s. 99.

[7] *Ibidem*.

Jak widać, wskazana definicja stara się ujmować definiowane w niej zjawisko w sposób bardzo szeroki – można by wręcz rzec, że nazbyt szeroko. Mowa w niej wszak o przejawach przestępnej działalności, gdy tymczasem cyberprzestępstwem może być wyłącznie przestępstwo, bo przecież – co oczywiste – cyberprzestępstwo jest po prostu jedynie szczególnym rodzajem przestępstwa – szczególnym za sprawą prawnokarnie niedozwolonego i specyficznego sposobu zachowania się sprawcy, przyjmującego postać wywołanej fizycznym jego zachowaniem się elektronicznej ingerencji informatycznej realizowanej przy użyciu urządzenia elektronicznego zdatnego do przeprowadzenia wskazanej ingerencji.

Właśnie za sprawą owego sposobu zachowania się sprawcy – jak powiedziano: konstytutywnego dla bytu cyberprzestępstwa – swoistą cechą cyberprzestępstwa jest to, iż miejsce zachowania się jego sprawcy nie będzie – co do zasady – pokrywało się z każdym miejscem skutku tego zachowania; ten bowiem – jako w istocie umiejscowiony w przestrzeni wirtualnej – będzie znamionował się potencjałem wystąpienia w każdym miejscu, w którym znajdowało się będzie urządzenie zdatne do odbioru prawnokarnie zabronionej transmisji danych. W tym też aspekcie niewątpliwie rację ma M. Nawrocki, stwierdzając, że: „[…] problematyka cyberprzestępczości wiąże się z różnym usytuowaniem sprawcy oraz efektów jego działalności”[8].

Przechodząc tym samym do problematyki miejsca popełnienia cyberprzestępstwa, odnotować należy, że w toku prowadzonej wokół niej dyskusji ścierają się dwa charakterystyczne zapatrywania, które w literaturze przedmiotu bywają określane mianem modeli wyznaczania miejsca popełnienia przestępstwa cybernetycznego[9].

Według pierwszego z nich i – jak donosi M. Nawrocki – dominującego w państwach europejskich, miejsce to powinno być wyznaczane według zasad ogólnych, a więc podług reguł odnoszących się do każdego rodzaju przestępstwa i nakazujących przyjąć za miejsce jego popełnienia:

---

[8] *Ibidem*.

[9] Tak w szczególności: *ibidem*.

1/ miejsce rzeczywistego (zabronionego prawnokarnie) zachowania się sprawcy,
2/ miejsce zaistniałego i będącego znamieniem typu czynu zabronionego skutku tego zachowania,
3/ oraz miejsce, w którym skutek będący znamieniem typu czynu zabronionego miał według zamiaru sprawcy wystąpić.

Jak wiadomo, wskazane zasady znamionują i polski obecnie obowiązujący Kodeks karny, w którym wyartykułowano je w przepisie art. 6 § 2. Zgodnie z tym przepisem – przypomnijmy – czyn zabroniony uważa się za popełniony w miejscu, w którym sprawca działał lub zaniechał działania, do którego był obowiązany, albo gdzie skutek stanowiący znamię czynu zabronionego nastąpił lub według zamiaru sprawcy miał nastąpić[10]. Dopowiedzmy jeszcze, że przyjęty w polskim Kodeksie karnym sposób wyznaczania miejsca popełnienia czynu zabronionego określa się jako koncepcję (zasadę) wielomiejscowości[11] lub rzadziej wszędobylstwa[12], aczkolwiek wskażmy, że ostatnie z wymienionych określeń jest jaskrawo nieadekwatne[13], bo przecież w ramach owego sposobu miejsce popełnienia czynu zabronionego sytuowane jest nie gdziekolwiek, lecz przypada wyłącznie na trzy (równorzędne[14]) miejsca wyznaczone przez statuujące ten sposób i zreferowane wyżej zasady.

Z kolei według drugiego zapatrywania i – jak referuje to M. Nawrocki – funkcjonującego w systemach prawa karnego państw amerykańskich i niektórych państw azjatyckich, za miejsce przestępstwa cybernetycznego uznaje się

[10] Szerzej nt. przyjętego w polskim k.k. sposobu wyznaczania miejsc popełnienia czynu zabronionego zob. *ibidem*, s. 45 i n., a także i przede wszystkim B. Filek, *Odpowiedzialność w Polsce za czyny zabronione popełnione za granicą*, Opole 2018 (maszynopis rozprawy doktorskiej), s. 18 i n.

[11] Tak w szczególności A. Zoll, *Miejsce popełnienia czynu zabronionego*, [w:] *Kodeks karny. Część ogólna. Tom I. Komentarz do art. 1–116*, red. A. Zoll, Warszawa 2012, s. 130.

[12] Odnotujmy przy tym, że koncepcję wielomiejscowości też określa się jako koncepcję wszędobylstwa – tak w szczególności M. Nawrocki, *op. cit.*, s. XXV.

[13] O tym, iż przyjętego w polskim k.k. modelu wyznaczania miejsc popełnienia czynu zabronionego nie powinno określać się mianem koncepcji wszędobylstwa, pisano wielokrotnie – zob. w szczególności Ł. Pohl, *Prawo karne. Wykład części ogólnej*, Warszawa 2019, s. 93.

[14] Szerzej na temat problemu równowartości miejsc popełnienia czynu zabronionego w modelu polskim zob. B. Filek, *op. cit.*, s. 48 i n.

miejsce usytuowania systemu informatycznego, na który poprzez transmisję danych oddziałuje sprawca[15].

Nie próbując rozstrzygać, który model wyznaczania miejsca popełnienia przestępstwa cybernetycznego jest właściwszy, warto zwrócić uwagę, że każdy z nich ma swoje zalety. Siłą modelu tradycyjnego jest to, że bierze on pod uwagę miejsce zachowania się sprawcy – miejsce, w którym wprowadza on do obiegu informatycznego niedozwoloną prawnokarnie transmisję danych. Z kolei mocną stroną modelu „pozaeuropejskiego" jest to, że pozwala on uznać za miejsce popełnienie interesującego nas przestępstwa miejsce usytuowania systemu informatycznego, na który rzeczona transmisja oddziałuje.

Możliwość ta jest istotna choćby z tego względu, że o zdecydowanej większości przestępstw cybernetycznych twierdzi się, iż są one przestępstwami bezskutkowymi, a więc przestępstwami o formalnym charakterze, które polegają na wprowadzeniu do obiegu informatycznego niedozwolnej prawnokarnie transmisji danych. Stąd też oczywiście może zdarzyć się sytuacja – sytuacja interesująca z perspektywy objęcia jej polską jurysdykcją karną – kiedy to sprawca formalnego przestępstwa cybernetycznego działał będzie poza granicami Polski, lecz oddziaływał na system informatyczny znajdujący się w jej granicach.

Sytuacja ta jest o tyle istotna, że ujawnia ona niedomagania modelu tradycyjnego, gdyż według niego Polska nie może być uznana za miejsce popełnienia przestępstwa cybernetycznego. Tymczasem – jak się wydaje – powinno być inaczej. Wszak w podanym przykładzie to właśnie w Polsce sprawca sfinalizował niedozwoloną prawnokarnie transmisję danych, wyrządzając tym samym na jej terytorium szkodę wynikającą z wprowadzonej przezeń zmiany w elektronicznym obiegu informacji. Słowem, występujące tu miejsce pokrzywdzenia powinno być brane pod uwagę jako prawnokarnie dopuszczalna ewentualność uznania go za miejsce popełnienia formalnego przestępstwa cybernetycznego.

Taki postulat był już zresztą zgłaszany przez polską doktrynę prawa karnego. Wystąpił z nim w szczególności Michał Sowa[16], podnosząc, że:

---

[15] Zob. M. Nawrocki, *op. cit.*, s. 99.

[16] M. Sowa, *Odpowiedzialność karna sprawców przestępstw internetowych*, „Prokuratura i Prawo" 2002, nr 4, s. 75 i n.

> Przyjęcie, iż miejscem popełnienia przestępstwa jest li tylko miejsce bezpośredniego działania sprawcy, prowadzi do sytuacji, w której osoba znajdująca się poza granicami Polski mogłaby bezkarnie umieszczać na polskich serwerach treści przez polskie prawo zakazane[17],

oraz wnioskując w konsekwencji, że:

> Wydaje się więc, iż zasadnym byłoby przyjęcie za miejsce działania sprawcy zarówno miejsca, w którym się znajdował, dokonując czynu zabronionego, jak i miejsca, w którym położony jest system komputerowy, na który sprawca oddziaływał[18].

Cytowany autor zastrzegł jednakże przy tym, że podaną puentę należałoby jednak ostatecznie rozpatrywać w kategoriach postulatu *de lege ferenda*, a nie w charakterze konkluzji interpretacyjnej będącej wynikiem wykładni przepisu art. 6 § 2 k.k.[19], z czym zresztą w pełni koresponduje jego propozycja poszerzenia art. 6 k.k. o paragraf 3, w którym wskazywano by, że:

> Czyn zabroniony popełniony z użyciem bądź skierowanym przeciwko systemowi komputerowemu uważa się za popełniony w miejscu określonym w § 2, a także w miejscu, w którym znajdował się system komputerowy[20].

W pełni podzielając wskazany punkt widzenia o zasadności poszerzenia miejsc popełnienia czynu zabronionego o miejsce usytuowania systemu informatycznego będącego przestrzenią, w ramach której realizowana i ujawniania jest nielegalna prawnokarnie transmisja danych[21], nie można jednocześnie tracić z pola widzenia, że zaproponowane rozwiązanie legislacyjne nie jest wolne od słabości. Nie oddaje ono bowiem precyzyjnie leżącego u jego podstaw *ratio legis*,

---

17 *Ibidem*, s. 76.
18 *Ibidem*.
19 *Ibidem*.
20 *Ibidem*.
21 Podziela go także M. Nawrocki – zob. M. Nawrocki, *op. cit.*, s. 103.

gdyż brakuje w nim zastrzeżenia dookreślającego system informatyczny, mianowicie dookreślenia precyzującego, że ma to być nie jakikolwiek system, lecz wyłącznie ten system, w którym realizowana jest niedozwolona prawnokarnie transmisja danych i w którym ostatecznie ujawnia się obiektywnie szkodliwy skutek owej transmisji.

W charakterze uzupełnienia wspierającego pomysł poszerzenia miejsc popełnienia czynu zabronionego o miejsce usytuowania wskazanego wyżej systemu informatycznego warto jeszcze dodać, że w wielu państwach problem ten rozwiązuje się poprzez spełnienie warunku szczególnego związku danego przestępstwa cybernetycznego z terytorium tych państw. Okoliczność tę odnotowuje w polskiej literaturze przedmiotu m.in. M. Nawrocki, pisząc, że:

> W angielskim prawie karnym przestępstwa polegające na naruszeniu integralności systemów komputerowych mogą być popełnione także przez sprawców niebędących obywatelami Wielkiej Brytanii, jak i poza terytorium tego państwa. Jurysdykcja tamtejszych organów ścigania i organów wymiaru sprawiedliwości będzie istniała o tyle, o ile popełniony czyn będzie pozostawał w „szczególnym związku" z terytorium Anglii, Walii, Szkocji czy Irlandii Północnej. Anglosaska doktryna i judykatura przyjmuje, że „szczególny związek" zachodzi wówczas, gdy w momencie popełnienia czynu sprawca znajdował się w swoim ojczystym państwie i podejmował próby uzyskania nieuprawnionego dostępu lub uzyskał nieuprawniony dostęp do jakiegokolwiek komputera zawierającego jakikolwiek program lub dane[22].

Oczywiście, postulat poszerzenia miejsc popełnienia czynu zabronionego o wskazane wyżej miejsce określonego systemu informatycznego nie miałby podstaw w razie swoistej intelektualnej redefinicji większości przestępstw cybernetycznych – redefinicji przekształcającej ich strukturę dogmatyczną z formalnej na materialną. Propozycja zmiany postrzegania wskazanych przestępstw (obecnie wszak powszechnie uznawanych za typy formalne) wydaje się zresztą częściowo uzasadniona, bowiem w przypadku owych przestępstw

[22] *Ibidem*, s. 102.

da się oddzielić zachowanie się sprawcy, polegające na wprowadzaniu do obiegu informatycznego zabronionej prawnokarnie transmisji danych, od jej efektu w postaci ujawnienia w tym obiegu finalnego kształtu tej transmisji. Uznanie owego efektu za skutek rzeczonych przestępstw nadawałoby im status typów materialnych, a status ten – co oczywiste – odbierałby uzasadnienia na rzecz poszerzenia miejsc popełnienia czynu zabronionego o miejsce systemu informatycznego będącego obiektem prawnokarnie nielegalnej transmisji danych i jej obiektywnie szkodliwego efektu. Wówczas bowiem postulowane miejsce zaatakowanego zachowaniem się sprawcy systemu informatycznego byłoby jednocześnie miejscem rzeczywiście zaistniałego skutku, a więc miejscem uznawanym przez obecnie obowiązujący polski Kodeks karny za miejsce popełnienia czynu zabronionego.

Bibliografia

Adamski A., *Prawo karne komputerowe*, Warszawa 2000.

Filek B., *Odpowiedzialność w Polsce za czyny zabronione popełnione za granicą*, Opole 2018 (maszynopis rozprawy doktorskiej).

Hołyst B., *Internet jako miejsce zdarzenia*, „Prokuratura i Prawo" 2009, nr 4.

Nawrocki M., *Miejsce popełnienia czynu zabronionego*, Warszawa 2016.

Pohl Ł., *Prawo karne. Wykład części ogólnej*, Warszawa 2019.

Sowa M., *Odpowiedzialność karna sprawców przestępstw internetowych*, „Prokuratura i Prawo" 2002, nr 4.

Zoll A., *Miejsce popełnienia czynu zabronionego*, [w:] *Kodeks karny. Część ogólna. Tom I. Komentarz do art. 1–116*, red. A. Zoll, Warszawa 2012.

Szymon Pawelec

Criminal procedure grounds for gaining access to the content of electronic communication

At the beginning of the third decade of the 21st century, it is a truism to state the rather obvious fact that nowadays electronic correspondence is one of the principal channels of communication. As opposed to the early forms of this type of human contact, dating back to the 1960s, the present form of exchange of information among people does not only consist in a direct transfer of the traditional written correspondence into the digital world. Depending on the needs, modern electronic correspondence is quite often a written utterance which, to a smaller or bigger extent, is accompanied by various other forms of expression. It is enough to point out that a traditional e-mail that we send or receive most frequently contains some form of attachment. Such attachments range from simple text files, to increasingly popular audio recordings replacing written word, large graphic or audiovisual files, or so undesired (and often unintended by neither the sender nor the receiver) additions that hide malicious code.

Irrespective of the versatility of the very form of communication that includes e-mails and the related forms of information exchange, worth mentioning is the ease with which such information can be sent. Thinking back not necessarily to the distant beginnings of electronic correspondence, with its military and academic history, including for instance the times of ARPANET – the predecessor of the modern Internet, but just to the early 2000s, we can see that for a rather long time electronic communication required desktop computers plugged into wired (usually telephone) networks, which were used to connect to the Internet. At present, a considerable number of people use electronic mail

on mobile devices, principally smartphones[1], which have wireless access to the Internet. This means that access to electronic mail is practically unrestricted (provided the WiFi coverage is sufficient) and possible from any place, and no access to a cable Internet network or a desktop computer is required. It is worth remembering that by sending an e-mail, we not only transfer a specific message, but also lots of metadata, including, for instance, the IP address.

Of course, using electronic mail by means of a smartphone is just one of the possibilities of electronic communication. Because of a significantly lower level of uncertainty as to the identification of the appropriate regime of criminal procedure protection in comparison with other forms of electronic communication, this article ignores the fundamental form of remote communication – a live telephone call, made as part of a default service provided by a phone operator or using VoIP[2]. At the same time, in the modern world, electronic communication is not divided into live (by default – voice, but increasingly – fully audiovisual) communication and written communication, conducted with the use of a more or less sophisticated interface of an electronic mail client. That is mainly because e-mail services are supplemented with various more or less simple forms of remote correspondence, selected mainly based on the ease of use on mobile devices and their multimedia functionalities. When analysing them, one should consider both the simplest service of exchange of short text messages – provided since the moment when the first mobile telephony networks were set up, over time – when the networks became more advanced – complemented with systems for sending multimedia files[3], and communication by means of one

[1] On a historical note, with reference to a very dynamic development of IT technology, it is worth mentioning that 1999 saw the launch of WAP, i.e. a simplified protocol for wireless applications, which opened the Internet for mobile phones. A little earlier, in 1996, one of the first mobile phones providing access to electronic mail (including the Nokia 9000 Communicator, today regarded as a breakthrough product) were made available on the general market.

[2] More broadly on criminal procedural aspects of access to conversations in the form of VoIP cf. A. Kiedrowicz, *Zagadnienie kontroli przekazów informacji w ramach telefonii internetowej* [*Surveillance of information transmission in VoIP*], "Prokuratura i Prawo" 2008, no. 10, p. 125–134.

[3] This is a reference to popular SMSs (Short Message Service) and introduced – along with the expansion of the UMTS technology – multimedia messages, i.e. MMSs (Multimedia Messaging Service).

of several leading instant messengers, which enable a fully comprehensive set of forms of communication[4].

Thus, there is no doubt that e-mail correspondence and any related forms of electronic communication may constitute a very important source of evidence in criminal cases. It is worth stressing that it is not about such extreme and generally rather unrealistic situations in which an e-mail correspondence participant would directly admit to commission of a serious crime. Reconstruction of an e-mail exchange provides, above all else, a rich source of indirect evidence, which enables judicial bodies to build chains of clues and eliminate versions of the events presented *post factum* by the accused and their defence. Access to the professional correspondence of a person is also, as a rule, an excellent source of material that enables reconstruction of the features of the subjective side, i.e. the key elements where it is necessary to separate principally unpunishable inadvertence from deliberateness, with an intent at least possible. It is enough to mention one of the simplest examples from trial practice in economic criminal cases: acquisition and analysis of e-mail correspondence of a person suspected in the case of numerous types of managerial crimes often constitutes one of the key pieces of evidence, which determines the further course of the proceedings and the change of the person's status to a formal suspect. This is because a record of e-mail messages sent and received by the suspected person may determine how investigative agencies, and later on – the court, will perceive the subjective side of the behaviour of a given person at the time of the act, in particular whether the person knew or may have surmised a particular factor

[4] Within the context of the further discussion, it is worth pointing out that the doctrine of criminal procedure signals the view that chat messages should be regarded as a type separate from that of e-mail messages and more akin to an ordinary telephone call rather than e-mail correspondence, and that, consequently, a different regime of criminal procedural protection should be applied to chat correspondence from that in the case of e-mail correspondence – cf. P. Hofmański, E. Sadzik, K. Zgryzek, *Kodeks postępowania karnego. Komentarz do art. 1–296* [*The Code of Criminal Procedure. Comments to Art. 1296*]. *Volume I, 2011*, electr. pub. Legalis, comments on Art. 218 CCP. Of course, it should be remembered that the view was expressed a number of years ago, but nevertheless the author of this article does not share it. That is mainly because modern e-mail services may be used in a way very similar to old chat messages – especially in corporate contact practice in many entities, where e-mail programs are used even for very short correspondence, and communication takes place practically on an ongoing basis, being shared on a same server.

(an economic event, a violation by a company official, a risk factor, etc.). As a formality, it should be pointed out that even where the meaning of the acquired e-mail correspondence is unambiguous, principally, it may not be regarded as the only, isolated proof of the circumstances mentioned in it. Considering that an e-mail exchange takes place between at least two people (though some conversations may have as many as tens of participants), who are witnesses – or possibly a witness and an accused, or two accused – i.e. people who may or even should be interrogated as part of the proceedings to take evidence, in accordance with the appropriate regime for officially recording such an act. In such a situation, the protective regulation of Art. 174 of the Code of Criminal Procedure (CCP) should be applied, under which evidence by explanations given by the accused or evidence provided by witnesses may not be replaced with the content of documents, notes or official memos. Of course, following the general guidelines arising from Art. 7 CCP, the authority conducting proceedings may lend credence to evidence resulting from the acquired content of an e-mail message originating from or addressed to a witness or an accused, and to refuse to give credence to evidence or explanations provided directly in the course of the proceedings as to the circumstances mentioned in the e-mail. However, the act of direct interrogation should not be omitted.

A very important aspect, which however falls entirely outside the scope of this article, is the decisive determination of the fact of the authenticity of a given e-mail message and the establishment of an evidence-proof link between a specific individual and a party to e-mail correspondence. The first case regards situations in which there is an attempt to fabricate evidence – either by means of traditional printing techniques or by directly tampering with the electronic record[5]. The other case is about establishing whether the person indicated as the user of a given e-mail address or another electronic communication identifier[6]

[5] More broadly about examples of this kind, even unintentional manipulations, cf. Sz. Pawelec, B. Trętowski, *Strona internetowa jako źródło dowodowe* [*A website as a source of evidence*], "Przegląd Prawa Handlowego" 2011, no. 7, p. 42–43.

[6] In the case of instant messengers, the most common identifier of this type is the mobile phone number or a profile created in the app of a given communication service provider, or, more broadly, a social networking service.

was indeed that party to the correspondence in question, whether they had just made their access data (or a device with their access data already entered) available to another person, or whether those data were illegally intercepted with a view to personating such party.

The above pointed out that electronic communication is used universally and so it is significant from the perspective of potential evidence. However, this article is trying to find an answer to the question about the choice of the appropriate criminal procedure regime for accessing such sources by judicial authorities. Interestingly enough, despite the obvious, considerable importance of the selection of the appropriate legal basis for trial-related access to such information, because of the difficult-to-interpret solutions provided for in CCP, the doctrine has failed to work out a uniform position on this issue. Even if a particular line of interpretation is assumed, it is hard not to come up with a number of critical remarks and suggestions for future legislation. The essence of the problem is whether access to electronic communication should be regulated by the provisions of Chapter 25 (Seizure of objects, searches) or Chapter 26 (Surveillance and recording of conversations) CCP. To some extent, the relation between these two Chapters can be perceived as: general regulation (Chapter 25) vs. specific regulation (Chapter 26); however, with peculiar features of the latter, which makes it somehow separated from the general normalisations of the institution of evidence search, set out in Chapter 25. Chapter 25 CCP lays down the general principles of acquisition for trial purposes of, above all, material evidence (though also items subject to seizure with a view to securing financial penalties, financial punitive measures, forfeiture, compensatory measures or indemnification claims, or to finding, detaining or bringing about compulsory appearance of a suspected person) for purposes related to a proceeding.

In turn, Chapter 26 sets out the rules for surveillance and recording of telephone calls with a view to detecting and obtaining evidence for a proceeding in progress or to preventing commission of another crime. What is important is that in both of the Chapters referred to above the legislator explicitly refers to electronic communication with an additional detailed normative regulation, which expands the scope of regulation of a given Chapter to cover those relatively new sources of evidence. In Chapter 25 CCP, it is Art. 218a, which sets out

the obligations of offices, institutions and entities engaged in telecommunication activities, as well as Art. 236a, which specifies the obligations of beneficial owners and users of IT systems or equipment containing IT data, regarding data kept on such equipment or systems or on carriers in possession of such parties, including correspondence sent by electronic mail. In Chapter 26 CCP, the traditional tapping related to a proceeding in progress is extended to means of electronic communication by Art. 241, which provides that the Chapter is applicable respectively to surveillance and recording by technical means of the content of other conversations or information transmissions, including correspondence sent by electronic mail. Thus, it is rather clear that because both of these Chapters deal with the access by criminal procedure authorities to the content of electronic communication of witnesses or the accused, two rather different formal regimes of such actions will compete with one another.

Allowing for certain distinct qualitative disparities between the institutions under Chapters 25 and 26 CCP, the difference in the level of protection of the individual's rights between the two is evident. A decision authorising the use of tapping related to a proceeding in progress is made incomparably more seldom than that about the existence of grounds for seizing objects and conducting searches, both from the perspective of subjective and objective elements. The decision on tapping related to a proceeding in progress may only be made by a court (an exceptional, prosecutorial decision is strictly limited in time and needs to be approved by a court in accordance with Art. 237 § 2 CCP). Despite the constantly expanded (*vide* Art. 237 § 3(12a) and (16a)(16g) CCP) list of crimes that allow for the use of tapping related to a proceeding in progress, the grounds for using the measure are still limited to serious prohibited acts[7].

[7] This general remark, however, should be accompanied by a comment, particularly with reference to economic crime. Considering such broad objective grounds for the admissibility of tapping related to a proceeding in progress as, for instance, Art. 237 § 3(15) CCP (i.e. the threshold of just PLN 200,000, which corresponds to the lower punishability threshold of the basic economic crime provided for in Art. 296 § 1 CCP), or Art. 237 § 3(12a) CCP (where it is sufficient to suspect forgery or alteration of an invoice or use of such a document, irrespective of the amount by which the public law payable has been depleted or threatened to be depleted), in the case of economic crimes it is exceptionally easy to demonstrate grounds for using such an invasive measure as tapping related to a proceeding in progress.

On the other hand, the grounds for seizure of objects and searches are based on a vague prerequisite which principally focuses on a category of things that may constitute evidence in a case or be subject to seizure. Although this may seem obvious, a very important qualitative difference between the two groups of institutions is the fact that, by its nature, tapping is only limited to activities in progress. In combination with the restrictive time limits for its use (*vide* Art. 238 §§ 1 and 2 CCP), it is guaranteed to finish within a specific time, and it is not possible to reach into the past as far as one might want to. Seizure of objects and searches, however, may regard carriers with data containing communication from any period of time – for instance, an e-mail saved on a server that was sent over ten years ago. The only structurally more advantageous aspect – in terms of the respect of the addressee's privacy – is the fact that, by its nature, a search is not a secret action. This circumstance results directly from the Code regulation, which not only confirms that the person on whose premises the search is being conducted should be aware of it, but also creates a number of related guarantees. The guarantees include, for instance, the rules of participation in the activity of not only the person on whose premises the search is to be conducted, but also of another designated person (Art. 224 CCP), or the making of an accurate, official record of the activity (Art. 229 CCP). It is aptly pointed out, when referring to the issue of a so-called 'remote search', that the nature of the institution of a search dealt with in Chapter 25 CCP prevents its conduct in a secret manner, as this would turn it into the institution of tapping[8]. Although the secret nature of tapping is not defined anywhere in Chapter 26, the very nature of the institution confirms this characteristic, supported indirectly by solutions such as the ability to adjourn the announcement of the court consent to conduct the activity, provided for in Art. 239 §1 CCP.

Considering the above, the following fundamental question arises: if the judicial authorities (i.e. the investigative agencies, which act inquisitionally the most often during preparatory proceedings) desire to gain access to the content of electronic communication of a given person in the form of their

[8] Cf. A. Lach, *Przeszukanie na odległość systemu informatycznego* [*A remote search of an information system*], "Prokuratura i Prawo" 2011, no. 9, p. 74.

e-mail messages sent or received from a given e-mail address or to messages sent via a specific instant messenger, may the grounds for this be a very easily obtainable order to conduct a search and to issue a demand to surrender objects, or should the special regime under Art. 237 CCP, in connection with Art. 241 CCP, that calls for a court order, be applicable?

What is rather surprising is that despite such a big importance of the issue, the doctrine has failed to develop a uniform position on it. Furthermore, the presented justifications for the selection of the first or the other cause of action are based on arguments of a very different nature, sometimes detached from the real significance of the differentiation. In the science of criminal proceedings, there is a clearly identifiable view that whether access to electronic correspondence of a given person should be regulated by the provisions of Chapter 25 or Chapter 26 CCP is dependent on the moment at which such correspondence is to be obtained. Thus, in the opinion of A. Lach, the only solution that prevents a positive conflict of the regulations is to accept that the provisions of Chapter 26 CCP – via its Art. 241 – should be applied to correspondence sent electronically at a given moment (i.e. during the transmission), while the provisions of Chapter 25 CCP regard correspondence before or after the transmission[9]. In the light of the above, it should be accepted that where electronic mail messages have been stored by a given person locally, on a disk of their own computer, Art. 217 CCP (or, consistently, Art. 219 CCP), in connection with Art. 236a CCP, is applicable. Where such messages are stored on a server of an entity carrying on telecommunication activity (and a given party sends and receives them, for instance, using an Internet browser as an e-mail client), it is appropriate to apply the special regulation of Art. 218 § 1 CCP, in connection with Art. 236a CCP. Where, however, electronic correspondence is to be surveilled and recorded during its transmission, it is necessary to apply

[9] Cf. A. Lach, *Dowody elektroniczne w procesie karnym* [*Electronic evidence in criminal proceedings*], Toruń 2004, p. 109; *idem*, *Karnoprocesowe instrumenty zwalczania pedofilii i pornografii dziecięcej w Internecie* [*Instruments of criminal procedure for preventing paedophilia and child pornography on the Internet*], "Prokuratura i Prawo" 2005, no. 10, p. 55. Similarly M. Rusinek, *Tajemnica zawodowa i jej ochrona w polskim procesie karnym* [*Professional secrecy and its protection under Polish criminal law*], Warszawa 2007, p. 212.

Art. 237 § 1 CCP, in connection with Art. 241 CCP. This view is expressed in commentaries by R.A. Stefański and S. Zabłocki[10], as well as J. Skorupka[11] and P. Hofmański, E. Sadzik and K. Zgryzek. The latter authors, just like A. Lach, point out that because of the presence of references to electronic correspondence either in Chapter 25 or Chapter 26 CCP, the existing system inconsistency may be eliminated by assuming that as regards an already existing and stored record of e-mail messages, the provisions concerning the handing over of correspondence and consignments should be applied, whereas "if a transmission of an electronic mail message is to be 'intercepted' live, as it were, the provisions on telephone tapping are applicable"[12].

Initially, this position seems logical and indeed enables a positive regulation conflict to be avoided. However, the problem is that considering the nature of electronic communication and the practical implications of such an approach, some of its aspects are hard to accept. If electronic communication in the form of e-mail messages occurred in the manner that a message sent from the sender's e-mail program were travelling via a network to the addressee's e-mail program for a noticeable period of time, and, furthermore, that such correspondence were stored on electronic devices at the exclusive disposal of the sender and the recipient, then the distinction might be regarded as real. The period during which a message might be 'intercepted' would indeed be observable and the very correspondence participant, by storing the historical communication on their computer, would decide whether they accept the risk that someone may gain access to it by taking the computer from them. In every case, they would be aware, because of a conducted non-secret search, that such an activity was performed. However, the situation seems entirely different in the case of modern electronic communication. Firstly, the 'travelling time' of an e-mail in the network is extremely short – in some situations, which is dependent on a number

[10] R.A. Stefański, S. Zabłocki, *Kodeks postępowania karnego. Tom II. Komentarz do art. 167–296* [*The Code of Criminal Procedure. Volume II. Comments to Art. 167–296*], electr. pub. Lex, comments to Art. 237a.

[11] J. Skorupka (ed.), *Kodeks postępowania karnego. Komentarz 2020* [*The Code of Criminal Procedure. Comments 2020*], ed. 33, electr. pub. Legalis, comments to Art. 241 CCP.

[12] P. Hofmański, E. Sadzik, K. Zgryzek, *op. cit.*, comments to Art. 218 CCP.

of technical aspects (such as the message size, network traffic, the locations of the sending and receiving servers), it is practically imperceptible. Secondly, even where a message has been sent, received and subsequently deleted, the deletion may be reversed, at least for a specified period of time, by the operator of a given mail system. Suffice it to say, a routine service offered by at least some of the global electronic mail system providers is the recovery of 'permanently' deleted e-mail messages from at least the last 25–30 days[13]. Thirdly and lastly, gaining access to another person's correspondence by applying the regulations on seizure of objects and searches may take place entirely without the knowledge of the person concerned. It is not necessary to conduct a search and seize the person's computer; access may be enabled by the electronic mail service provider.

What very often differentiates the gaining of access to another person's e-mail box on the service provider's server from the traditional handing over of correspondence and consignments is the fact that such an action usually involves not only the handing over of current correspondence (similarly to traditional correspondence, one might regard it as the handing over of correspondence and consignments in accordance with Art. 218 § 1 CCP). Nowadays, an overwhelming majority of e-mail users does not download e-mail messages from the e-mail server to their local electronic device permanently, at the same time deleting them from the virtual space (server), but rather connects via their device with the e-mail server on which they are stored. This solution is gaining popularity and by many people is regarded – in normal circumstances – as more stable (messages are not lost if their device is lost or breaks down), but also as much more universal and mobile (it enables access to the collection of their e-mail correspondence from various devices, including a computer or a smartphone). Thus, from the perspective of the rights of the individual – and more practically, an ordinary citizen, who does not use electronic mail with a view to committing crimes, but simply would not want all of their e-mails to be easily accessible to and viewed by prosecution agencies – the biggest and a real nuisance is the ease of access to e-mails already stored on the e-mail server, and not only to those 'on

[13] Cf., for instance, the information available here: https://support.google.com/a/answer/112445?hl=pl or https://support.apple.com/pl-pl/guide/iphone/iphb02be90ba/ios [access: 4.02.2021].

the move'. By accepting, without any additional reservations, the admissibility of the application of the provisions of Chapter 25 CCP to the accessing of e-mail correspondence, we agree to a situation in which under an issued order, based on a very vague indication that, for instance, the correspondence of a given person during the last five years may contain evidence pertinent to the case, thousands of pieces of information, letters, photos, video recordings relating to all areas of professional, family or private life of a person may be obtained, even without that person's knowledge. The order will be issued to the company that owns the electronic mail servers and it will be forced to hand over the required data. Consequently, from the perspective of the incursion into an individual's privacy, the severity of the use of the regime under Chapter 25 CCP instead of Chapter 26 is enormous. Even ignoring the issue of the limitations resulting exclusively from the judicial nature of the tapping decision only in cases regarding specific crimes, of extreme importance is the differentiation, already referred to above, that under Art. 238 CCP, in connection with Art. 241 CCP, access to electronic correspondence by tapping related to a proceeding in progress may only cover a specified period of time, up to three months, which only in particularly well justified cases may extend to another three months. Under the regime of Chapter 25, it is possible to obtain a person's correspondence from any period of time, thus exploring their past practically without any time limits. Considering the above, it is striking that there is no convincing axiological justification for providing a so much higher protective regime for electronic correspondence 'on the move' than for electronic correspondence stored on the e-mail server of a given person.

In the light of the above, appreciation and support is due in the case of the views in the doctrine that seek to link the admissibility of the application of the provisions of Chapter 25 instead of those of Chapter 26 CCP to e-mail correspondence to criteria other than the very differentiation whether we have managed to capture a message during the second (or its small part) in which it was 'on the move' or not. The author of this article is very interested in the synthetic argument put forward by A. Lach during his analysis of the institution of a remote search that access to e-mail messages may be gained under

the provisions of Chapter 25 CCP if it does not take place in a secret manner[14]. From the point of view of an individual, however, such a solution also does not amount to openness, which characterises a standard search. The context of the author's utterance indicates that, as regards a search of data stored on a server and not locally on a computer of a given person, the openness of such an action would apply to the party that owns the e-mail server available to individual e-mail account users, and not to the users themselves. The search would not cover the electronic equipment of such users, but only the e-mail server of a given provider. It is worth pointing out that if Art. 218 § 2 CCP, which provides for the obligation to deliver an order to seize and surveil correspondence also to the correspondence addressees, is to be used, the said article enables the information that the search was conducted to be withheld for a certain period of time, similarly to Art. 239 CCP.

A definitely more far-reaching and more serious differentiation of the admissibility of the application to electronic communication of the provisions of Chapter 25 CCP instead of the provisions on tapping related to a proceeding in progress is related to the views that bind the possibility of using the provisions regarding seizure of objects and searches in relation of electronic communication only with certain elements of such correspondence, principally not covering its content. An interesting approach to this issue, expressed in the context of access to data stored in a virtual cloud, has been presented by J. Kudła and A. Stasiak, by referring to the starting IT distinctions. Based on the division, which in the authors' opinion is important in terms of the obligations under Art. 218 CCP, into an electronic mail service and an electronic mail provision service, the authors came to the conclusion that because e-mail services encompass such elements as "making an individual e-mail account available, providing the ability to receive electronic mail sent to the account, storing of electronic mail, and – in our opinion – also the determining of the IP address, in this case it is sufficient to apply Art. 218 § 1 CCP". A separate scope of so-called 'data' is constituted by an electronic mail transmission service (below: 'the transmission service'), when the content of verbal communications (or visual

[14] Cf. A. Lach, *Przeszukanie…*, p. 74.

or audio records) is transmitted. In such a situation, it is imperative to submit to the court a motion for surveillance and recording of conversations in accordance with Art. 237 § 1–2 CCP"[15]. The authors' view is also referred to by R.A. Stefański and S. Zabłocki[16]. The discussion on the subject should certainly be intensified and the views on this qualitative differentiation of the regime of access to electronic communication, i.e. to some of its identifying elements in accordance with the provisions of Chapter 25 CCP and its content in accordance with the provisions of Chapter 26 CCP, should be exchanged more often. Although this construction is supported by the author of this article, from the *de lege lata* perspective it significantly narrows down the scope of application of the provisions of Art. 218 CCP, in connection with Art. 236a, which can be identified on the basis of linguistic interpretation. In this situation, in order to promote this type of distinction between trial-related grounds for access to e-mail correspondence, an appropriate adjustment could be made by additional, fine tuning statements in Art. 236a CCP and, similarly, in Art. 218a CCP, indicating that such activities may not regard the content (simply put, which calls for a definition, of electronic correspondence), because with regard to surveillance of such content, the provisions of Chapter 26 CCP should apply accordingly.

It should be remembered that such a postulate, which has just been signalled here, should be backed up with appropriate, in-depth system analyses, which should, of course, seek to ensure the required standard of protection of the fundamental rights and liberties, including the right to privacy, not to mention other legal goods, such as business secrecy[17]. At the same time, the standard should not paralyse the operation of investigative agencies, preventing them from effectively combating serious crime, in particular cybercrime, which constitutes a new and increasingly serious source of danger. It should also not promote any behaviours on the part of the prosecution agencies that

[15] Cf. J. Kudła, A. Stasiak, *Procesowa i operacyjna kontrola korespondencji przechowywanej w tzw. chmurze* [*Trial and operational surveillance of correspondence stored in the so-called cloud*], "Prokuratura i Prawo" 2017, no. 7–8, p. 37.

[16] Cf. R.A. Stefański, S. Zabłocki, *op. cit.*, comments to Art. 237a.

[17] Cf. Sz. Pawelec, *Ochrona tajemnicy przedsiębiorstwa w prawie karnym materialnym i procesowym* [*Protection of business secrecy in criminal law and procedure*], Warszawa 2015, p. 301–309.

are particularly undesirable from the perspective of the rule of law standards, i.e. any violation or perversion of excessively restrictive evidence prohibitions formulated by the legislator, because of their own beliefs in the need to act for a higher good, i.e. fighting crime. Irrespective of the above, an obvious requirement when new, more precise legislative regulations are promoted in the field, is to ensure that they are used consistently throughout the legal system, and not only in the isolated area of the provisions of the Code of Criminal Procedure. In the light of all of the above remarks on modern conditions of use of electronic correspondence, one should firmly oppose the functioning in legal relations – especially at the level of the Code of Criminal Procedure, which is a fundamental legal act for criminal proceedings – of constructions that enable excessive discretion as regards the choice between two extreme regimes of access to the content of our principal forms of communication, i.e. electronic correspondence. Similarly, there should be no situations in which the distinction between the protective regimes would only be linked to the hard-to-determine technical aspect of whether a given electronic message is still being transmitted or it has already reached the recipient's server.

Bibliography

Hofmański P., Sadzik E., Zgryzek K., *Kodeks postępowania karnego. Komentarz do art. 1–296* [*The Code of Criminal Procedure. Comments to Art. 1296*]. *Volume I, 2011*, electr. pub. Legalis.

Kiedrowicz A., *Zagadnienie kontroli przekazów informacji w ramach telefonii internetowej* [Surveillance of information transmission in VoIP], "Prokuratura i Prawo" 2008, no. 10.

Kudła J., Stasiak A., *Procesowa i operacyjna kontrola korespondencji przechowywanej w tzw. chmurze* [*Trial and operational surveillance of correspondence stored in the so-called cloud*], "Prokuratura i Prawo" 2017, no. 7–8.

Lach A., *Dowody elektroniczne w procesie karnym* [*Electronic evidence in criminal proceedings*], Toruń 2004.

Lach A., *Karnoprocesowe instrumenty zwalczania pedofilii i pornografii dziecięcej w Internecie* [*Instruments of criminal procedure for preventing paedophilia and child pornography on the Internet*], "Prokuratura i Prawo" 2005, no. 10.

Lach A., *Przeszukanie na odległość systemu informatycznego* [*A remote search of an information system*], "Prokuratura i Prawo" 2011, no. 9.

Pawelec Sz., *Ochrona tajemnicy przedsiębiorstwa w prawie karnym materialnym i procesowym* [*Protection of business secrecy in criminal law and procedure*], Warszawa 2015.

Pawelec Sz., Trętowski B., *Strona internetowa jako źródło dowodowe* [*A website as a source of evidence*], "Przegląd Prawa Handlowego" 2011, no. 7.

Rusinek M., *Tajemnica zawodowa i jej ochrona w polskim procesie karnym* [*Professional secrecy and its protection under Polish criminal law*], Warszawa 2007.

Skorupka J. (ed.), *Kodeks postępowania karnego. Komentarz 2020* [*The Code of Criminal Procedure. Comments 2020*], ed. 33, electr. Pub. Legalis.

Stefański R.A., Zabłocki S., *Kodeks postępowania karnego. Tom II. Komentarz do art. 167–296* [*The Code of Criminal Procedure. Volume II. Comments to Art. 167–296*], electr. Pub. Lex.

Łukasz Wojcieszak

Phishing – charakterystyka problemu i zapobieganie jego przyczynom w aspekcie zagrożenia wirusem COVID-19

1. Wprowadzenie

Wśród oszustw, które popełniane są w cyberprzestrzeni szczególnie częste oraz niebezpieczne dla osób w niej działających są przestępstwa określane mianem „phishing". Są one zarazem stosunkowo trudne do ścigania, co jest wynikiem zmian stale zachodzących w *modus operandi* sprawców tego rodzaju przestępstw. Wzrost zagrożenia phishingiem wypływa z dynamicznego rozwoju różnorodnych (w tym bankowych) usług dostępnych w cyberprzestrzeni. Wraz z licznymi korzystnymi aspektami wnikającymi ze zwiększenia możliwości, jakie daje dostęp do Internetu, warto skoncentrować się na szczególnie groźnym zjawisku, które się z tym wiąże, a takim niewątpliwie jest phishing.

Chociaż problem phishingu istnieje od dziesięcioleci, okres restrykcji związanych z walką z wirusem COVID-19, w szczególności konieczność realizacji wielu obszarów aktywności w miejscu zamieszkania, pogorszył istniejącą sytuację. W nawiązaniu do powyższych uwarunkować należy postawić tezę, że kryzys wywołany zwalczaniem wirusa COVID-19 przyczynił się do zwiększenia zagrożenia phishingiem. Celem opracowania jest nie tylko ukazanie specyfiki phishingu, ale także jego rodzajów oraz sposobów zwalczania. Warto także postawić pytania o ewolucję sposobów działania sprawców tego rodzaju przestępstw oraz metod zwalczania phishingu, także w świetle możliwych przyszłych modyfikacji *modus operandi* sprawców tego rodzaju czynów.

W opracowaniu wykorzystano kilka metod badawczych: metodę analizy prawnej wybranych przepisów kodeksu karnego, metodę prognostyczną, a także elementy analizy porównawczej. Autor zastosował również podejście prakseologiczne przy analizie najskuteczniejszych sposobów zwalczania phishingu.

2. Definicja i rodzaje phishingu

Jak wskazuje Daniel Lubowiecki, termin „phishing" powstał w połowie lat 90. XX w., natomiast po raz pierwszy posłużono się nim na łamach magazynu „2600". Phishing zwykle tłumaczy się, jako *password harvesting fishing* (łowienie haseł), a spotkać można się też z opinią, że powstało ono poprzez połączenie słów *fishing* (rybołówstwo) oraz *phreaking* (łamanie zabezpieczeń komputerowych). Ten rodzaj oszustwa polega na podszywaniu się przez sprawcę pod inną osobę lub organizację w celu wyłudzenia określonych poufnych informacji (często bankowych) lub nakłonienia ofiary do realizacji pewnych działań za sprawą przesyłanych do nich nieprawdziwych informacji zawartych w e-mailach i SMS-ach. Phishing, nazywany jest niekiedy „nową kategorią cyberprzestępczości XXI wieku", choć atak phishingowy na dużą skalę odnotowano już w 1995 r.[1]

Ze względu na to, że sprawcy chcą za każdym razem dowieść swojej wiarygodności podczas tworzenia fałszywych stron internetowych banków lub też innych organizacji, stale aktualizują szablony, szaty graficzne, sposób funkcjonowania stron, aby rozwiać jakiekolwiek wątpliwości logującego się użytkownika co do ich autentyczności. Sprawcy mogą również rozsyłać za pośrednictwem komunikatorów oprogramowanie szpiegowskie lub *keyloggery*, które na bieżąco wychwytują i przesyłają do użytkowników końcowych wszystkie informacje, jakie zapisywane są na danym komputerze. Narażone na kradzież mogą więc być dane osobowe, treści komunikatów do innych użytkowników lub też inne dane, które są zapisywane na komputerze[2]. Pozyskane dane mogą być w szczególności sprzedawane sprawcom wyłudzeń należącym do przestępczości zorganizowanej. Rozwojowi phishingu sprzyja przede wszystkim nieostrożność, łatwowierność i naiwność użytkowników Internetu. Sprawcy tego rodzaju przestępstw wykorzystują w szczególności techniki manipulacyjne należące do inżynierii społecznej[3].

---

[1] D. Lubowiecki, *Prawno-kryminalistyczna problematyka phishingu, ze szczególnym uwzględnieniem środowiska bankowości internetowe*, „Kwartalnik Prawo-Społeczeństwo-Ekonomia" 2017, nr 1, s. 30.

[2] A. Rogowski, *Phishing*, „Kwartalnik Policyjny" 2017, nr 4, http://kwartalnik.csp.edu.pl/kp/archiwum-1/2017/nr-42017/3723,Phishing.html (dostęp: 12.11.2021 r.).

[3] D. Lubowiecki, *op. cit.*, s. 31. Wykorzystując lęk społeczeństwa spowodowany atakami na World Trade Center w dniu 11 września 2001 r., zgłosili się do jego klientów z żądaniem

Rodzajem phishingu jest *likejacking*, polegający na gromadzeniu fanów poprzez automatyczne „polubienie" danego profilu lub strony na Facebooku. Użytkownik jest wabiony atrakcyjną treścią umieszczoną na wallu swojego znajomego (najczęściej o treści erotycznej), jednak link nie umożliwia uzyskania dostępu do obiecywanej zawartości. Kliknięcie w ten wpis powoduje przeniesienie do strony, która automatyczne zaznacza „polubienie" jej przez daną osobę bez jej wiedzy oraz umieszczenie tej informacji na jej profilu. Dzięki temu spam tego rodzaju szybko rozprzestrzenia się wśród kolejnych osób. Warto zaznaczyć, że zazwyczaj na docelowej stronie znajduje się również szkodliwe oprogramowanie, które dodatkowo narażają użytkownika na niebezpieczeństwa[4]. Należy też wspomnieć o *pharmingu*, polegającym na takim zmanipulowaniu „pytań kierunek", zgłaszanych przez komputer, w celu odnalezienia danej strony internetowej, które powoduje dyskretne przekierowanie do fałszywej witryny stworzonej przez sprawcę. Można to osiągnąć w dwojaki sposób – przez ingerencję w pamięć podręczną DNS7 komputera lokalnego lub ingerencję w pamięć adresów DNS na serwerze[5]. Istnieje także tzw. phishing dynamitowy, polegający na wybieraniu konkretnych rozmów, które zawierają linki do dokumentów i e-maile. Chociaż treść wiadomości e-mail, a nawet tekst łącza są w większości ignorowane przez wirusa, to samo łącze jest zastępowane i prowadzi do zainfekowanego dokumentu[6].

---

niezwłocznego potwierdzenia swoich danych personalnych, co argumentowali koniecznością ochrony gospodarki państwa w związku z możliwą wojną na terenie USA. W tym przypadku wiele osób wpadło w zastawioną pułapkę (*ibidem*). Podobnym zjawiskiem jest vishing, który nie wymaga od przestępców zaawansowanej wiedzy informatycznej. Sprawcy wyłudzają dane używając do tego celu wyłącznie telefonu od czego pochodzi sama nazwa: *voice* i *phising*, M. Kowalska, *Co to jest vishing i dlaczego jest niebezpieczny?*, Politykabezpieczeństwa.pl, 27.04.2021, https://www.politykabezpieczenstwa.pl/pl/a/co-to-jest-vishing-i-dlaczego-jest-niebezpieczny (dostęp: 8.11.2021 r.).

[4] T. Pączkowski, *Słownik cyberbezpieczeństwa*, Katowice 2017, s. 37.

[5] A. Kiedrowicz-Wywiał, *Pharming i jego penalizacja*, „Prokuratura i Prawo" 2011, nr 6, s. 25.

[6] S. Rothenbühler, *Namite phishing – emotet can forge e-mails almost perfectly*, InfoGuard.ch, 18.04.2019, https://www.infoguard.ch/en/blog/dynamite-phishing-emotet-can-forge-e-mails-almost-perfectly (dostęp: 21.12.2021 r.). W niektórych przypadkach zauważono również, że na krótko przed linkiem wstawiono informację o treści: „Ważne dokumenty można znaleźć pod poniższym linkiem". Innym wariant polega na tym, że zainfekowany dokument jest dołączany bezpośrednio do wiadomości e-mail (*ibidem*).

Innym rodzajem ataku sieciowego typu phishing jest również *tabnapping*, który polega na wykorzystywaniu faktu otwierania stron w wielu zakładkach przeglądarki internetowej. Witryna atakująca podmienia wówczas zawartość innej strony znajdującej się w innej zakładce przeglądarki. Jeśli podmienioną w tle stroną jest np. strona banku, użytkownik może przypadkowo próbować się zalogować na podszywającą się pod prawdziwą witrynę banku spreparowaną stronę, która zdobędzie hasło do jego konta bankowego. Co ważne, podmieniana może być również strona logowania serwisu aukcyjnego lub systemu pocztowego[7]. Innym rodzajem phishingu jest tzw. *spear-phishing*, czyli ukierunkowany na konkretnego adresata atak[8], mający na celu wywarcie określonego wpływu lub wymuszenie działania w stosunku do odbiorcy. Przestępcy mogą podszywać się pod partnerów biznesowych danej osoby, a wiadomość może być spersonalizowana, tzn. bezpośrednio odwoływać się do istniejących relacji. Taki typ ataku jest często poprzedzony dokładnym rozpoznaniem przez atakującego określonego przedsiębiorstwa, urzędu lub informacji dostępnych o danej osobie w mediach społecznościowych[9]. Kolejnym rodzajem phishingu jest tzw. *clone*

[7] T. Pączkowski, *op. cit.*, s. 56.

[8] *Spear phishing* jest bardziej wyrafinowaną formą ataku phishingowego – ofiary otrzymują wiadomość e-mail, która rzekomo pochodzi od zaufanej osoby, firmy lub organizacji. Według FBI w Darknecie kwitnie handel narzędziami służącymi do przeprowadzania ataków phishingowych. Cyberprzestępcy opracowują i sprzedają narzędzia mające na celu skłonić konsumentów zaopatrujących się w znane marki do ujawnienia informacji o koncie osobistym w celu złamania zabezpieczeń kont i ominięcia protokołów bezpieczeństwa online. Internauta jest przekierowywany na stroną oszusta, gdzie pozostawia swoje dane uwierzytelniające, a gdy napastnicy uzyskają dostęp do kont internetowych konsumenta, mogą przechwycić wiadomości e-mail za pomocą kodów 2FA. Zaleca się, aby konsumenci nadal korzystali z opcji 2FA lub uwierzytelniania wieloskładnikowego oraz unikali używania podstawowego adresu e-mail do logowania. Warto także utworzyć unikalną nazwę użytkownika, która nie jest powiązana z podstawowym adresem e-mail, *Oszuści sięgają po inteligentny phishing*, Wgospodarce.pl, 30.11.2021, https://wgospodarce.pl/informacje/104482-oszusci-siegaja-po-inteligentny-phishing (dostęp: 30.11.2021 r.).

[9] *Czym jest PHISHING i jak nie dać się nabrać na podejrzane wiadomości e-mail oraz SMS-y?*, Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/baza-wiedzy/czym-jest-phishing-i-jak-nie-dac-sie-nabrac-na-podejrzane-widomosci-e-mail-oraz-sms-y (dostęp: 9.11.2021 r.). Należy w tym kontekście wspomnieć o jednym z największych zagrożeń współczesnego Internetu, jakim są botnety, a więc sieci botów, składające się z dużej liczby komputerów, które zostały przejęte przez złośliwe oprogramowanie w celu posłużenia hakerom, którzy je stworzyli. Dzięki kontroli nad setkami albo tysiącami maszyn hakerzy mogą wysyłać spam i wirusy, kraść dane osobowe lub przeprowadzać ataki DDoS. W wyniku ulepszonych

phishing – w tym przypadku nadawca nie tworzy sam fałszywego maila, lecz opiera się na wiadomości pochodzącej od danej instytucji, zmieniając tylko jej załączniki lub zastępując istniejący link, a następnie wysyła z adresu e-mail bardzo podobnego do prawdziwego. Specyficznym rodzajem phishingu jest *whaling*, który dotyczy osób znanych, czy też zajmujących ważne stanowiska. Jego celem może być uzyskanie dostępu do prywatnych dokumentów poprzez ściągnięcie na dysk złośliwego oprogramowania[10].

3. Charakterystyka phishingu i jego penalizacja

Przesyłane wiadomości, mające wyłudzić informacje, mają na celu skłonienie atakowanej osoby do określonego działania. W wiadomościach phishingowych często pojawiają się sformułowania nakłaniające do kliknięcia w link, sprawdzenia szczegółów, zweryfikowania danych, ustawień lub wręcz prośby o zalogowanie się np. w systemie bankowym. Kluczowym czynnikiem, który wpływa na skuteczność takich działań, jest łudząco podobny format wiadomości, a w szczególności zastosowanie tych samych czcionek, stopki w mailu, logo przedsiębiorstwa, czy też stylu jego komunikacji. Celem jest to, aby użytkownik lub klient był przekonany, że otrzymał wiadomość od istniejącego rzeczywiście przedsiębiorstwa[11]. Wiadomości phishingowe są przygotowywane

---

mechanizmów kontroli i rozwiązań bezpieczeństwa ruchu botnetowego, osoby przeprowadzające ataki zaczynają wykorzystywać farmy kliknięć. Oznacza to, że dziesiątki zdalnych „pracowników" systematycznie próbują zalogować się na docelowej stronie internetowej przy użyciu ostatnio zebranych danych uwierzytelniających. Połączenie pochodzi od osoby korzystającej ze standardowej przeglądarki internetowej, co utrudnia wykrycie oszustwa, J. Ojczyk, R. Skibińska, *Coraz więcej ataków phishingowych. Uważać muszą i banki, i ich klienci*, Prawo.pl 27.02.2021, https://www.prawo.pl/biznes/phishing-w-pandemii-co-powinny-robic-banki-i-klienci,506725.html (dostęp: 16.11.2021 r.).

[10] M. Jankowiak, M. Staniszewski, *Phishing – na czym polega i jak mu przeciwdziałać?*, Kancelaria prawna RPMS, 14.01.2021, https://rpms.pl/phishing-na-czym-polega-i-jak-mu-przeciwdzialac (dostęp: 12.11.2021 r.).

[11] R. Stępniewski, *Co to jest phishing?*, Politykabezpieczeństwa.pl, 04.02.2020, https://www.politykabezpieczenstwa.pl/pl/a/co-to-jest-phishing (dostęp: 13.11.2021 r.). Słowo „phishing" pierwszy raz pojawiło się w 1996 r. w kontekście wyłudzenia informacji od użytkowników dużego amerykańskiego serwisu AOL (*America Online*). Hakerzy wysłali wówczas

przez cyberprzestępców w taki sposób, aby wyglądały na autentyczne[12]. Mogą próbować skłonić daną osobę do ujawnienia poufnych informacji, zawierając link do strony internetowej rozprzestrzeniającej szkodliwe oprogramowanie (często przestępcy używają podobnych do autentycznych nazw witryn) lub przesyłając zainfekowany załącznik. Cyberprzestępcy, podszywając się m.in. pod firmy kurierskie, urzędy administracji, operatorów telekomunikacyjnych, czy nawet znajomych potencjalnych ofiar, starają się wyłudzić dane do logowania np. do ich kont bankowych lub używanych przez nich kont społecznościowych, a także systemów biznesowych. Coraz częściej oszuści działają także za pośrednictwem komunikatorów i portali społecznościowych, jak np. poprzez „metodę na BLIK-a"[13].

Phishing może funkcjonować dzięki wykorzystaniu narzędzi komunikacyjnych, m.in. poczty elektronicznej, komunikatorów internetowych oraz niektórych portali społecznościowych. Niekiedy sprawcy tego rodzaju czynów starają się przestraszyć potencjalne ofiary. Przykładem takiego działania może być wysłanie za pośrednictwem poczty elektronicznej wiadomości do użytkownika, w której zostanie on poproszony o pilne zalogowanie się na swoje konto bankowe, aby zaktualizować dane, z zastrzeżeniem, iż jeśli tego nie uczyni, straci możliwość logowania na to konto bankowe i posługiwania

spreparowane wiadomości z prośbą o udostępnienie danych dostępowych do kont użytkowników, zaś wielu z tych ostatnich nieświadomie podawało im komplet informacji (*ibidem*).

[12] Należy wspomnieć o wyroku Sądu Okręgowego w Warszawie z dnia 12 maja 2018 r., I C 566/17, LEX nr 2501476, na rzecz powoda, który pomimo zachowania należytej staranności w wyniku phishingu stracił niemal 80 tys. zł, przyznano od pozwanego banku kwotę niemal 107 tys. zł wraz z odsetkami (por. wyrok SA w Białymstoku z dnia 3 października 2019 r., I ACa 228/19, LEX nr 2932533), M. Jankowiak, M. Staniszewski, *op. cit.*, *passim*.

[13] *Czym jest PHISHING…*, *passim*. Na uwagę zasługuje także pojawienie się wirusa Zeus. Do zainfekowania komputera złośliwym oprogramowaniem dochodzi po otwarciu niebezpiecznego pliku lub w trakcie odwiedzania słabo zabezpieczonych stron internetowych (bardzo często niebudzących podejrzenia). Sama infekcja nie jest widoczna do chwili zalogowania się na stronie bankowości elektronicznej banku, który znajduje się na liście w pliku konfiguracyjnym trojana. Trojan Zeus p2p po zalogowaniu modyfikuje lokalnie na zainfekowanym komputerze klienta wygląd oryginalnej strony banku, w efekcie czego klient otrzymuje informację rzekomo pochodzącą z banku o tym, że w ramach testowania bankowości elektronicznej bank prosi o dokonanie przelewu testowego w określonej kwocie na podany rachunek. Ten komunikat jest podstawiony przez trojana i nie pochodzi z banku, ale wymusza na kliencie zatwierdzenie oszukańczego przelewu za pomocą używanego przez klienta sposobu autoryzacji, T. Pączkowski, *op. cit.*, s. 43.

się kartami płatniczymi. Wiadomość, którą otrzymuje odbiorca, zawiera link przekierowujący do fałszywej strony banku, której wygląd odpowiada oryginałowi; użytkownik wpisuje następnie swoje dane do logowania na stronę banku, otrzymując informację z podziękowaniem za zalogowanie, aktualizację danych oraz dostaje możliwość wylogowania się z serwisu. Takie strony są niekiedy tak zaprogramowane, aby wyświetlić użytkownikowi uaktualnienie numeru PIN do karty płatniczej, zaś wiadomość zawiera instrukcję o wprowadzeniu do formularza aktualizacji numeru karty klienta oraz aktualnego numeru PIN. Sprawca, dzięki takiemu działaniu, otrzyma zatem dane logowania na konto bankowe oraz karty płatniczej wraz z numerem PIN[14].

Należy zgodzić się z opinią, że w przyszłości ataki phishingowe staną się bardziej wyrafinowane, lepiej ukierunkowane i złożone, co umożliwi wyższy stopień automatyzacji. Nacisk na oszustwa e-mailowe będzie się stopniowo zmniejszał, a zamiast tego będzie coraz częściej zastępowany przez inne kanały. W przewidywalnej perspektywie nastąpi dalsza ekspansja nowych technologii, takich jak boty głosowe, które realistycznie imitują prawdziwe telefony od dyrektorów lub współpracowników, czy zwodniczo prawdziwe „głęboko fałszywe" filmy, które będą lub mogą być udostępniane szerszej publiczności, aby bardzo skutecznie manipulować pracownikami. Postępująca zmiana ataków phishingowych umożliwiona przez wyższy stopień automatyzacji, uwidoczniła

[14] A. Rogowski, *op. cit.*, *passim*. Strony internetowe podszywające się pod banki lub inne instytucje zazwyczaj są wykrywane i usuwane przez administratorów po ok. pięciu dniach. W tym czasie filtry antyphishingowe odnajdują taką stronę i dodają ją do stron zagrożonych, dlatego też sprawcy przestępstw muszą stale tworzyć i konfigurować nowe strony, aby zachować ciągłość swojego procederu. Sprawcy po uzyskaniu danych poufnych mogą użyć ich np. do wycofywania pieniędzy z kont bankowych, jak również do podrabiania kart płatniczych lub nadawania im numerów identyfikacyjnych odpowiadających oryginalnym kartom, aby za ich pośrednictwem wypłacać pieniądze. Wypłata i logowanie na konta bankowe oszukanych użytkowników odbywają się zazwyczaj w państwach słabo rozwiniętych, jak na przykład Nigeria. Osoby zajmujące się phishingiem, które weszły w posiadanie danych użytkowników, aby ograniczyć do minimum identyfikację oraz wykrycie przez organy ścigania, zazwyczaj sprzedają uzyskane dane innym osobom lub organizacjom przestępczym. Jednym z głównych celów sprawców jest uzyskiwanie danych, dzięki którym otrzymają dostęp do środków finansowych swoich ofiar. Bardzo popularna jest również kradzież poświadczeń pocztowych, dzięki którym sprawcy uwierzytelniają swoje działania, mając możliwość rozpowszechniania wirusów lub innych aplikacji (*ibidem*).

się już na przykładzie „phishingu dynamitowego”[15]. Oznaczać to będzie dalszy spadek znaczenia przestępstw e-mailowych, a więc „klasycznej” wręcz formy tego czynu.

Penalizacja phishingu została wprowadzona do Kodeksu karnego na mocy art. 1 ust. 2 ustawy z dnia 25 lutego 2011 r. o zmianie ustawy Kodeks karny (Dz.U. Nr 72 poz. 381), która weszła w życie z dniem 6 czerwca 2011 r.[16] Przestępstwo polegające na podszywaniu się pod określony podmiot w celu wyłudzenia danych osoby fizycznej wypełnia znamiona czynu przestępczego wymienione w art. 190a. § 2 kodeksu karnego. Jak brzmi § 1 tegoż artykułu,

> kto przez uporczywe nękanie innej osoby lub osoby jej najbliższej wzbudza u niej uzasadnione okolicznościami poczucie zagrożenia, poniżenia lub udręczenia lub istotnie narusza jej prywatność, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

Natomiast wspomniany § 2 tego samego artykułu:

> tej samej karze podlega, kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek, inne jej dane osobowe lub inne dane, za pomocą których jest ona publicznie identyfikowana, w celu wyrządzenia jej szkody majątkowej lub osobistej[17].

Przestępstwo stypizowane w art. 190a § 2 k.k. ma charakter powszechny, formalny i może być popełnione jedynie w zamiarze kierunkowym, co oznacza iż zostaje dokonane już w momencie podszycia się za ofiarę tego przestępstwa przez sprawcę wykorzystującego jej wizerunek oraz dane osobowe. Czynności

---

[15] N. Hellemann, *Phishing in the Pandemic – How Hackers Exploit the ‘Human Factor’*, September 2020, https://www.dotmagazine.online/issueFs/securing-the-future/human-firewall-for-it-security/phishing-the-human-factor (dostęp: 17.11.2021 r.).

[16] *Odpowiedź podsekretarza stanu w Ministerstwie Sprawiedliwości – z upoważnienia ministra – na interpelację nr 16546 w sprawie wzrastającej liczby różnego rodzaju przestępstw bankowych w Polsce*, Sejm Rzeczypospolitej Polskiej, https://www.sejm.gov.pl/sejm7.nsf/InterpelacjaTresc.xsp?key=095C4A56 (dostęp: 6.12.2021 r.).

[17] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. Dz.U. z 2022 r. poz. 1138 z późn. zm.).

sprawcze muszą być przy tym podjęte w celu wyrządzenia pokrzywdzonemu szkody majątkowej lub osobistej. Uzyskanie danych osobowych na potrzeby ataku phishingowego może być następstwem tzw. przestępstwa komputerowego o którym mowa w art. 287 k.k.[18] Phishing jest przy tym rodzajem oszustwa, a zatem przestępstwa uregulowanego w art. 267 k.k.

4. Wpływ zagrożenia wirusem COVID-19

Z uwagi na sytuację epidemiczną bardzo wiele osób zmuszonych było zmienić tryb pracy z tradycyjnej na zdalną. W efekcie braku odpowiedniego przygotowania pracownicy dokonywali czynności służbowych na prywatnych komputerach, co zwiększyło prawdopodobieństwo wykradzenia danych. Brak świadomości pracowników wynikał często z małej ilości lub niskiej jakości prowadzonych szkoleń[19]. Stąd odnotowywany w tak wielu państwach świata wzrost liczby przypadków phishingu. Dotyczyło to w szczególności wyłudzeń danych do kont bankowych. Kryzys spowodowany przez walkę z COVID-19 znacznie wzmocnił cyfryzację; w szczególności znacząco wzrosło wykorzystanie narzędzi do wideokonferencji i oprogramowania zdalnego, gdyż wielu zatrudnionych pracuje zdalnie w domu. Cyberprzestępcy stosunkowo szybko wykorzystali ogólny chaos i brak bezpieczeństwa. Znamienny jest przykład dostawcy zabezpieczeń Barracuda Networks, który w okresie od lutego do marca 2020 r. odnotował wzrost o ponad 667% ataków phishingowych związanych z koronawirusem[20].

[18] D. Lubowiecki, *op. cit.*, s. 35–36. W myśl tego przepisu, kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych, podlega karze pozbawienia wolności od 3 miesięcy do 5 lat. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku. Przestępstwo to może zostać popełnione na dwa sposoby: pierwszy z nich polega na wpłynięciu bez upoważnienia na przetwarzanie, gromadzenie lub przekazywanie danych informatycznych, natomiast drugi wiąże się z wpłynięciem na istniejące informacje – *ibidem*, s. 36.

[19] M. Piątek, *Cyberbezpieczeństwo a ochrona danych osobowych*, Instytut Nowej Europy, 05.05.2021, https://ine.org.pl/cyberbezpieczenstwo-a-ochrona-danych-osobowych (dostęp: 8.11.2021 r.).

[20] N. Hellemann, *op. cit.*, *passim*.

Według raportu amerykańskiej firmy informatycznej F5 Labs pt. „Raport o wyłudzeniu informacji i oszustwach 2020" liczba ataków phishingowych wzrosła o 220% w „szczycie pandemii", w porównaniu do średniej rocznej. Generalnie czynów przestępczych zaliczanych do phishingu jest o 15% więcej rok do roku. Według Ireneusza Wiśniewskiego, dyrektora zarządzającego F5 Poland, ryzyko wyłudzenia informacji w tak szczególnych warunkach jest większe niż kiedykolwiek, zaś oszuści coraz częściej używają certyfikatów cyfrowych, aby ich witryny wyglądały na autentyczne. Problem dostrzega też Komisja Nadzoru Finansowego, która zwraca uwagę, że pandemia przyczyniła się też do rozwoju elektronicznych kanałów dostępu do usług bankowych, czego dowodem jest to, że taki kontakt preferuje coraz więcej klientów. Jednocześnie jednak, zdaniem przewodniczącego KNF, Jacka Jastrzębskiego, świadomość klientów co do zagrożeń związanych z korzystaniem z nowoczesnych technologii jest niedostateczna, gdyż nie znają oni podstawowych zasad bezpieczeństwa korzystania ze zdalnych kanałów dostępu do usług finansowych związanych z powierzonymi środkami pieniężnymi. To z kolei wymusza działania po stronie sektora[21].

W pierwszym kwartale 2020 r. odnotowano 1 752 przypadki ataku phishingowego, co stanowiło niemal połowę wszystkich tego rodzaju ataków zarejestrowanych w całym 2019 r.[22] Zespół reagowania na incydenty cyberbezpieczeństwa (CSIRT NASK) zarejestrował w 2019 roku 6484 incydentów, wśród których 4100 było atakami typu „fraud", czyli oszustw internetowych)[23]. Po przeanalizowaniu 14 mln logowań miesięcznie w organizacji świadczącej usługi finansowe odnotowano aż 0,4% „manualnych" oszustw, a więc równowartość 56 tys. nieuczciwych prób logowania dokonywanego przez wynajęte osoby. Odnotowany został również wzrost liczby serwerów RTTP (protokół transferu w czasie rzeczywistym), które mogą przechwytywać oraz wykorzystywać rekomendowane

[21] J. Ojczyk, R. Skibińska, *Coraz więcej ataków phishingowych. Uważać muszą i banki, i ich klienci*, Prawo.pl 27.02.2021, https://www.prawo.pl/biznes/phishing-w-pandemii-co-powinny-robic-banki-i-klienci,506725.html (dostęp: 16.11.2021 r.).

[22] Dane CERT Polska za pierwszy kwartał 2020 r. pokazują, że w okresie pandemii liczba zagrożeń wzrasta, NASK Państwowy Instytut Badawczy, https://www.nask.pl/pl/aktualnosci/3835,Dane-CERT-Polska-za-pierwszy-kwartal-2020-roku-pokazuja-ze-w-okresie-pandemii-li.html (dostęp: 16.11.2021 r.).

[23] *Czym jest PHISHING…*, *passim*.

przez KNF kody uwierzytelniania wieloskładnikowego (MFA). RTPP działa jako „pośrednik", przechwytując transakcje ofiary z prawdziwą witryną internetową, a z uwagi na to, że atak następuje w czasie rzeczywistym, złośliwa witryna może zautomatyzować proces przechwytywania i odtwarzania uwierzytelniania opartego na czasie, takiego jak kody MFA. Może on także dokonywać kradzieży oraz ponownie wykorzystywać pliki cookie sesji[24].

O ile przed ogłoszeniem stanu pandemii przestępcy byli zmuszeni inwestować czas i zasoby w badanie celów, to okresie walki z COVID-19 mogą oni po prostu wynająć usługi *ransomware*[25] w ciemnej sieci lub kupić oprogramowanie, aby atakować za pomocą poczty e-mail. Masowe przejście do pracy zdalnej stworzyło nowy, gruby cel dla cyberprzestępców, ponieważ wielu pracowników pracujących w domu korzystało z niezabezpieczonych smartfonów i komputerów osobistych. W przypadku pracowników przyzwyczajonych do pracy w biurze przejście na model pracy domowej wymagało od nich integracji życia osobistego. W związku z tym cyberprzestępcy zmienili swoje techniki, aby atakować pracowników poprzez kampanie phishingowe i socjotechniczne o tematyce COVID, aby wykorzystać stres i niepokój związany z utrzymująca się trudną sytuacją. Warto zauważyć, że szczególnie atrakcyjni dla oszustów okazali się pracownicy usług finansowych, służby zdrowia, administracji publicznej i handlu detalicznego. Dyrektorzy usług finansowych i ubezpieczeniowych doświadczyli największego wzrostu liczby prób wyłudzenia okupu i informacji w ciągu 2020 r. Ataki typu „błędna dostawa", które nakłaniają ofiary do wysłania poufnych danych do zewnętrznego, złego podmiotu, stanowiły już ok. 55% zagrożeń skierowanych na pracowników usług finansowych. Dane skradzione z jednej witryny były wykorzystywane do włamywania się do kont w innej witrynie[26].

---

[24] J. Ojczyk, R. Skibińska, *op. cit.*, *passim*.

[25] *Ransomware* to złośliwe oprogramowanie, tworzone przez przestępców, które może dostać się komputera w szczególności poprzez odwiedzanie zainfekowanych stron. Uniemożliwia ono korzystanie z urządzenia, uzależniając przywrócenie pierwotnego stanu od zgody na określone warunki sprawcy.

[26] D. Patterson, *Cybercrime is thriving during the pandemic, driven by surge in phishing and ransomware*, CBSNews.com, 19.05.2021, https://www.cbsnews.com/news/ransomware-phishing-cybercrime-pandemic (dostęp: 17.11.2021 r.).

Według *Anti-Phishing Working Group* liczba przypadków phishingu na całym świecie podwoiła się w 2020 r. Sprawcy wykorzystują fakt, że wielu klientów dokonuje zakupów online, ma problemy z płynnością finansową, a także pragnie zaszczepić się przeciwko COVID-19. Inni używają COVID jako wymówki, by poprosić swoich klientów o aktualizację swoich danych osobowych przed kradzieżą tych informacji. Przedsiębiorstwa są atakowane przez oszustów podszywających się pod swoich dostawców w czasie, gdy wiele z nich koncentruje się tylko na próbie pozostania otwartymi[27]. Warto również zaznaczyć, że sprawcy zwykle nie wykorzystają własnych kont bankowych, posługując się osobami podstawionymi, co znacznie zwiększa bezpieczeństwo ich działania.

W USA, w pierwsze połowie 2020 r., gdy wielu Amerykanów pozostawało bezrobotnymi, przedsiębiorstwo Aura, zajmująca się bezpieczeństwem cyfrowym odnotowało 40-krotny wzrost oszustw phishingowych, których celem było zawiadomienie o bezrobociu. Niektóre próby phishingu polegały na podszywaniu się pod e-maile z korporacyjnych działów zasobów ludzkich z prośbą o dowód szczepienia. Pojawiały się e-maile od fałszywych organizacji zdrowotnych, zawierające w szczególności informacje o stosowanych środkach ostrożności lub możliwości leczenia COVID-19. Nadawcy zamieszczali m.in. nawet dane dotyczące infekcji koronawirusem i zgonów w treści każdej wiadomości e-mail, co dodatkowo zmuszało odbiorców do otwarcia załącznika[28].

W 2021 r. dochodziło również do oszustw za pomocą fałszywych wiadomości e-mail dotyczących dotacji na COVID-19. Użytkownicy byli proszeni o podanie danych karty bankowej w celu wypłaty środków, które nigdy do nich nie dotarły. W drugim kwartale 2021 r. powszechne były również fałszywe załączniki, które wysyłały użytkowników biznesowych do fałszywych portali logowania do usługi Office365 lub innego oprogramowania biznesowego,

[27] J. Chowdhury, *How the pandemic made phishing worse*, La Trobe University, 26.10.2021, https://www.latrobe.edu.au/news/articles/2021/opinion/how-the-pandemic-made-phishing-worse (dostęp: 17.11.2021 r.).

[28] T. Hunter, *That email asking for proof of vaccination might be a phishing scam*, Washingtonpost.com, 24.08.2021, https://www.washingtonpost.com/technology/2021/08/24/covid-vaccine-proof-scam-email (dostęp: 19.11.2021 r.).

oszustwa związane z przesyłaniem strumieniowym filmów online oraz związane z inwestycjami i nieruchomościami. Sprawcy doskonalą się również w sposobie dokonywania oszustw. Gdy WhatsApp został ściślej zintegrowany z Facebookiem na początku 2021 r., oszuści szybko dostosowali się do tej zmiany. Oszustwa na czacie lub wiadomościach zachęcały użytkowników do czatowania z „pięknymi nieznajomymi", przekierowują użytkowników na phishingową stronę logowania na Facebooku. Stwierdzono również, że wiadomości e-mail do użytkowników WhatsApp zawierały złośliwe oprogramowanie, które może wpływać na urządzenia mobilne[29].

5. Sposoby zwalczania phishingu

Niewątpliwie nie ma jednej i całkowicie skutecznej metody ochrony przed phishingiem. Znaczący wzrost liczby czynów uznawanych za phishing w sytuacji zagrożenia wirusem COVID-19 każe jednak postawić pytanie o sposoby przeciwdziałania temu zjawisku. Popularność ataków typu phishing sprawiła, że użytkownicy stali się bardziej świadomi istniejącego niebezpieczeństwa. Niereagowanie na korespondencję elektroniczną pochodzącą rzekomo z banku, w której jest się proszonym o ujawnienie swoich danych, własnoręczne wpisywanie adresu URL w pasku przeglądarki zamiast korzystania z linków zamieszczonych w wiadomościach lub na stronach internetowych, sprawdzanie certyfikatu strony logowania przed każdorazowym wprowadzeniem danych – to sposoby na uniknięcie większości dotychczas spotykanych zagrożeń. Mogą one jednak okazać się mało skuteczne w konfrontacji z *pharmingiem*[30]. Podobnie jest też w przypadku otrzymywania wiadomości e-mail z aktualizacjami dotyczącymi koronawirusa, gdzie nader trudno o powstrzymanie się przed działaniem motywowanym lękiem połączonym ze zwykłą ciekawością.

---

[29] B. Vigliarolo, *Phishing nadal atakuje duże firmy i wykorzystuje obawy związane z COVID-19 w II kwartale 2021 r.*, https://www.techrepublic.com/article/phishing-continues-to-target-big-businesses-and-exploit-covid-19-fears-in-q2-2021 (dostęp: 19.11.2021 r.).

[30] A. Kiedrowicz-Wywiał, *Pharming i jego penalizacja*, „Prokuratura i Prawo" 2011, nr 6, s. 25.

Można stwierdzić, że ataki phishingowe będą skuteczne, dopóki będzie istniał człowiek, którym można w określony sposób manipulować. Istotne jest to, aby zarówno mechanizmy kontroli bezpieczeństwa, jak i przeglądarki internetowe były sprawniejsze we wskazywaniu użytkownikom fałszywych witryn[31]. Użytkownicy powinni uważać na nieoczekiwane wiadomości e-mail oraz na załączniki do nich lub odsyłacze. Przedsiębiorstwa pozostają najpopularniejszymi celami ataków phishingowych, zaś oszustwa w różnorodny sposób związane z COVID-19 pozostają wciąż popularne[32]. W szczególności jest to zauważalne w przypadku banków. Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych nakłada na banki szereg obowiązków mających zapewnić bezpieczeństwo środków pieniężnych przechowywanych na rachunku bankowym. Praktyka sądowa uznająca roszczenia ofiar phishingu o zwrot nieautoryzowanych transakcji stanowi asumpt dla banków do stałego ulepszania zabezpieczeń oraz narzędzi autoryzacyjnych. Banki informują zatem na stronie logowania o zasadach bezpieczeństwa oraz potencjalnych zagrożeniach związanych z atakami phishingowymi[33]. Stąd też szczególnie ważne jest prowadzenie szkoleń pracowników tych przedsiębiorstw.

Nie należy klikać w przesyłane linki, a także na nie odpowiadać dopóki nie ma się pewności, że nadawca jest prawdziwy. W wiadomościach SMS lub e-mailach często wykorzystywane są tzw. tiny-URL, a więc skrócone adresy stron internetowych. Zalecane jest zwracanie szczególnej uwagi na nazwy

[31] J. Ojczyk, R. Skibińska, *op. cit.*, *passim*.

[32] B. Vigliarolo, *op. cit.*, *passim*.

[33] D. Lubowiecki, *op. cit.*, s. 42. W świetle ustawy o usługach płatniczych, klienci banków są objęci dodatkowym prawnym płaszczem ochrony, który jest w stanie częściowo zniwelować negatywne skutki dokonanego ich kosztem oszustwa. Ten mechanizm wynika z przepisów dotyczących autoryzowania transakcji płatniczych. Według art. 40 tejże ustawy transakcję uważa się za autoryzowaną, jeżeli płatnik wyraził zgodę na jej wykonanie w sposób przewidziany w umowie między nim, a jego dostawcą, a więc bankiem. Żaden przelew nie jest zatem autoryzowany, jeśli nie została wyrażona świadoma zgoda klienta, natomiast w przypadku nieautoryzowanej transakcji płatniczej, mocą art. 46 pkt 1, bank jest obowiązany niezwłocznie zwrócić płatnikowi jej kwotę. Co ważne, w art. 45 pkt 1 wprowadzono przy tym wyjątek od zasady ogólnej z art. 6 Kodeksu cywilnego, dzięki czemu to po stronie banku, a nie klienta, leży ciężar udowodnienia, że transakcja była autoryzowana. Musi on wykazać, że transakcja była autoryzowana lub że została wykonana nieautoryzowana umyślnie albo wskutek rażącego niedbalstwa płatnika, dotyczącego korzystania z instrumentu płatności – M. Jankowiak, M. Staniszewski, *op. cit.*, *passim*.

stron internetowych, które przesyłane są w budzących wątpliwości e-mailach oraz SMS-ach. Istotne jest przy tym jest ustalenie, czy wiadomość e-mail jest autentyczna. Należy zauważyć, że wiele wiadomości phishingowych ma niepoprawną gramatykę, interpunkcję, pisownię, czy też brak jest polskich znaków diakrytycznych np. nie używa się „ą", „ę" itd. Adres mailowy nadawcy jest niekiedy wręcz niewiarygodny, czy też nie jest tożsamy np. z podpisem pod treścią e-maila[34]. Jednocześnie jednak należy mieć na uwadze fakt, iż sposób przeprowadzania ataków phishingowych uległ w ostatnim czasie pewnej zmianie. Błędy ortograficzne, niepoprawna gramatyka i fałszywe zwroty grzecznościowe zostały zastąpione zwodniczo autentycznymi wiadomościami, które znacznie trudniej odróżnić od prawdziwych wiadomości e-mail pod względem wyglądu i treści[35].

Należy zaznaczyć, że pewne szczegóły mogą świadczyć o tym, że użytkownik został przekierowany na stronę zawierającą wirusa pobierającego dane osobowe. Strona wysłana przez przestępców ma także łudząco podobny adres do właściwej strony. Różnica może jednak wystąpić w końcówce adresu lub nawet w jego głównej treści. Tytułem przykładu można podać, że zamiast końcówki .com, zostaje użyta .com.pl, zaś nazwę dwuczłonową rozdziela się określnikiem zamiast myślnikiem. W treści wiadomości phishingowej może znaleźć się wezwanie do działania, takie jak np. prośba o uzupełnienie opłaty za paczkę w przedsiębiorstwie kurierskim lub wezwanie do zapłaty za abonament telefoniczny, a ponadto istnieją wiadomości, które pojawiają się w wybranym okresie w ciągu roku. Przykładem mogą być tutaj e-maile wysyłane w czasie rozliczania podatku dochodowego, w których najczęściej pojawia się wezwanie do uzupełnienia kwoty należnej z tytułu niedopłaty w pobranych zaliczkach. Również czas pandemii koronawirusa uaktywnił nowy typ wiadomości, które mogą dotyczyć np. wezwania do uiszczenia opłaty za dezynfekcję paczki przez przedsiębiorstwo kurierskie[36].

---

[34] Czym jest PHISHING…, *passim*.

[35] N. Hellemann, *op. cit.*, *passim*.

[36] *Czym jest phishing i jak się przed nim bronić? Jak rozpoznać wiadomości phishingowe?*, Payback.pl, 21.01.2021, https://www.payback.pl/ekstra/finanse/phishing?adobe_mc_ref=https://www.google.pl (dostęp: 14.12.2021 r.).

Jednocześnie należy zaznaczyć, że bank lub jakakolwiek inna instytucja nigdy nie powinna prosić klientów o podanie w wiadomości e-mail danych osobowych. Urzędy administracji publicznej nigdy nie proszą przy pomocy SMS lub maili o dopłatę do szczepionki, czy uregulowanie należności podatkowych. Stąd też wszelkie polecenia lub pytania w wiadomości e-mail na przykład dzwoniąc do banku z pytaniem czy rzeczywiście wysłana została taka wiadomość, należy także sprawdzać, czy dany link faktycznie prowadzi do właściwej strony. Wskazane byłoby także, aby podejrzanego e-maila oznaczać w skrzynce odbiorczej jako spam lub wiadomości śmieci lub podejrzany, co spowoduje usunięcie go ze skrzynki odbiorczej. Warto przy tym poinformować dostawcę poczty e-mail, że wiadomość została zidentyfikowana jako potencjalnie niebezpieczna[37]. Najprostszym rozwiązaniem jest także kontakt z danym przedsiębiorstwem w celu potwierdzenie lub wyjaśnienia odnośnie do przesłanej wiadomości. Tak też należy postępować w przypadku, gdyby mail pochodził od członka rodziny (podszywanie się pod takie osoby ma miejsce w przypadku oszustw dokonywanych metodą „na wnuczka").

W kontekście zagrożenia ze strony phishingu bardzo istotna jest możliwość rozpoznawania fałszywych stron internetowych. Przede wszystkim należy sprawdzić, czy adres danej strony jest prawidłowy. Certyfikat SSL chroni transakcje i zabezpiecza przesyłane przez pocztę i stronę WWW informacje, takie jak hasła, loginy, dane osobowe. Jeżeli adres strony WWW, na którą kieruje link ma literówkę lub kieruje na inny adres niż w rzeczywistości powinien albo jaki podany jest w treści linku, to jest to wyraźny sygnał ostrzegawczy. Nie należy klikać w linki przesłane w wiadomościach budzących wątpliwości (np. pochodzące od przedsiębiorstw z którymi dana osoba nigdy nie współpracowała), także w trybie *incognito* lub z innej przeglądarki, z której na co dzień się nie korzysta[38]. Zaleca się także nie korzystać z bankowości elektronicznej

[37] *Czym jest PHISHING…*, *passim*. Samo zgłaszanie phishingu jest stosunkowo proste. Będąc na stronie internetowej zespołu reagowania na incydenty komputerowe CERT Polska https://incydent.cert.pl/, należy wypełnić formularz online i dołączyć podejrzaną wiadomość. W razie uzasadnionego podejrzenia, że jest się ofiarą oszustwa lub wykrycia jego podejrzenia, należy zgłosić ten fakt także Policji lub do prokuratury, *ibidem*.

[38] R. Stępniewski, *op. cit.*, *passim*.

za pośrednictwem linków w przychodzących wiadomościach e-mail, ignorować linki i załączniki znajdujące się w wiadomościach trafiających do spamu. Istotne jest także regularne skanowanie komputera i korzystania z aktualnego oprogramowania antywirusowego[39].

6. Wnioski

Jak wykazano w niniejszym opracowaniu, walka z wirusem COVID-19 spowodowała pojawienie się okoliczności, które sprzyjały zwiększeniu się zagrożenia phishingiem. Jest to efektem upowszechnienia się modelu życia, w którym coraz to nowe pola aktywności jednostki realizowane się za pośrednictwem Internetu. Sam phishing, bazujący na ludzkich emocjach (w tym także strachu przed wirusem), braku wystarczającej wiedzy, ostrożności czy wręcz naiwności, skłania nieświadome zagrożenia ofiary do dokonywania działań na szkodę swojego majątku, pozostając wciąż poważnym zagrożeniem dla osób korzystających z dobrodziejstw, jakie niesie ze sobą Internet.

Obejmująca cały świat walka z wirusem COVID-19 implikuje powstanie warunków szczególnie korzystnych dla dokonywania przestępstw określonych mianem „phishingu". Jednocześnie jednak sprawcy tego rodzaju przestępstw stosują coraz bardziej wyrafinowane i złożone metody, aby wzbudzić zaufanie potencjalnych ofiar. Na przełomie drugiej i trzeciej dekady XXI w. daje się zauważyć znacząca ewolucja dotycząca zarówno *modus operandi* sprawców tego rodzaju przestępstw, ale także metod zwalczania phishingu. Wraz ze zmianami zachodzącymi w sposobie działania sprawców phishingu, ewoluować musi także sposób ochrony przed tego rodzaju działalnością przestępczą.

Obecnie dokonywane ataki phishingowe są przeprowadzone w sposób dużo bardziej zaawansowany. Rzadsze są przypadki pojawienia się chociażby błędów ortograficznych, czy takich „usterek", które pozwalają mieć wątpliwości co do proweniencji e-maila. W przewidywalnej przyszłości nastąpi zapewne ekspansja

[39] *Phishing – nie daj się złapać na haczyk!*, https://www.upc.pl/blog/phishing/ (dostęp: 13.11.2021 r.).

nowych technologii (botów głosowych), czy filmów pozwalających skutecznie manipulować pracownikami. Przykładem postępującej zmiany charakteru ataków jest w szczególności „phishing dynamitowy".

Stale zachodzące zmiany w *modus operandi* sprawców ataków pishingowych wymuszają konieczność prowadzenia działań o charakterze prewencyjnym. Niezależnie od wprowadzanych rozwiązań technicznych, odpowiednio edukowani powinni być tym zakresie pracownicy przedsiębiorstw. Jest to szczególnie istotne w kontekście pojawiania się kolejnych sposobów przechwytywania danych przez oddziaływanie na psychikę adresatów wiadomości mailowych dotyczących COVID-19, wykorzystujących ich obawy przed możliwym zakażeniem. W przyszłości należy spodziewać się kontynuacji tych działań przy zastosowaniu coraz bardziej wyrafinowanych sposobów działania.

Bibliografia

Chowdhury J., *How the pandemic made phishing worse*, La Trobe University, 26.10.2021, https://www.latrobe.edu.au/news/articles/2021/opinion/how-the-pandemic-made-phishing-worse (dostęp: 17.11.2021 r.).

Czym jest PHISHING i jak nie dać się nabrać na podejrzane wiadomości e-mail oraz SMS-y?, Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/baza-wiedzy/czym-jest-phishing-i-jak-nie-dac-sie-nabrac-na-podejrzane-widomosci-e-mail-oraz-sms-y (dostęp: 9.11.2021 r.).

Czym jest phishing i jak się przed nim bronić? Jak rozpoznać wiadomości phishingowe?, Payback.pl, 21.01.2021, https://www.payback.pl/ekstra/finanse/phishing?adobe_mc_ref=https://www.google.pl (dostęp: 14.12.2021 r.).

Hellemann N., *Phishing in the Pandemic – How Hackers Exploit the 'Human Factor'*, September 2020, https://www.dotmagazine.online/issues/securing-the-future/human-firewall-for-it-security/phishing-the-human-factor (dostęp: 17.11.2021 r.).

Hunter T., *That email asking for proof of vaccination might be a phishing scam*, Washingtonpost.com, 24.08.2021, https://www.washingtonpost.com/technology/2021/08/24/covid-vaccine-proof-scam-email (dostęp: 19.11.2021 r.).

Jankowiak M., Staniszewski M., *Phishing – na czym polega i jak mu przeciwdziałać?*, Kancelaria prawna RPMS, 14.01.2021, https://rpms.pl/phishing-na-czym-polega-i-jak-mu-przeciwdzialac (dostęp: 12.11.2021 r.).

Kiedrowicz-Wywiał A., *Pharming i jego penalizacja*, „Prokuratura i Prawo" 2011, nr 6.

Kowalska M., *Co to jest vishing i dlaczego jest niebezpieczny?*, Politykabezpieczeństwa.pl, 27.04.2021, https://www.politykabezpieczenstwa.pl/pl/a/co-to-jest-vishing-i-dlaczego-jest-niebezpieczny (dostęp: 8.11.2021 r.).

Lubowiecki D., *Prawno-kryminalistyczna problematyka phishingu, ze szczególnym uwzględnieniem środowiska bankowości internetowe*, „Kwartalnik Prawo-Społeczeństwo-Ekonomia" 2017, nr 1.

NASK Państwowy Instytut Badawczy, https://www.nask.pl/pl/aktualnosci/3835,-Dane-CERT-Polska-za-pierwszy-kwartal-2020-roku-pokazuja-ze-w-okresie-pandemii-li.html (dostęp: 16.11.2021 r.).

Odpowiedź podsekretarza stanu w Ministerstwie Sprawiedliwości – z upoważnienia ministra – na interpelację nr 16546 w sprawie wzrastającej liczby różnego rodzaju przestępstw bankowych w Polsce, Sejm Rzeczypospolitej Polskiej, https://www.sejm.gov.pl/sejm7.nsf/InterpelacjaTresc.xsp?key=095C4A56 (dostęp: 6.12.2021 r.).

Ojczyk J., Skibińska R., *Coraz więcej ataków phishingowych. Uważać muszą i banki, i ich klienci*, Prawo.pl 27.02.2021, https://www.prawo.pl/biznes/phishing-w-pandemii-co-powinny-robic-banki-i-klienci,506725.html (dostęp: 16.11.2021 r.).

Oszuści sięgają po inteligentny phishing, Wgospodarce.pl, 30.11.2021, https://wgospodarce.pl/informacje/104482-oszusci-siegaja-po-inteligentny-phishing (dostęp: 30.11.2021 r.).

Patterson D., *Cybercrime is thriving during the pandemic, driven by surge in phishing and ransomware*, CBSNews.com, 19.05.2021, https://www.cbsnews.com/news/ransomware-phishing-cybercrime-pandemic (dostęp: 17.11.2021 r.).

Pączkowski T., *Słownik cyberbezpieczeństwa*, Katowice 2017.

Phishing – nie daj się złapać na haczyk!, https://www.upc.pl/blog/phishing/ (dostęp: 13.11.2021).

Rogowski A., *Phishing*, „Kwartalnik Policyjny" 2017, nr 4, http://kwartalnik.csp.edu.pl/kp/archiwum-1/2017/nr-42017/3723,Phishing.html (dostęp: 12.11.2021 r.).

Rothenbühler S., *Namite phishing – emotet can forge e-mails almost perfectly*, InfoGuard.ch, 18.04.2019, https://www.infoguard.ch/en/blog/dynamite-phishing-emotet-can-forge-e-mails-almost-perfectly (dostęp: 21.12.2021 r.).

Stępniewski R., *Co to jest phishing?*, Politykabezpieczeństwa.pl, 04.02.2020, https://www.politykabezpieczenstwa.pl/pl/a/co-to-jest-phishing (dostęp: 13.11.2021 r.).

Vigliarolo B., *Phishing nadal atakuje duże firmy i wykorzystuje obawy związane z COVID-19 w II kwartale 2021 r.*, https://www.techrepublic.com/article/phishing-continues-to-target-big-businesses-and-exploit-covid-19-fears-in-q2-2021 (dostęp: 19.11.2021 r.).

Joanna Taczkowska-Olszewska

Odpowiedzialność za dostarczanie, wprowadzanie do obrotu i korzystanie z systemów sztucznej inteligencji – projekty rozwiązań prawnych w świetle gwarancji praw podstawowych

1. Wprowadzenie

Prace ustawodawcy europejskiego zmierzające do osiągnięcia celu definiowanego jako „zapewnieniu prawidłowego funkcjonowania jednolitego rynku przez stworzenie warunków sprzyjających rozwijaniu i wykorzystywaniu w Unii wiarygodnej sztucznej inteligencji”[1] znalazły się na końcowym etapie[2]. Zwieńczenie prac ma stanowić przyjęcie przez Parlament Europejski i Radę projektu rozporządzenia ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji)[3]. Ocena projektowanej regulacji została wyrażona przez organy ustawodawcze państw członkowskich UE,

[1] Uzasadnienie wniosku Komisji Europejskiej z dnia 21 kwietnia 2021 r. Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii, COM(2021) 206 final, s. 1, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52021PC0206 (dostęp: 27.12.2022 r.).

[2] Projekt został przyjęty przez Komisję 21 kwietnia 2021 r. i tego samego dnia został przekazany Radzie i Parlamentowi Europejskiemu. Polska wersja projektu została przekazana Sejmowi 7 czerwca 2021 r. Tego samego dnia został przekazany list Komisji informujący o przesłaniu izbom parlamentów narodowych wszystkich wersji językowych projektu. Od tej daty rozpoczął bieg ośmiotygodniowy termin na przesłanie przewodniczącym Parlamentu Europejskiego, Rady i Komisji uzasadnionej opinii zawierającej powody, dla których parlament narodowy (lub izba parlamentu narodowego) uznaje, że projekt nie jest zgodny z zasadą pomocniczości (na podstawie art. 6 protokołu nr 2) (Zob. Opinia BAS z dnia 19 lipca 2022 r. na temat wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze Unii (COM(2021) 206 final).

[3] Projekt Rozporządzenia Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji)

w tym Polski[4]. Nie wniesiono istotnych zastrzeżeń, ani w zakresie przyjętych w projekcie rozporządzenia rozwiązań, ani w odniesieniu do charakteru zaproponowanego przez Komisję Europejską instrumentu regulacyjnego. Krajowy ustawodawca uznał zatem, że odpowiednim instrumentem regulacyjnym jest rozporządzenie[5].

Projekt rozporządzenia Akt w sprawie sztucznej inteligencji stanowi element większego kompleksowego pakietu środków mających w zamyśle prawodawcy europejskiego, zapewnić utrzymanie wiodącej pozycji UE w zakresie technologii[6], a także zapewnienie rozwiązań prawnych przy założeniu, że „sztuczna inteligencja powinna działać na rzecz ludzi i społeczeństwa, a ostatecznym celem jest zwiększenie dobrostanu człowieka"[7].

---

i zmieniające niektóre akty ustawodawczeUnii, COM(2021) 206 final, s. 1 https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52021PC0206 (dostęp: 27.12.2022 r.).

[4] Projekt Wniosku KE dotyczącego rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) był przedmiotem opinii przygotowanej na zlecenie Biura Analiz Sejmowych a także był opiniowany w dniu 22 lipca 2021 r. przez Sejmową Komisję ds. UE. Komisja Sejmowa nie wniosła uwag ani zastrzeżeń do projektu. Przedstawiciel rady Ministrów obecny na posiedzeniu zwrócił uwagę, że pewnym mankamentem projektowanych regulacji jest zbyt wąska definicja „sztucznej inteligencji", która w jego ocenie może prowadzić do nieuzasadnionej nadregulacji(zob. zapis przebiegu posiedzenia, https://orka.sejm.gov.pl/zapisy9.nsf/o/F693847336ADC379C1258728003484C0/%24File/0158109.pdf, dostęp: 27.12.2022 r.) W dniu 07 października 2021 r. projekt rozporządzenia był opiniowany przez Senacką Komisję Spraw Zagranicznych i Unii Europejskiej.Komisja Senacka wyraziławątpliwości co do możliwości wyjątkowego użycia systemu zdalnej identyfikacji biometrycznej „w czasie rzeczywistym" w przestrzeni publicznej do celów egzekwowania prawa bez wcześniejszego zezwolenia wydanego przez organ sądowy lub niezależny organ administracyjny państwa członkowskiego (art. 5 ust. 3 i 4). W ocenie KSZUE przypadki, w których może dojść do takiej sytuacji powinny zostać ograniczone i doprecyzowane, a sądowa kontrola takiego zezwolenia wzmocniona zbyt szerokiego zdefiniowania zakresu pojęciowego „systemu sztucznej inteligencji" (Zob. Opinia Komisji Spraw Zagranicznych iUE, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CONSIL:ST_12778_2021_REV_1&from=PL, dostęp: 27.12.2022 r.).

[5] Należy zgodzić się tymczasem ze stanowiskiem wyrażonym w opinii Biura Analiz Sejmowych, zgodnie z którym odwołanie się przez KE do art. 14 TFUE jako podstawy prawnej uzasadniającej wybór rozporządzenia jako instrumentu regulacyjnego nie jest prawidłowe. Za niewystarczające należy bowiem uznać uzasadnienie sprowadzające się do stwierdzenia, że proponowane rozporządzenie ogranicza możliwość posługiwania się niektórymi systemami AI przez organy państw członkowskich. Słusznie zatem podkreślono, żew analizowanym przypadku uzasadnienie przez Komisję Europejską wyboru rozporządzenia jako preferowanego środka nie jest zadowalające (zob. Opinia BAS, s. 15).

[6] *Ibidem*, s. 2.

[7] *Ibidem*, s. 3.

2. Założenia i cele badawcze

Pomimo istnienia zasadniczo słusznego celu regulacji a także przyjmując, że jest ona niezbędna ze względu na występowanie rozproszonych, niespójnych i niekompletnych uregulowań przyjmowanych w poszczególnych państwach UE, może rodzić się pytanie, czy przyjęty przez KE sposób normowania zakresów i zasad odpowiedzialności oraz rozkład obowiązków spoczywających na podmiotach wprowadzających do obrotu systemy SI lub korzystających z takich systemów gwarantuje skuteczną ochronę osobom, do których systemy te znajdą zastosowanie, a zatem osobom – jak należy przyjąć – narażonym na zastosowanie sztucznej inteligencji. Zagadnienie to dotyczy zarówno ustalenia zakresu i charakteru obowiązków związanych ze stosowaniem systemów SI jak również ustalenia kręgu adresatów tych obowiązków oraz zasad ponoszenia odpowiedzialności za ich naruszenie. U podłoża wskazanego problemu pojawia się założenie, zgodnie z którym przyszłe rozwiązania prawne promujące rozwój systemów sztucznej inteligencji następować będą kosztem praw podstawowych. Nie jest bowiem możliwy rozwój sztucznej inteligencji bez przetwarzania danych osobowych, a okoliczność ta przesądza o nieuchronności ingerencji w prawa i wolności człowieka. Zakłada się zarazem, że zapewnienie skutecznego środka ochrony tych praw wymaga od ustawodawcy ukształtowania nowego reżimu ochrony powiązanego ze skalą rzeczywistych lub ewentualnych naruszeń wywołanych działaniem systemów sztucznej inteligencji.

3. Charakter i cele projektowanych rozwiązań prawnych

Przyjęcie w niedalekiej przyszłości Aktu w sprawie sztucznej inteligencji[8] oznaczać będzie, że sytuacja prawna obywateli państw UE zostanie osadzona w nowej rzeczywistości cyfrowej, której fundamenty zdecydowano się unormować

[8] Wniosek Komisji Europejskiej z dnia 21 kwietnia 2021 r. Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii, COM(2021) 206 final, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52021PC0206 (dostęp: 27.12.2022 r.).

wykorzystując do tego celu rozporządzenie jako akt prawny, który ma zasięg ogólny, wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich[9]. W projekcie rozporządzenia prawodawca europejski porządkuje katalog podmiotów odpowiedzialnych za działanie sztucznej inteligencji, dokonując nie tylko specyfikacji zadań i zakresów odpowiedzialności, ale także rozstrzygając o statusie prawnym systemów sztucznej inteligencji i odsyłając w tym zakresie do stosowania przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1020 z dnia 20 czerwca 2019 r. w sprawie nadzoru rynku i zgodności produktów[10]. Komisja realizuje w ten sposób zalecenie zawarte w rezolucji Parlamentu Europejskiego z dnia 20 października 2020 r. w sprawie systemu odpowiedzialności cywilnej za sztuczną inteligencję (2020/2014(INL))[11]. Parlament Europejski zwrócił w tym dokumencie uwagę na potrzebę udzielenie odpowiedzi, w jakim zakresie do systemów SI, a także odpowiedzialności za treści i usługi cyfrowe znajdować mogą zastosowanie pojęcia: „produkt", „producent", „wada", „szkoda", definiowane w dyrektywie Rady 85/374/EWG z dnia 25 lipca 1985 r. w sprawie zbliżenia przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich dotyczących odpowiedzialności za produkty wadliwe[12]. Parlament Europejski zauważył, że dyrektywę w sprawie odpowiedzialności za produkty należy nadal stosować w odniesieniu do roszczeń z tytułu odpowiedzialności cywilnej producenta wadliwego systemu SI, jeżeli system taki można uznać za „produkt" w rozumieniu tej dyrektywy[13]. Parlament Europejski wskazał, że kwestia odpowiedzialności w odniesieniu do szkód spowodowanych przez

[9] Art. 288 TFUE.

[10] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1020 z dnia 20 czerwca 2019 r. w sprawie nadzoru rynku i zgodności produktów oraz zmieniające dyrektywę 2004/42/WE oraz rozporządzenia (WE) nr 765/2008 i (UE) nr 305/2011 (Dz.Urz. UE L Nr 169, s. 1).

[11] https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_PL.html (dostęp: 27.12.2022 r.).

[12] Dyrektywa Rady z dnia 25 lipca 1985 r. (85/374/EWG) w sprawie zbliżenia przepisów ustawowych, wykonawczych i administracyjnych Państw Członkowskich dotyczących odpowiedzialności za produkty wadliwe (Dz.Urz. UE L Nr 210, s. 29 z późn. zm.).

[13] Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. z zaleceniami dla Komisji w sprawie systemu odpowiedzialności cywilnej za sztuczną inteligencję (2020/2014(INL)), pkt. 7.

system SI jest jednym z kluczowych aspektów, którymi należy się zająć w ramach tych przepisów, a w konsekwencji zalecił rozważenie, by powszechne zasady dotyczące systemów sztucznej inteligencji przyjęły formę rozporządzenia.

Komisja Europejska realizuje, w części dotyczącej klasyfikacji systemów SI, wskazane powyżej zalecenie zarówno poprzez wybór rozporządzenia jako instrumentu regulacji, jak również poprzez zastosowanie na gruncie aktu w sprawie SI przepisów rozporządzenia (UE) nr 2019/1020 w sprawie nadzoru rynku i zgodności produktów[14]. Zarówno zdefiniowane tam pojęcie „podmiotu gospodarczego", jak również pojęcie „produktu" zostały przeniesione na grunt projektu rozporządzenia w sprawie SI. Oznacza to, że wszelkie odniesienia do „podmiotu gospodarczego" zawarte w rozporządzeniu (UE) nr 2019/1020 obejmują także wszystkich operatorów systemów SI. Natomiast wszelkie odniesienia do „produktu" znajdujące się w rozporządzeniu (UE) nr 2019/1020 obejmują wszystkie systemy sztucznej inteligencji wchodzące w zakres rozporządzenia w sprawie SI[15]. „Podmiot gospodarczy" oznacza producenta, upoważnionego przedstawiciela, importera, dystrybutora, dostawcę usług realizacji zamówień lub każdą inną osobę fizyczną lub prawną podlegającą obowiązkom związanym z wytwarzaniem produktów, udostępnianiem ich na rynku lub oddawaniem do użytku zgodnie z odpowiednim unijnym prawodawstwem harmonizacyjnym[16]. Status producenta posiadać będą zatem wszyscy operatorzy w rozumieniu tytułu III rozdział 3 rozporządzenia w sprawie SI. Pojęcie „operatora" obejmuje wiele podmiotów[17], którym w różnych okresach „życia" SI projektodawca powierza

[14] W art. 63 ust. 1 projektu rozporządzenia „Akt w sprawie SI" postanowiono, że w odniesieniu do wszystkich systemów sztucznej inteligencji, a zatem niezależnie od poziomu generowanego przez nie ryzyka,zastosowanie mają przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1020 z dnia 20 czerwca 2019 r. w sprawie nadzoru rynku i zgodności produktów oraz zmieniające dyrektywę 2004/42/WE oraz rozporządzenia (WE) nr 765/2008 i (UE) nr 305/2011 (Dz.Urz. UE L Nr 169, s. 1).

[15] Art. 63 ust. 1 lit. a i b projektu rozporządzenia w sprawie SI.

[16] Art. 3 pkt 12 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1020 z dnia 20 czerwca 2019 r. w sprawie nadzoru rynku i zgodności produktów oraz zmieniające dyrektywę 2004/42/WE oraz rozporządzenia (WE) nr 765/2008 i (UE) nr 305/2011 (Dz.Urz. UE L Nr 169, s. 1).

[17] Pojęcie „operatora" w rozumieniu tytułu III projektu rozporządzenia w sprawie SI obejmuje: 1) dostawców systemów sztucznej inteligencji; 2) producentów produktu wymienionego w załączniku II sekcja A (chodzi zatem o: zabawki; jednostki pływające i skutery

zadania, nakłada na nie obowiązki i przypisuje – adekwatnie do przypisanych zadań i obowiązków – zakresy odpowiedzialności. Na operatorze ciąży zarazem generalny obowiązek podjęcie wszelkich odpowiednich działań naprawczych w odniesieniu do wszystkich odnośnych systemów sztucznej inteligencji, które operator wprowadził do obrotu w całej UE[18].

4. Reżimy odpowiedzialności

Komisja Europejska w projektowanych rozwiązaniach prawnych zrezygnowała z wprowadzania nowych form osobowości prawnej w odniesieniu do sztucznej inteligencji (osobowość elektroniczna), realizując w tym zakresie postulat zgłaszany przez Europejski Komitet Ekonomiczno-Społeczny oraz Parlament Europejski.

W projekcie rozporządzenia „Akt w sprawie SI" przesądzono – jak się wydaje ostatecznie[19] – o rezygnacji z nadawania systemom sztucznej inteligencji form osobowości prawnej, a w miejsce tej koncepcji zaproponowano kaskadowo uporządkowaną strukturę podmiotów odpowiedzialnych na różnych etapach „życia" sztucznej inteligencji za jej niewadliwe działanie rozumiane jako osiąganie przez systemy SI określonych przez człowieka i pod jego nadzorem celów[20]. Operatorzy, w zależności od rodzaju podejmowanej aktywności (dostawcy, importerzy,

wodne; dźwigi i elementy dźwigów; urządzenia i systemy ochronne przeznaczone do użytku w atmosferze potencjalnie wybuchowej; urządzenia radiowe; urządzenia ciśnieniowe; urządzenia kolei linowych; środki ochrony indywidualnej; urządzenia spalające paliwa gazowe; wyroby medyczne oraz wyroby do diagnostyki *in vitro*); jeśli jest system SI jest z nim powiązany; 3) importerów; 4) użytkowników systemów SI; 5) dystrybutorów.

[18] Art. 65 ust. 4 projektu rozporządzenia w sprawie SI.

[19] PE w projekcie wniosku w sprawie projektu wniosku PE i rady dotyczącego w sprawie odpowiedzialności za działanie systemów sztucznej inteligencji podkreśla, że Wszelkie zmiany wymagane w obowiązujących ramach prawnych powinny rozpocząć się od wyjaśnienia, że systemy SI nie mają osobowości prawnej ani sumienia, a ich jedynym zadaniem jest służenie ludzkości (motyw 6).

[20] W art. 14 ust. 1 projektu rozporządzenia wskazano, że systemy sztucznej inteligencji wysokiego ryzyka projektuje się i opracowuje się w taki sposób, w tym poprzez uwzględnienie odpowiednich narzędzi interfejsu człowiek-maszyna, aby w okresie wykorzystywania systemu sztucznej inteligencji wysokiego ryzyka mogły je skutecznie nadzorować osoby fizyczne.

dystrybutorzy, użytkownicy, producenci), ponosić będą odpowiedzialność indywidualną zarówno z działania, jak i z zaniechania. Dla porządku należy wskazać, że pojęcie „operator" zostało także zdefiniowane w projekcie rozporządzenie w sprawie odpowiedzialności cywilnej za działanie SI[21] i oznacza zarówno operatora *front-end*, jak i operatora *back-end*. Operatora *front-end* definiuje się jako osobę fizyczną lub prawną, która do pewnego stopnia kontroluje ryzyko związane z obsługą i funkcjonowaniem systemu SI i korzysta z jego działania. Operatora *back-end* należy zdefiniować jako osobę fizyczną lub prawną, która w sposób ciągły określa cechy technologii, dostarcza dane i podstawowe usługi wsparcia, a zatem sprawuje również pewną kontrolę nad ryzykiem związanym z obsługą i funkcjonowaniem systemu SI.

Projektodawca decyduje się na odmienne ukształtowanie odpowiedzialności w odniesieniu do systemów wysokiego ryzyka oraz pozostałych systemów odpowiedzialności[22]. Spostrzeżenie to dotyczy zarówno charakteru i płaszczyzny odpowiedzialności, jak również jej zakresu, trybu i zasad. Na płaszczyźnie administracyjnoprawnej państwa członkowskie będą mogły nakładać administracyjne kary pieniężne na operatorów systemów SI, przy czym rozmiar kary powinien uwzględniać okoliczności wskazane w art. 71 ust. 6 projektu rozporządzenia, tj.:

a) charakter, wagę i czas trwania naruszenia oraz jego konsekwencje;
b) czy inne organy nadzoru rynku nałożyły już na tego samego operatora administracyjne kary pieniężne za to samo naruszenie;
c) wielkość operatora dopuszczającego się naruszenia i jego udział w rynku.

Najwyższa kara 30 mln euro albo – w odniesieniu do przedsiębiorstwa – do 6% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego może zostać nałożona na operatora systemu SI w razie naruszenia jednego z zakazów wskazanych w art. 5 projektu rozporządzenia w sprawie SI

[21] Wniosek dotyczący Rozporządzenia PE i Rady w sprawie odpowiedzialności za działanie systemów sztucznej inteligencji, https://www.europarl.europa.eu/doceo/document/A-9-2020-0178_PL.html (dostęp: 27.12.2022 r.).

[22] A. Michalak, *Projekt rozporządzenia Paramentu UE o odpowiedzialności cywilnej za działania sztucznej inteligencji – krok w dobrym kierunku czy niepotrzebne odstępstwo od zasad ogólnych?*, [w:] *Prawo sztucznej inteligencji i nowych technologii*, red. B. Fischer, A. Pązik, M. Świerczyński, Warszawa 2021, s. 44.

lub w przypadku niezgodności systemu SI z wymogami opisanymi w art. 10, który określa sposób korzystania przez operatorów z danych treningowych, walidacyjnych i testowych.

W odniesieniu do odpowiedzialności cywilnej o charakterze odszkodowawczym projektodawca przewiduje dwa reżimy odpowiedzialności. Operatorzy systemów wysokiego ryzyka ponosić mają odpowiedzialność na zasadzie ryzyka podczas, gdy do odpowiedzialności operatorów pozostałych systemów nadal powinny znajdować zastosowanie reguły odpowiedzialności na zasadzie winy stosowane jak w przypadku odpowiedzialności za produkty wadliwe[23]. Wszelkie fizyczne bądź wirtualne działania, urządzenia czy procesy sterowane systemem SI, które nie zostały wymienione jako obarczone wysokim ryzykiem w rozporządzeniu, powinny być – jak zaleca PE – nadal objęte odpowiedzialnością na zasadzie winy, chyba że w mocy są surowsze przepisy krajowe i prawodawstwo w zakresie ochrony konsumentów. Prawo krajowe państw członkowskich, w tym wszelkie odnośne orzecznictwo, odnoszące się do kwoty i zakresu odszkodowania, jak również do okresu przedawnienia powinno mieć nadal zastosowanie. Osoba poszkodowana w wyniku działania systemu SI, który nie został wymieniony jako obarczony wysokim ryzykiem, powinna korzystać z domniemania winy operatora[24].

Czynnikiem determinującym odpowiedzialność jest rodzaj systemu SI, nad którym sprawuje kontrolę dany operator. System SI, który z natury wiąże się ze znacznym ryzykiem i działa autonomicznie, potencjalnie zagraża ogółowi społeczeństwa w znacznie większym stopniu. Zasadne jest wobec tego, w ocenie PE, stworzenie powszechnego surowego systemu odpowiedzialności dla tych autonomicznych systemów SI obarczonych wysokim ryzykiem. Za właściwe PE uznaje do tych systemów podejście oparte na ryzyku, przy czym powinno

[23] Na gruncie dyrektywy Rady 85/374/EWG z dnia 25 lipca 1985 r. w sprawie zbliżenia przepisów ustawowych, wykonawczych i administracyjnych Państw Członkowskich dotyczących odpowiedzialności za produkty wadliwe (Dz.Urz. UE L Nr 210, s. 29 z późn. zm.) odpowiedzialność niezależna od winy powinna mieć zastosowanie jedynie do rzeczy ruchomych pochodzących z produkcji przemysłowej.

[24] Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. z zaleceniami dla Komisji w sprawie systemu odpowiedzialności cywilnej za sztuczną inteligencję (2020/2014(INL)), pkt 17.

się ono opierać się na jasnych kryteriach i odpowiedniej definicji „wysokiego ryzyka" oraz zapewniać pewność prawa[25].

Odpowiedzialność operatora opiera się na przekonaniu, że do pewnego stopnia kontroluje on ryzyko związane z działaniem systemu SI, które jest porównywalne z ryzykiem, jakie ponosi właściciel samochodu[26]. Poszkodowany powinien mieć prawo zgłaszania roszczeń z tytułu odpowiedzialności w całym łańcuchu odpowiedzialności i w całym cyklu życia systemu SI. Określone w rozporządzeniu zasady odpowiedzialności powinny zasadniczo odnosić się też do wszystkich systemów SI niezależnie od tego, gdzie działają i czy ich działanie ma charakter fizyczny czy wirtualny[27]. Określenie, z jakim prawdopodobieństwem systemy SI obciążone wysokim ryzykiem mogą spowodować szkody, zależy od wzajemnych powiązań między celem zastosowania, dla którego system SI jest wprowadzany do obrotu, sposobem wykorzystania systemu SI, powagą ewentualnych szkód, stopniem autonomiczności w podejmowaniu decyzji, które mogą spowodować szkodę, a prawdopodobieństwem, że zagrożenie rzeczywiście wystąpi[28].

W rozporządzeniu „Akt w sprawie sztucznej inteligencji" Komisja Europejska, zgodnie z zaleceniem Parlamentu Europejskiego, stosuje podejście oparte na analizie ryzyka, wprowadzając rozróżnienie między zastosowaniami AI, które stwarzają:

1/ niedopuszczalne ryzyko,

2/ wysokie ryzyko oraz

3/ niskie lub minimalne ryzyko[29].

Obciążenia regulacyjne nakłada się tylko w przypadku, gdy system SI może stwarzać wysokie ryzyko dla praw podstawowych. W przypadku systemów nieobarczonych wysokim ryzykiem wprowadzono jedynie bardzo ograniczone obowiązki dotyczące zapewnienia przejrzystości[30].

---

25 *Ibidem*, pkt 8.
26 *Ibidem*, pkt 10.
27 *Ibidem*, pkt 12.
28 *Ibidem*, pkt 13.
29 Uzasadnienie wniosku Komisji Europejskiej z dnia 21 kwietnia 2021 r., s. 15.
30 *Ibidem*, s. 8.

Ustawodawca europejski kształtuje na gruncie obu projektów (rozporządzenie w sprawie SI, jak i rozporządzenie w sprawie odpowiedzialności cywilnej) obowiązki operatorów systemów SI w taki sposób, by było możliwe przypisanie odpowiedzialności za szkody spowodowane działaniem SI konkretnemu podmiotowi. Wskazuje się zatem, że systemy sztucznej inteligencji wysokiego ryzyka należy projektować i opracowywać w taki sposób, aby osoby fizyczne mogły nadzorować ich funkcjonowanie. W tym celu przed wprowadzeniem systemu do obrotu lub jego oddaniem do użytku dostawca systemu powinien określić odpowiednie środki związane z nadzorem ze strony człowieka. W szczególności, w stosownych przypadkach, takie środki powinny gwarantować, że system podlega wbudowanym ograniczeniom operacyjnym, których sam nie jest w stanie obejść, i reaguje na działania człowieka–operatora systemu, oraz że osoby fizyczne, którym powierzono sprawowanie nadzoru ze strony człowieka, posiadają niezbędne kompetencje, przeszkolenie i uprawnienia do pełnienia tej funkcji.

5. Systemy sztucznej inteligencji wysokiego ryzyka

Przez „systemy sztucznej inteligencji stwarzające ryzyko" rozumie się „produkt mogący mieć niekorzystny wpływ na zdrowie i bezpieczeństwo osób w ujęciu ogólnym, zdrowie i bezpieczeństwo w miejscu pracy, ochronę konsumentów, środowiska, bezpieczeństwa publicznego i innych interesów publicznych chronionych przez obowiązujące unijne prawodawstwo harmonizacyjne, w stopniu wykraczającym poza wpływ uważany za uzasadniony i dopuszczalny w stosunku do zamierzonego celu produktu lub w zwykłych lub dających się racjonalnie przewidzieć warunkach używania produktu, w tym długości okresu jego używania oraz, w stosownych przypadkach, wymagań dotyczących oddania do użytku, instalacji i konserwacji"[31].

[31] Art. 3 pkt 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1020 z dnia 20 czerwca 2019 r. w sprawie nadzoru rynku i zgodności produktów oraz zmieniające dyrektywę 2004/42/WE oraz rozporządzenia (WE) nr 765/2008 i (UE) nr 305/2011 (Dz.Urz. UE L

Klasyfikacja systemu sztucznej inteligencji jako systemu wysokiego ryzyka opiera się na przeznaczeniu systemu AI, zgodnie z obowiązującymi przepisami dotyczącymi bezpieczeństwa produktów. Dlatego też zaklasyfikowanie systemu jako systemu SI wysokiego ryzyka zależy nie tylko od funkcji pełnionej przez system sztucznej inteligencji, ale także od konkretnego celu i trybu jego wykorzystania. Wysokie ryzyko oznacza znaczącą potencjalną możliwość wyrządzenia przez autonomicznie działający system sztucznej inteligencji losowo występujących szkód jednej osobie lub większej liczbie osób w taki sposób, że wykracza to poza okoliczności, jakich można by racjonalnie oczekiwać; znaczenie tego potencjału zależy od wzajemnego powiązania między powagą ewentualnej szkody, stopniem autonomiczności w podejmowaniu decyzji, prawdopodobieństwem, że zagrożenie rzeczywiście wystąpi, oraz sposobem i kontekstem użycia systemu sztucznej inteligencji[32]. Oceny, czy dany produkt stwarza poważne ryzyko czy też nie, dokonuje się na podstawie właściwej oceny ryzyka uwzględniającej charakter niebezpieczeństwa i prawdopodobieństwo jego wystąpienia[33]. Kombinacja czynników: rozmiarów szkody (krzywdy) oraz prawdopodobieństwa jej wystąpienia jako istotnych elementów definicji „ryzyka" pojawia się na gruncie wielu aktów prawnych, w szczególności posługuje się nimi krajowy ustawodawca w art. 2 pkt 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[34].

Wyrażenie „wysokie ryzyko" odnosi się do – zarówno potencjalnego, jak i rzeczywistego – wkroczenia systemów opartych o SI w sferę praw człowieka. Zastosowanie sztucznej inteligencji zarówno wówczas, gdy system ten jest przeznaczony do wykorzystania jako związany z bezpieczeństwem element produktu objętego unijnym prawodawstwem harmonizacyjnym[35], jak również

Nr 169, s. 1). Do zastosowanej w tym przepisie definicji prawodawca europejski odsyła wprost w treści art. 62 aktu w sprawie SI.

[32] Art. 3 lit. c Wniosku dotyczącego Rozporządzenia PE i Rady w sprawie odpowiedzialności za działanie systemów sztucznej inteligencji, https://www.europarl.europa.eu/doceo/document/A-9-2020-0178_PL.hrt. (dostęp: 27.12.2022 r.).

[33] Art. 19 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1020 z dnia 20 czerwca 2019 r. w sprawie nadzoru rynku i zgodności produktów.

[34] T.j. Dz.U. z 2022 r. poz. 1863.

[35] Art. 6 ust. 1 lit. a i b aktu w sprawie SI.

wtedy gdy jako produkt podlega takiej ocenie[36], zawsze stanowi ingerencję w sferę praw i wolności człowieka.

Zastosowanie systemów sztucznej inteligencji wiąże się bezpośrednio z ingerencją w prawa podstawowe. Ingerencja ta może dotyczyć każdego prawa, którego ochronę zapewnia Karta Praw Podstawowych (KPP). Skutek, jakiego prawodawca oczekuje w związku z zastosowaniem przepisów zawartych w rozporządzeniu w sprawie SI, polegać ma na „minimalizowaniu"[37] lub „łagodzeniu"[38] ryzyka dla praw podstawowych. Zastosowanie SI nie tylko zatem ingeruje w prawa podstawowe, ale także „może mieć negatywny wpływ na prawa podstawowe"[39]. Ingerencja w prawa i wolności następuje wraz z uzyskaniem przez systemy SI dostępu do danych, w szczególności danych osobowych, a także innych danych nieposiadających charakteru osobowego, do których uprawnionemu przysługują prawa wyłączne. Ingerencja w prawa podstawowe może następować niezależnie od woli i wiedzy człowieka i niezależnie od podejmowanej przez niego płaszczyzny aktywności.

[36] Unijne akty prawa wprowadzające harmonizację stosowanych we wszystkich państwach UE wymogów oraz ich zgodności w odniesieniu do niektórych produktów zostało wskazane w Załączniku nr II do Aktu w sprawie sztucznej inteligencji. Wskazano w nim 19 aktów prawnych. Są to w szczególności: Dyrektywa 2006/42/WE Parlamentu Europejskiego i Rady z dnia 17 maja 2006 r. w sprawie maszyn zmieniająca dyrektywę 95/16/WE (Dz.Urz. L Nr 157, s. 24) [uchylona rozporządzeniem w sprawie maszyn]; dyrektywa Parlamentu Europejskiego i Rady 2009/48/WE z dnia 18 czerwca 2009 r. w sprawie bezpieczeństwa zabawek (Dz.Urz. L Nr 170, s. 1); dyrektywa Parlamentu Europejskiego i Rady 2013/53/UE z dnia 20 listopada 2013 r. w sprawie rekreacyjnych jednostek pływających i skuterów wodnych i uchylająca dyrektywę 94/25/WE (Dz.Urz. L Nr 354, s. 90); rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 300/2008 z dnia 11 marca 2008 r. w sprawie wspólnych zasad w dziedzinie ochrony lotnictwa cywilnego i uchylające rozporządzenie (WE) nr 2320/2002 (Dz.Urz. L Nr 97, s. 72); rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 168/2013 z dnia 15 stycznia 2013 r. w sprawie homologacji i nadzoru rynku pojazdów dwu- lub trzykołowych oraz czterokołowców (Dz.Urz. L Nr 60, s. 52).

[37] Art. 7 ust. 2 lit. h, art. 14 ust. 2 i art. 43 ust. 6 aktu w sprawie SI.

[38] Uzasadnienie wniosku Komisji Europejskiej z dnia 21 kwietnia 2021 r., s. 8.

[39] *Ibidem*, s. 13.

6. Korelacja pomiędzy zastosowaniem systemów SI a ingerencją w prawa podstawowe

O ile nie ulega wątpliwości, że wdrożenie i zastosowanie systemów SI może przekładać się na poziom osiąganych zysków przez dostawców,operatorów (importerów i dystrybutorów) oraz użytkowników systemów SI[40], o tyle nie jest jasne, jakiego rodzaju korzyści miałyby płynąć z zastosowania SI dla obywateli państw UE wówczas, gdy korzystanie z systemów SI nie jest nakierowane na osiąganie korzyści gospodarczych. Jest bowiem truizmem podszytym naiwnością twierdzenie, że rekompensatą dla ponoszonych przez obywateli kosztów związanych w szczególności z intensywnością, częstotliwością i dolegliwością ingerencji w sferę prywatności i innych praw podstawowych obywateli stanowić miałaby rzekoma użyteczność tych systemów w życiu codziennym lub poprawa jakości życia[41]. Niezależnie zatem od oczekiwań, jakie część środowisk łączy z zastosowaniem SI[42], uzasadniona wydaje się obawa związana z prawdopodobieństwem ograniczenia albo całkowitego wyłączenia autonomii informacyjnej jednostki. Istnieje bowiem ryzyko, że człowiek, wykonując nawet proste czynności życia codziennego, będzie zdany na korzystanie z systemów SI. Zarazem utrata autonomii rozumianej jako utrata prawa do podejmowania wolnych od technologicznego nacisku decyzji odnoszących się do zakresu i sposobu uczestnictwa w globalnym obrocie danymi, bycia poddanym profilowaniu lub

[40] Zyski z SI.

[41] Parlament Europejski wskazuje, że technologie oparte na SI mogłyby i powinny poprawić jakość życia w niemal każdej sferze: od życia osobistego, obejmującego np. transport, dostosowaną do potrzeb danej osoby edukację, pomoc osobom znajdującym się w trudnej sytuacji, programy w zakresie fitnessu i przyznawanie kredytów, poprzez środowisko pracy, np. uwolnienie od uciążliwych i powtarzających się zadań, po wyzwania globalne, takie jak zmiana klimatu, opieka zdrowotna, żywienie czy logistyka (Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. z zaleceniami dla Komisji w sprawie systemu odpowiedzialności cywilnej za sztuczną inteligencję (2020/2014(INL); https://www.europarl.europa.eu/doceo/document/TA-9-2020-10-20_PL.html#sdocta9 (dostęp: 27.12.2022 r.).

[42] W pracach Europejskiego Komitetu Ekonomiczno-Społecznego wskazano, że niesie także obietnicę umożliwienia ludziom rozwoju inteligencji, jaka do tej pory nie istniała, co utoruje drogę dla nowych odkryć i pomoże rozwiązać niektóre z największych współczesnych wyzwań: od leczenia chorób przewlekłych, przewidywania wystąpienia choroby lub zmniejszenia liczby ofiar śmiertelnych w wypadkach drogowych po przeciwdziałanie zmianie klimatu lub przewidywanie zagrożeń dla cyberbezpieczeństwa.

monitorowaniu ze względu na posiadane cechy osobowości, preferencje lub predyspozycje, prowadzić może do naruszenia integralności moralnej i psychicznej.

Słusznie przyjmuje się zatem, że zasady odpowiedzialności dotyczące operatora powinny obejmować wszelkie działania systemów SI niezależnie od tego, gdzie są one realizowane i czy mają charakter fizyczny czy wirtualny. Parlament Europejski zauważa, że potencjalni poszkodowani często nie są świadomi działania systemu i często nie mieliby umów, które dawałyby im prawo do zgłaszania roszczeń wobec operatora. W momencie gdy dojdzie do szkody, osoby takie mogłyby zgłaszać tylko roszczenia na zasadzie winy, a dowiedzenie winy operatora systemu SI mogłoby okazać się trudne i tym samym odpowiednie roszczenia z tytułu odpowiedzialności spełzłyby na niczym.

Zarazem rozwój systemów sztucznej inteligencji jest możliwy tylko pod warunkiem zapewnienia dostępu do wysoko referencyjnych, dokładnych i aktualizowanych danych. Wysokiej jakości zbiory danych treningowych, walidacyjnych i testowych wymagają wdrożenia odpowiednich praktyk w zakresie zarządzania danymi. Przełomowe znaczenie dla realizowanej przez UE wizji nowej, cyfrowej rzeczywistości opartej na danych, której zasadniczy element mają stanowić systemy działające w oparciu o SI posiadało rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[43], a także rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej[44]. Komisja Europejska zauważa, że dane stały się kluczowym czynnikiem produkcji, a wartością przez nie wygenerowaną należy się podzielić z całym społeczeństwem uczestniczącym w dostarczaniu danych[45]. W konsekwencji udzielenie dostępu do danych, w szczególności

[43] Dz.Urz. UE L Nr 119, s. 1.

[44] Dz.Urz. UE L Nr 303, s. 59.

[45] Komunikat Komisji pt. „Kształtowanie cyfrowej przyszłości Europy" COM(2020) 67 final, s. 8, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52020DC0067 (dostęp: 27.12.2022 r.).

danych osobowych, utraciło charakter uprawnienia przynależnemu każdemu podmiotowi danych, a stało się jego obowiązkiem.

Zmiana zapatrywań w tym zakresie widoczna była, choć mało eksponowana w piśmiennictwie i rzadko podnoszona, w sposobie uregulowania przesłanek legalizujących przetwarzanie danych osobowych wymienionych w art. 6 ust. 1 RODO. Ustawodawca europejski postanowił, że dla ocena zgodności z prawem przetwarzanie danych osobowych nie jest konieczne wykazania istnienia zgody podmiotu danych osobowych. Każda bowiem z wymienionych w art. 6 RODO okoliczności usprawiedliwiających przetwarzanie danych osobowych ma charakter autonomiczny i niezależny oraz są one, co do zasady, równoprawne[46].

Dopiero zastosowanie instrumentów prawnych, które zachęciły do tworzenia rynku danych oraz zobligowały podmioty prawa prywatnego oraz podmioty publiczne do ich udostępniania i wykorzystania w ramach prowadzonej działalności, umożliwiło rozwój technologii opartych o systemy SI. Nakreślone wizje przyszłości w ujęciu faktycznych zastosowań zazwyczaj opisywanych w takiej perspektywie, która sygnalizuje przede wszystkim pożytki płynące z wykorzystania systemów opartych o SI[47], wywołały potrzebę wdrożenia na obszarze wszystkich państw członkowskich zharmonizowanych przepisów jednolicie regulujących zasady opracowania, wprowadzania do obrotu i wykorzystania produktów i usług opartych o sztuczną inteligencję. Zharmonizowane regulacje silnie oddziałują jednak na aktualną sytuację prawną jednostek, które wcześniej, powołując się na autonomię informacyjną i ochronę prywatności, mogły swobodnie decydować o zakresie, trybie i formie udostępniania informacji i danych. Jednolite rozwiązania dotyczące systemów SI normować będą bowiem te sytuacje faktyczne i stany, które dotychczas były wolne od działania systemów SI. Oznacza to zawężenie wolności jednostek, których profile wykreowane w oparciu o dane przetworzone w systemach SI staną się przedmiotem obrotu

[46] P. Fajgielski, *Ogólne rozporządzenie o ochronie danych*, Warszawa 2021, s. 160.

[47] Eksponuje się zatem wspólne zdolności cyfrowe; zmniejszenia kosztów realizacji szybkich sieci łączności elektronicznej; utworzenie wspólnej jednostki ds. cyberbezpieczeństwa; tworzenie jednolitego rynku w dziedzinie cyberbezpieczeństwa (Komunikat Komisji pt. „Kształtowanie cyfrowej przyszłości Europy", s. 9).

niezależnie od ich wiedzy i woli. Działanie systemów SI może w konsekwencji stanowić odczuwalną i nieusuwalną dla nich dolegliwość.

Świadomość nieuchronności istnienia powyżej wskazanych ingerencji w sferę praw podstawowych, a zarazem istnienie przekonania, popartego wynikami obserwacji odnośnie do braku odwrotu od szybkiego tempa rozwoju nowych technologii i ich zastosowań, skłoniły ustawodawcę europejskiego do zdefiniowania katalogu praktyk, których stosowanie zostało zakazane bez względu na charakter systemu SI oraz bez względu na jego funkcjonalność i przeznaczenie. Zakazy obejmują:

1/ stosowanie technik podprogowych będących poza świadomością danej osoby w celu istotnego zniekształcenia zachowania tej osoby w sposób, który powoduje lub może powodować u niej lub u innej osoby szkodę fizyczną lub psychiczną;
2/ wykorzystywanie dowolnej słabości określonej grupy osób ze względu na ich wiek, niepełnosprawność ruchową lub zaburzenie psychiczne w celu istotnego zniekształcenia zachowania osoby należącej do tej grupy w sposób, który powoduje lub może powodować u tej osoby lub u innej osoby szkodę fizyczną lub psychiczną;
3/ wykorzystywanie systemów sztucznej inteligencji przez organy publiczne lub w ich imieniu na potrzeby oceny lub klasyfikacji wiarygodności osób fizycznych prowadzonej przez określony czas na podstawie ich zachowania społecznego lub znanych bądź przewidywanych cech osobistych lub cech osobowości (punktowa ocena społeczna[48]);
4/ wykorzystywanie systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym" w przestrzeni publicznej do celów egzekwowania prawa[49].

[48] Chodzi o ocenę prowadzącą do prowadzi do krzywdzącego lub niekorzystnego traktowania niektórych osób fizycznych lub całych ich grup (art. 5 ust. 1 lit. c akt w sprawie SI).

[49] Z wyjątkiem sytuacji gdy systemy SI są ukierunkowane na poszukiwania konkretnych potencjalnych ofiar przestępstw, w tym zaginionych dzieci; zapobiegnięcia konkretnemu, poważnemu i bezpośredniemu zagrożeniu życia lub bezpieczeństwa fizycznego osób fizycznych lub atakowi terrorystycznemu; wykrywania, lokalizowania, identyfikowania lub ścigania sprawcy przestępstwa lub podejrzanego o popełnienie przestępstwa, które jest zagrożone karą co najmniej trzech lat pozbawienia wolności (art. 5 ust. 2 lit. d akt w sprawie SI).

Człowiek, wbrew pozorom, nie znajduje się w centrum zainteresowania systemów SI przetwarzających w sposób zautomatyzowany dane. Centralnym przedmiotem zainteresowania są jego emocje, predyspozycje, możliwości fizyczne i psychiczne oraz dokonywane wybory, w tym konsumenckie. Przetwarzanie danych w systemach SI następuje zatem w oderwaniu od przyrodzonych człowiekowi wartości, takich jak w szczególności godność, prywatność, kult pamięci, mir domowy. Nie są one bowiem nośnikiem wartości gospodarczych, a w konsekwencji pozostają poza zakresem poznania SI. Europejski Komitet Ekonomiczno-Społeczny zwrócił uwagę, że wiele technologii identyfikacji biometrycznej nie ma na celu jednoznacznej identyfikacji osoby, lecz jedynie ocenę zachowania lub emocji danej osoby[50]. Zastosowania te mogą nie wchodzić w zakres definicji (przetwarzania) „danych biometrycznych" tym bardziej pozostaną jednak przedmiotem obrotu z tego powodu, że stanowią wartość gospodarczą. SI jako system oparty na danych byłby bowiem bezużyteczny wówczas, gdyby przy jego tworzeniu, testowaniu i wykorzystaniu nie korzystano z danych generowanych przez człowieka, w szczególności danych osobowych jak również danych stanowiących składnik szerszej kategorii dóbr niematerialnych objętych prawami wyłącznymi[51]. Ingerowanie w sferę praw podstawowych ma charakter permanentny i jest nieuniknione oraz nieuchronnie związane z zastosowaniem systemów SI. Zasada pewności prawa, której konsekwencję stanowi zasada ochrony uzasadnionych oczekiwań wobec prawodawcy europejskiego

[50] Opinia Europejskiego Komitetu Ekonomiczno-Społecznego „Biała księga w sprawie sztucznej inteligencji – Europejskie podejście do doskonałości i *zaufania*" (*COM*(2020) 65 final), pkt 19, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52020AE1110 (dostęp: 27.12.2022 r.).

[51] E. Traple zauważa, że „zawartość danych, z których korzystają systemy SI jest bardzo zróżnicowana, mogą to być dane wyrażone słowem, obrazem, dźwiękiem, mogą dotyczyć czystych faktów i statystyk" (zob. E. Traple, *Granice eksploracji tekstów i danych na potrzeby maszynowego uczenia się przez systemy sztucznej inteligencji*, [w:] *Prawo sztucznej inteligencji i nowych technologii*, red. B. Fischer, A. Pązik, M. Świerczyński, Warszawa 2021, s. 20). Autorka ta odkreśla, że skorzystanie z danych podlegających ochronie prawa autorskiego lub baz danych chronionej prawem autorskim lub prawem *sui generis* w celu eksploracji tekstu i danych wymaga zezwolenia podmiotu uprawnionego. Zwraca zarazem uwagę, że ewentualny dostęp do w/w danych nie jest objęty wyjątkiem wskazanym w art. 4 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/790 z dnia 17 kwietnia 2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE (Dz.Urz. UE Nr 130, s. 92). Zob. *ibidem*, s. 38.

i krajowego, wymaga, by przepisy prawne były jasne i precyzyjne, a ich skutki przewidywalne, zwłaszcza wówczas, gdy pociągają one za sobą niekorzystne konsekwencje dla jednostek i przedsiębiorstw[52]. Zasada ta wyraża podstawowe założenie, iż „podmioty prawa muszą znać aktualny kształt prawa, by móc planować swoje działania w zgodzie z obowiązującym w danym momencie prawem. Zasada ta nabiera szczególnego znaczenia w odniesieniu do prawa regulującego działalność gospodarczą jednostek, gdyż prowadzenie takiej działalności zakłada planowanie «na przyszłość»"[53].Bezpieczeństwo prawne jednostki związane z pewnością prawa umożliwia więc przewidywalność działań organów państwa a także prognozowanie działań własnych. W ten sposób urzeczywistniana jest wolność jednostki, która według swoich preferencji układa swoje sprawy i przyjmuje odpowiedzialność za swoje decyzje, a także jej godność, poprzez szacunek porządku prawnego dla jednostki, jako autonomicznej, racjonalnej istoty[54].

Bezpieczeństwo prawne jednostki pozostawać może w kolizji z innymi wartościami, których realizacja wymaga wprowadzenia zmian do systemu prawnego. Jednostka ma prawo jednak oczekiwać, że regulacja prawna nie zostanie zmieniona na jej niekorzyść w sposób arbitralny. Prawodawca nie może w sposób dowolny kształtować treści obowiązujących norm, traktując je jako instrument do osiągania stale to innych celów, które sobie dowolnie wyznacza[55]. Ustawodawca może zdecydować się na zmianę prawa i wdrożenie nowego prawa, jeżeli przemawia za tym ważny interes publiczny, którego nie można wyważyć z interesem jednostki[56]. Prawodawca narusza zasadę pewności prawa wtedy, gdy jego rozstrzygnięcie jest dla jednostki zaskoczeniem. Jednostka ma prawo oczekiwać, że regulacja prawna nie zostanie zmieniona na jej niekorzyść w sposób arbitralny[57].

---

[52] Wyrok TSUE z dnia 11 czerwca 2015 r., C-98/14, *Berlington Hungary Tanácsadó És Szolgáltató Kft i in. v.. Magyar Állam*, LEX nr 1729527, pkt 77. Podobnie wyroki TSUE: CC-17/03, *VEMW i in.*, EU:C:2005:362, pkt 80 i przytoczone tam orzecznictwo; CC-347/06, *ASM Brescia*, EU:C:2008:416, pkt 69; C-362/12, *Test Claimants in the Franked Investment Income Group Litigation*, EU:C:2013:834, pkt 44.

[53] P. Ostojski, *Zasady uzasadnionych oczekiwań i pewności prawa a zmiany prawodawstwa unijnego i krajowego*, „Ius Novum" 2020, nr 2, s. 173.

[54] Z. Tabor, *Teoretyczne problemy legalności,* Katowice 1998, s. 65 i n.

[55] Wyrok TK z dnia 14 czerwca 2000 r., P 3/00, Legalis.

[56] Wyrok TK z dnia 2 marca 1993 r., K 9/92, Legalis.

[57] B. Banaszak, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2009, s. 25.

7. Wnioski

Akt o sztucznej inteligencji stanowi zwieńczenie aktywności prawotwórczej UE w dziedzinie „kształtowania cyfrowej przyszłości Europy"[58]. Komisja Europejska porównuje tworzenie Europy na miarę ery cyfrowej do kompletowanie układanki składającej się z wielu wzajemnie ze sobą powiązanych elementów; „tak jak w przypadku każdej układanki, całości obrazu nie da się zobaczyć bez połączenia ze sobą wszystkich elementów"[59]. Budowanie układanki UE rozpoczęła od rozwiązań miękkich tworzących środowisko przyjazne wdrażaniu rozwiązań technicznych i technologicznych[60] po to, by regulując kolejne obszary, w tym obejmujące dostęp i przetwarzania danych wdrożyć rozwiązania sprzyjające rozwojowi „gospodarki opartej na danych"[61], która otworzyła drogę do zastosowania systemów sztucznej inteligencji.

Potrzeba normowania sfer aktywności związanych z wdrażaniem systemów opartych na SI jest rezultatem przymusu technologicznego i presji ekonomicznej wywieranej przez gospodarki państw innych regionów świata dążących do osiągnięcia pozycji światowego lidera w sferze nowych rozwiązań, a w konsekwencji uzyskania przewagi ekonomicznej nad pozostałymi państwami[62]. Akt w sprawie sztucznej inteligencji realizuje zatem podwójne cele, jakim jest, po pierwsze, promowanie stosowania SI oraz, po drugie, minimalizowanie zagrożeń związanych z zastosowaniem SI[63].

---

[58] Komunikat Komisji pt. „Kształtowanie cyfrowej przyszłości Europy", *passim*.

[59] *Ibidem*, s. 3.

[60] Do takich regulacji zaliczyć należy w szczególności dyrektywę Parlamentu Europejskiego i Rady 2014/61/UE z dnia 15 maja 2014 r. w sprawie zmniejszenia kosztów realizacji szybkich sieci łączności elektronicznej, a także dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie bezpieczeństwa sieci i systemów informatycznych.

[61] Wniosek dotyczący rozporządzenia w sprawie europejskiego zarządzania danymi (akt w sprawie zarządzania danymi) COM(2020) 767, s. 3 i n., https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52020PC0767 (dostęp: 27.12.2022 r.).

[62] Parlament Europejski zauważa, że globalny wyścig ku sztucznej inteligencji już trwa, a UE powinna odegrać w nim czołową rolę, wykorzystując swój potencjał naukowy i technologiczny (rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. z zaleceniami dla Komisji w sprawie systemu odpowiedzialności cywilnej za sztuczną inteligencję (2020/2014(INL), pkt 4 https://www.europarl.europa.eu/doceo/document/TA-9-2020-10-20_PL.html#sdocta9, dostęp: 27.12.2022 r.).

[63] Uzasadnienie wniosku Komisji Europejskiej z dnia 21 kwietnia 2021 r., s. 1.

Potrzeba normowania aktywności operatorów systemów SI jest rezultatem świadomości prawodawcy dotyczącej nieuchronności występowania naruszeń praw człowieka. Nieprzewidywalność zakresu tych naruszeń generuje zarazem obowiązek poszukiwania nowych, adekwatnych do skali występujących zagrożeń reżimów ochrony. Prawodawca europejski zdecydował się na wykorzystanie znanych już wcześniej instrumentów ochrony. Zarazem zaproponowane rozwiązania poszerzają zakresy odpowiedzialności i zaostrzają jej rygory w stosunku do systemów SI wysokiego ryzyka. Mechanizmy te mają wzmocnić pozycję jednostek narażonych na działanie systemów SI. Nie wydaje się jednak prawdopodobne, by mogły one kompensować różnorodność i intensywność dolegliwości związanych z ingerencją SI w sferę praw osobistych.

Bibliografia

Banaszak B. (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2009.

Fajgielski P., *Ogólne rozporządzenie o ochronie danych*, Warszawa 2021.

Michalak A., *Projekt rozporządzenia Paramentu UE o odpowiedzialności cywilnej za działania sztucznej inteligencji – krok w dobrym kierunku czy niepotrzebne odstępstwo od zasad ogólnych?*, [w:] *Prawo sztucznej inteligencji i nowych technologii*, red. B. Fischer, A. Pązik, M. Świerczyński, Warszawa 2021.

Ostojski P., *Zasady uzasadnionych oczekiwań i pewności prawa a zmiany prawodawstwa unijnego i krajowego*, „Ius Novum" 2020, nr 2.

Tabor Z., *Teoretyczne problemy legalności,* Katowice 1998.

Traple E., *Granice eksploracji tekstów i danych na potrzeby maszynowego uczenia się przez systemy sztucznej inteligencji*, [w:] *Prawo sztucznej inteligencji i nowych technologii*, red. B. Fischer, A. Pązik, M. Świerczyński, Warszawa 2021.

Marek Bielecki

Ochrona dzieci przed szkodliwym i przestępczym oddziaływaniem publikacji internetowych

1. Wprowadzenie

Z uwagi na swą niedojrzałość fizyczną i psychiczną dziecko jest szczególnie narażone na różnorodne ataki, skierowane wobec jego osoby. Przestrzenią, w której dochodzi do szczególnej ingerencji w dobro małoletniego, jest Internet. Okres pandemii i związanej z tym zdalnej nauki spowodował, że czas, jaki dziecko spędza przed komputerem, znacznie się wydłużył. Z raportu Państwowego Instytutu Badawczego NASK wyłania się mało optymistyczny obraz, prezentujący zaangażowanie młodego pokolenia w wirtualną rzeczywistość, jak również stosunek do tego faktu rodziców i opiekunów prawnych[1]. Oprócz zajęć szkolnych, które pochłaniały ok. 7 godzin dziennie, nastolatki spędzają w sieci średnio 4 godziny i 50 minut dziennie. W dni wolne od nauki czas ten wydłuża się do 6 godzin i 10 minut. 11,5% badanych jest aktywnych w sieci ponad 8 godzin dziennie, a co piąty spędza przed monitorem 21,3% doby. 16,9% korzysta z Internetu po godzinie 22.00. Co piąty nastolatek przyznaje, że doświadczył przemocy w Internecie. Jako przejawy agresji w ankiecie wskazywano m.in.: wyzywanie – 29,7%, ośmieszanie – 22,8%, poniżanie – 22%, zastraszanie – 13,4%, podszywanie się pod respondenta – 11,00%, rozpowszechnianie kompromitujących materiałów – 10,2%, szantażowanie 10,5%. 48,4% badanych stwierdziło, że nie spotkało się z cyberprzemocą, a 20% udzieliło odpowiedzi, że „trudno powiedzieć" czy doświadczyło tego zjawiska. Wartym podkreślenia jest fakt, że aż 75% rodziców jest przekonanych o tym, że ich dziecko nie

[1] R. Lange (red.), *Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów*, Warszawa 2021, https://www.nask.pl/pl/raporty/raporty/4295,RAPORT-Z-BADAN-NASTOLATKI-30-2021.html (dostęp: 14.03.2022 r.).

spotkało się z przemocą w Internecie, zaś 15% przyznało się, że nie ma wiedzy w tym zakresie. Jak zauważają autorzy raportu, ten brak wiedzy dorosłych może być wynikiem ich niskiej świadomości na temat cyberzagrożeń lub brakiem własnych doświadczeń[2]. Powyższe dane jasno wskazują na fakt, że niezmiernie istotne jest zintensyfikowanie działań, mających na celu zarówno edukowanie młodego pokolenia, jak również rodziców i opiekunów prawnych.

Przedmiotem niniejszego opracowania są kwestie związane z ochroną dzieci przed szkodliwym i przestępczym oddziaływaniem publikacji internetowych. W grę wchodzą zatem treści obecne w sieci, które bezpośrednio ukierunkowane są na osobę dziecka, jak również te, z którymi dziecko może się zetknąć, a przeznaczone są dla nieograniczonej liczby odbiorców. Niektóre z czynów, jakich sprawcy dopuszczają się w cyberprzestrzeni, zostały już stypizowane i uregulowane w aktach normatywnych. Niemniej jednak należy zdawać sobie sprawę z tego, że mało która dziedzina życia rozwija się tak dynamicznie jak wirtualna rzeczywistość. W związku z tym ogromne wyzwanie ciąży na prawodawcy, aby adekwatnie reagować w zależności od pojawiania się nowych zagrożeń.

2. Relacje rodzic – dziecko

Obowiązek troski o prawa dziecka jest klauzulą powszechną, obejmującą nieograniczony zakres adresatów. Zgodnie z art. 72 ust. Konstytucji RP, Rzeczpospolita ma obowiązek zapewnić ochronę praw dziecka. Natomiast każdy ma prawo żądać od organów władzy publicznej ochrony dziecka przed przemocą, okrucieństwem, wyzyskiem i demoralizacją[3]. Zgodnie z Konwencją o prawach dziecka (KoPD), największe zadanie spoczywa na rodzicach i opiekunach prawnych, którzy ponoszą odpowiedzialność za wychowanie i rozwój dziecka. Przedmiotem ich największej troski ma być jak najlepsze zabezpieczenie interesów

[2] *Ibidem*, s. 78–80.

[3] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483 ze zm.).

dziecka (art. 18)[4]. Dobro i interesy dziecka winny być również przedmiotem działań szeroko pojmowanych władz, publicznych i prywatnych instytucji opieki społecznej oraz sądów. Wszelkie działania podejmowane przez państwo powinny zaś uwzględniać prawa i obowiązki rodziców, opiekunów prawnych oraz innych osób prawnie odpowiedzialnych za osoby nieletnie (art. 18 KoPD).

Analizując możliwości niekorzystnego oddziaływania Internetu na osobę dziecka, warto zauważyć jeszcze jeden fakt. Otóż osoba nieletnia może w niektórych sytuacjach sprzeciwiać się ograniczeniom, jakie mogą nakładać na nią rodzice. Chodzić może o przeglądanie materiałów, zawierających treści szkodliwe dla młodego człowieka, np. przemoc, pornografia itp. Powstaje w związku z tym wątpliwość, czy dziecko może negować zdanie opiekunów i żądać dostępu do Internetu. Zagadnienie owo jest związane z korelacją praw dziecka i rodziców, związanych bezpośrednio ze sprawowaniem przez tych ostatnich władzy rodzicielskiej.

Zasada konieczności kierowania się dobrem dziecka jest naczelną wartością w procesie sprawowania opieki nad jego sobą. Zwraca na to uwagę m.in. Trybunał Konstytucyjny w wyroku z 16 grudnia 2020 r., gdy podkreśla, że dobro dziecka stanowi konstytucyjną klauzulę generalną, której rekonstrukcja powinna odbywać się poprzez odwołanie do aksjologii konstytucyjnej i ogólnych założeń systemowych[5]. Ponadto jak dalej zauważa Trybunał:

> nakaz ochrony dobra dziecka stanowi podstawową, nadrzędną zasadę polskiego systemu prawnego; pojęcie „praw dziecka" w przepisach Konstytucji należy rozumieć jako nakaz zapewnienia ochrony interesów małoletniego, który w praktyce sam może jej dochodzić w bardzo ograniczonym zakresie.

Czy zatem można wbrew woli dziecka ustanawiać określone zakazy, kierując się jego dobrem? Aby udzielić odpowiedzi na tak postawione pytanie, należy rozważyć wpływ na prawa dziecka klauzuli stopnia jego dojrzałości (rozwoju), która determinuje zachowanie rodziców względem osoby nieletniej.

[4] Konwencja o prawach dziecka z dnia 20 listopada 1989 r. (Dz.U. z 1991 r. Nr 120, poz. 526).

[5] Wyrok TK z dnia 16 grudnia 2020 r., SK 26/16, OTK-A 2020, poz. 69.

W obowiązujących regulacjach prawodawca, uzależniając możliwość podejmowania przez dziecko autonomicznych decyzji, posługuje się tą kategoria wielokrotnie. W art. 48 ust. 1 Konstytucji RP przyznaje się rodzicom prawo do wychowania dzieci zgodnie z własnymi przekonaniami, zastrzega się jednocześnie, że powinno ono uwzględniać m.in. stopień dojrzałości dziecka. W art. 12 ust. 1 KoPD, nałożono na państwa – strony obowiązek zapewnienia dziecku, które jest zdolne do kształtowania własnych poglądów, prawa do ich swobodnego wyrażania we wszystkich sprawach dotyczących dziecka, przyjmując je z należytą wagą stosownie do wieku oraz jego dojrzałości. Ponadto na podstawie normy wyrażonej w Kodeksie rodzinnym i opiekuńczym (k.r.o.), rodzice przed powzięciem decyzji w ważniejszych sprawach dotyczących osoby lub majątku dziecka powinni je wysłuchać, jeżeli rozwój umysłowy, stan zdrowia i stopień dojrzałości dziecka na to pozwala, uwzględniając w miarę możliwości jego rozsądne życzenia (art. 95 § 4). Również przepisy kodeksu postępowania cywilnego (k.p.c.)[6] uzależniają możliwość dokonywania czynności prawnych w zależności od osiągnięcia przez dziecko odpowiedniego poziomu rozwoju. Zgodnie z art. 216[1] k.p.c., sąd w sprawach dotyczących osoby małoletniego dziecka wysłucha je, jeżeli jego rozwój umysłowy, stan zdrowia i stopień dojrzałości na to pozwala. Ponadto, stosownie do powyższych okoliczności, sąd uwzględni jego zdanie i rozsądne życzenia. Również na mocy art. 576 § k.p.c. sąd w sprawach dotyczących osoby lub majątku dziecka wysłucha je, uwzględniając w miarę możliwości jego rozsądne życzenia, jeżeli te trzy przesłanki zostaną spełnione.

Wzajemne korelacje pomiędzy uprawnieniami dzieci a ich rodziców i opiekunów prawnych istnieją również na płaszczyźnie prawa do prywatności. Obszar ten ściśle związany jest z problematyką podejmowaną w niniejszym opracowaniu. Według jednej z zaproponowanych w doktrynie definicji, „prywatność" w sensie szerokim oznacza możność jednostki do samodzielnego decydowania o własnym życiu i dokonywanych w nim wyborów. Sprowadza się to m.in. do wolności wyboru drogi życiowej bez jakiejkolwiek ingerencji ze

[6] Ustawa z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (t.j. Dz.U. z 2020 poz. 1575).

strony innych osób. W ujęciu wąskim zaś, prywatność utożsamiana jest z brakiem możliwości ze strony innych podmiotów do wglądu w życie jednostki[7]. Płaszczyzna potencjalnej ingerencji w prywatność jednostki jest niezmiernie szeroka i obejmuje takie wartości jak: życie rodzinne, mir domowy, dobra osobiste, integralność człowieka, ochronę danych osobowych, tajemnicę korespondencji czy sferę intymną osoby ludzkiej[8]. Zgodnie ze stanowiskiem Europejskiego Trybunału praw Człowieka (ETPCz), pojęcie to obejmuje fizyczną i psychologiczno-psychiczną integralność osoby i może odnosić się także do fizycznej i społecznej tożsamości jednostki[9].

Źródeł prawa do prywatności osoby nieletniej należy dopatrywać się zarówno na płaszczyźnie rozwiązań krajowych, jak i w obowiązujących w Polsce standardach międzynarodowych. Zgodnie z art. 47 Konstytucji RP, każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. Ponadto ustrojodawca zapewnia wolność i ochronę tajemnicy komunikowania się. Ograniczenia w tym zakresie mogą nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony (art. 49 Konstytucji RP). Oczywiście art. 31 ust. 3, zawierający katalog przesłanek warunkujących ograniczenia wszystkich praw i wolności konstytucyjnych, będzie miał również zastosowanie w tym przypadku. Przykładem regulacji odnoszących się bezpośrednio do osoby poniżej 18. roku życia są zasady zawarte w ustawie Postępowanie w sprawach nieletnich (u.p.n.)[10]. Zgodnie z art. 66 § 3 u.p.n., korespondencja nieletniego umieszczonego w ośrodku, zakładzie poprawczym lub schronisku może być kontrolowana przez dyrektora ośrodka, zakładu lub schroniska bądź przez upoważnionego przez niego pracownika pedagogicznego, wyłącznie w przypadkach powzięcia uzasadnionego podejrzenia, iż zawiera ona treści godzące

---

[7] E. Rodzik, *Prawo do prywatności dziecka a rodzicielska kontrola jego aktywności w Internecie*, [w:] *Prawo do prywatności – współczesne wyzwania*, red. M. Wiącek, Warszawa 2019, s. 147.

[8] M. Pryciak, *Prawo do prywatności*, „Studia Erasmiana Wratislaviensia" 2010, nr 4, s. 214.

[9] Wyrok ETPCz z dnia 29 kwietnia 2002 r., skarga nr 2346/02, HUDOC.

[10] Ustawa z dnia 26 października 1982 r. Postępowanie w sprawach nieletnich (t.j. Dz.U. z 2018 r. poz. 969 z późn. zm.).

w porządek prawny, bezpieczeństwo ośrodka, zakładu lub schroniska, w zasady moralności publicznej bądź może wpłynąć niekorzystnie na przebieg toczącego się postępowania lub resocjalizacji nieletniego. Wyjątek dotyczy korespondencji z organami państwowymi i samorządowymi, w szczególności z Rzecznikiem Praw Obywatelskich i z Rzecznikiem Praw Dziecka oraz organami powołanymi na podstawie ratyfikowanych w drodze ustawy przez Rzeczpospolitą Polską umów międzynarodowych dotyczących ochrony praw człowieka. Ochrona prawa do prywatności została również potwierdzona m.in. w: Powszechnej Deklaracji Praw Człowieka (art. 12)[11], Międzynarodowym Pakcie Praw Obywatelskich i Politycznych (art. 17)[12], Karcie Praw Podstawowych (art. 7)[13], czy też Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności (art. 8)[14]. Powyższe dokumenty przyznają prawo do prywatności każdej jednostce ludzkiej. Natomiast wprost do sytuacji osób nieletnich odnoszą się normy zawarte Konwencji o Prawach Dziecka. Zgodnie z art. 16, żadne dziecko nie może podlegać arbitralnej lub bezprawnej ingerencji w sferę jego życia prywatnego, rodzinnego lub domowego czy w korespondencję ani bezprawnym zamachom na jego honor i reputację. W razie naruszenia powyższych zasad dziecko ma prawo do ochrony prawnej.

Sfera ochrony prywatności dziecka dotyczy nie tylko jego rodziców i opiekunów prawnych, ale obejmuje nieograniczony zakres podmiotów, które mogą ingerować w owe uprawnienia. W jednym ze swoich orzeczeń ETPCz zajął się zagadnieniem naruszenia tego prawa poprzez treści umieszczane w Internecie. Sprawa dotyczyła dwunastoletniego chłopca zamieszkałego w Finlandii, a odnosiła się do zdarzeń, które miały miejsce w 1999 r. Za sprawą osoby dorosłej doszło do opublikowania w sieci ogłoszenia o charakterze seksualnym, które w imieniu chłopca umieszczono na jednym z profili randkowych. Pomimo

[11] Powszechna Deklaracja Praw Człowieka z dnia 10 grudnia 1948 r., https://www.unesco.pl/fileadmin/user_upload/pdf/Powszechna_Deklaracja_Praw_Czlowieka.pdf (dostęp: 5.03.2022 r.).

[12] Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (Dz.U. z 1977 r. Nr 38, poz. 167).

[13] Karta Praw Podstawowych Unii Europejskiej (Dz.Urz. UE C Nr 303, s. 1).

[14] Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności z dnia 4 listopada 1950 r. (Dz.U. z 1993 r. Nr 61, poz. 284).

ewidentnej ingerencji w sferę prywatności tegoż dziecka, tożsamość sprawcy nie mogła zostać ujawniona przez dostawcę usług internetowych, z uwagi na obowiązujące wówczas przepisy. ETPCz uznał, że na państwie spoczywał obowiązek zapewnienia praktycznej i skutecznej ochrony skarżącego. W tym celu należało wdrożyć system ochrony dziecięcych ofiar przed narażeniem na bycie celem prób zbliżania się do nich, za pośrednictwem Internetu, pedofilów. Trybunał rozważył również relacje pomiędzy swobodą wypowiedzi a ochroną prywatności osoby nieletniej. W świetle zaprezentowanego stanowiska:

> wolność wypowiedzi oraz poufność kontaktów to kwestie pierwszorzędne, a użytkownicy usług telekomunikacyjnych i internetowych muszą mieć gwarancję, iż ich własna prywatność i wolność wypowiedzi będzie poszanowana, gwarancja taka nie może być bezwzględna i musi czasami ustępować innym uzasadnionym prawnie nakazom, takim jak ochrona porządku lub zapobieganie przestępczości i ochrona praw i wolności innych [podkr. M.B.]. Nie rozstrzygając w przedmiocie pytania, czy zachowanie osoby, która umieściła łamiące prawo ogłoszenie w Internecie, może być chronione przez art. 8 i 10 Konwencji, zważywszy na naganny charakter tego zachowania, należy wskazać, iż zapewnienie ram prawnych dla pogodzenia różnych żądań, które konkurują między sobą o ochronę w tym kontekście, należy do zadań ustawodawcy. Takie ramy prawne jednakże w odnośnym czasie nie istniały, wskutek czego pozwane Państwo nie mogło wywiązać się ze swego pozytywnego obowiązku względem skarżącego[15].

Powyższe stanowisko koresponduje z regulacjami zawartymi w polskiej Konstytucji, która przewiduje, że jedną z przesłanek dla ograniczeń praw i wolności konstytucyjnych jednostki są prawa i wolności drugiej osoby (art. 31 ust. 3).

Analizując powyższe normy, należy stwierdzić, że nie można wykluczyć ewentualności, iż dziecko, powołując się na swe prawa, będzie oponować zdanie rodziców. Nie można również kategorycznie stwierdzić, że w każdej sytuacji wola rodziców będzie miała decydujące znaczenie, dlatego że sporne

[15] Wyrok ETPCz z dnia 2 grudnia 2008 r., skarga nr 2872/02, LEX nr 468377.

zagadnienia mogą być przedmiotem rozstrzygnięcia wymiaru sprawiedliwości. Kluczową kwestią jest doprecyzowania tego, w którym momencie dziecko osiąga taki stopień rozwoju, iż może samodzielnie podejmować decyzje dotyczące swojej osoby. W psychologii rozwojowej nie ma co do tego zagadnienia jednomyślności. Według Jeana Piageta, w okresie między 11 a 12 rokiem życia dziecko staje się wrażliwe na bodźce moralne[16]. Potrafi dokonać w oparciu o własne doświadczenie analizy sytuacji, w której się znajdzie, poprzez wyciągniecie właściwego wniosku z istniejących przesłanek. Z kolei Coleman i Hendri stwierdzili, że mimo trudności z ustaleniem jaki procent młodzieży i w jakim wieku osiąga kolejne etapy rozwoju poznawczego, nie ma wątpliwości, że przed ukończeniem 16. roku życia wciąż mniejsza część populacji przekracza próg najbardziej zaawansowanego poziomu myślenia formalnego[17]. Na gruncie rozwiązań normatywnych możemy również wskazać granice temporalne, po przekroczeniu których prawodawca uznaje skuteczność woli wyrażonej przez osobę nieletnią. Z uwagi na to, że zagadnienie to jest już szeroko opisywane w literaturze przedmiotu, należy stwierdzić, że wiek ten waha się między 13 a 16 rokiem życia[18]. W polskich realiach wiele rozwiązań normatywnych daje rodzicom narzędzie do tego, aby wiążąco wpływać na zachowanie swoich dzieci. Przykładem jest chociażby cytowany już art. 48 ust. 1, który przyznaje im prawo do wychowania dziecka zgodnie z ich przekonaniami. Kodeks rodzinny i opiekuńczy stanowi, że dziecko pozostające pod władzą rodzicielską winno okazywać rodzicom posłuszeństwo (art. 95 § 2 k.r.o.). Klauzula dobra dziecka, uwzględniana nawet wbrew woli osoby małoletniej, powinna być decydująca przy poodejmowaniu określonych decyzji. Jak zauważa bowiem Sąd Najwyższy:

---

[16] M. Magda, *Wrażliwość moralna a rozwój moralny człowieka*, „Wychowanie Na Co Dzień" 2000, nr 1, s. 12.

[17] P.E. Brynat, A.M. Coleman, *Psychologia rozwojowa*, Poznań 1997, s. 101.

[18] M. Bielecki, *Ochrona rodziny i życia rodzinnego w kontekście wychowywania zgodnie z przekonaniami rodziców*, Warszawa 2020 – i wskazana tam literatura – https://iws.gov.pl/wp-content/uploads/2020/11/IWS_Bielecki-M._Ochrona-rodziny-i-%C5%BCycia-rodzinnego-w-kontek%C5%9Bcie-wychowywania-zgodnie-z-przekonaniami-rodzic%C3%B3w.pdf (dostęp: 15.03.2022 r.).

> Wprawdzie podstawowym założeniem naszego prawa rodzinnego jest dążenie do realizacji w każdej sprawie dobra małoletniego dziecka, ale założenia tego nie można rozumieć w ten sposób, że eliminuje ono całkowicie, jako jedną z przesłanek rozstrzygania spraw z zakresu stosunków między rodzicami a dziećmi, interes rodziców. Założenie to oznacza tylko, że interes rodziców nie może być decydujący dla rozstrzygnięcia sprawy w takiej sytuacji, gdy nieuwzględnienie tego interesu jest warunkiem *sine qua non* zapewnienia ochrony interesu małoletniego dziecka. Jeżeli natomiast ochrona dobra dziecka da się pogodzić – nawet przy założeniu, że rozstrzygnięcie spowoduje pewne przejściowe ujemne skutki dla dziecka – z interesem rodziców, to sąd nie może tego ostatniego interesu nie wziąć pod uwagę[19].

Interesem rodziców w sytuacjach, gdy ingerują w prywatność swoich dzieci, będzie obowiązek troszczenia się o ich fizyczny i duchowy rozwój (art. 96 § 1 k.r.o.). Rodzic, podejmując konkretne działania ingerujące w sferę osobistą dziecka, bardzo rzadko będzie rozważać kwestię czy osiągnęło ono wymagany stopień rozwoju, jeżeli w jego przekonaniu może być zagrożone dobro małoletniej osoby. Z uwagi na to, że jest to bardzo delikatna sfera relacji pomiędzy dzieckiem a jego rodzicami, osobiście opowiadam się za przyznaniem tym ostatnim możliwości wyegzekwowania swej woli. Ewentualna opcja zanegowania zdania rodziców powinna być brana pod uwagę w wyjątkowych sytuacjach, gdy ingerowanie w prawa dziecka jest oczywiście bezzasadne. Naczelny Sąd Administracyjny w jednym ze swoich orzeczeń podkreślił fakt, że:

> […] art. 72 ust. 3 Konstytucji RP zobowiązuje do uwzględnienia zdania dziecka jedynie w miarę możliwości, a przepis art. 12 ust. 1 Konwencji o prawach dziecka przewiduje wysłuchanie dziecka, o ile jest ono zdolne do kształtowania własnych poglądów, a ocena wagi wypowiedzi musi odbywać się z uwzględnieniem wieku i dojrzałości dziecka. Oznacza to, że obowiązek wysłuchania przez organy stanowiska dziecka czy to wyrażonego bezpośrednio przez małoletniego, czy przez jego przedstawiciela, nie ma skutku

[19] Wyrok SN z dnia 5 maja 2000 r., II CKN 765/00, LEX nr 51981.

w postaci obowiązku każdorazowego uwzględnienia tego stanowiska w toku wydawania rozstrzygnięcia"[20].

3. Identyfikacja zagrożeń

Zarówno w literaturze przedmiotu, dotyczącej oddziaływania Internetu na osoby nieletnie, jak również w dokumentach o charakterze normatywnym dokonano identyfikacji zagrożeń, jakie mogą mieć miejsce. Należy jednakże mieć świadomość, że wirtualna rzeczywistość jest niezwykle dynamiczna i katalog negatywnych oddziaływań na dziecko może bardzo szybko ulec zmianie. Dla ustalenia w miarę aktualnego wykazu negatywnych praktyk stosowanych w sieci bardzo pomocne okazało się opracowanie przygotowane w ramach działalności Polskiego Centrum Programu Safer Internet[21].

Co jakiś czas do wiadomości opinii publicznej dociera informacja o targnięciu się na własne życie przez dziecko, a które zostało spowodowane poprzez treści zamieszczone w Internecie. Jak alarmują psychologowie, stany depresyjne doprowadzające do samobójstw wśród nieletnich, wynikają z tego, iż w okresie pandemii całe życie dziecka – szkolne i towarzyskie – toczy się w systemie online. Dzieci przyzwyczaiły się już do tego, że funkcjonując na różnego rodzaju portalach społecznościowych, „nagrodę" za swą aktywność otrzymują bardzo szybko. Jednakże kiedy spotykają się z krytyką, równie szybko się załamują[22]. W literaturze przedmiotu zjawisko to określa się mianem FOMO (ang. *fear of missing out*). Definiuje się je zaś jako uczucie lęku lub niepokoju przed wykluczeniem z jakiejś społeczności lub pominięciem[23]. W czasie nauki online również bardzo często dochodzi do przemocy rówieśniczej. Trudniej radzą sobie te

[20] Wyrok NSA z dnia 29 sierpnia 2018 r., II OSK 1041/18, LEX nr 2553581.

[21] *Bezpieczeństwo dzieci i młodzieży online. Kompendium dla rodziców i profesjonalistów*, red. A. Rywczyńska, Sz. Wójcik, Warszawa 2018, *passim*.

[22] J. Ćwirek, K. Kowalska, *Coraz więcej dzieci odbiera sobie życie. Najmłodsze miało osiem lat*, https://www.rp.pl/spoleczenstwo/art240171-coraz-wiecej-dzieci-odbiera-sobie-zycie-najmlodsze-mialo-osiem-lat (dostęp: 18.03.2022 r.).

[23] A. Jankiewicz, A. Kuszner, A. Maj, A. Nawarenko, *Nadużywanie internetu*, [w:] *Bezpieczeństwo dzieci i młodzieży online…*, s. 34.

dzieci, którym brakuje wsparcia w domu rodzinnym. Według danych Komendy Głównej Policji w 2020 r. na własne życie targnęło się 116 osób poniżej 18. roku życia. Wśród nich było ośmioletnie dziecko. Jest to wzrost na poziomie ok. 20% w stosunku do trzech poprzednich lat[24]. W chwili obecnej przekazy internetowe, również te, z których korzysta młodzież i dzieci, zdominowane są tematem wojny na Ukrainie. Stan ciągłego zagrożenia, podsycany sztucznie tworzonymi informacjami, wzmaga stany depresyjne wśród najmłodszych. Popularny serwis internetowy TikTok stał się obecnie formą przekazywania informacji o wojnie całemu światu przez młodych Ukraińców. Platforma znana w głównej mierze z rozrywkowych filmików stała się sposobem na rozładowanie emocji. Zdarzają się jednakże preparowane fejki oraz scamy, wobec których należy zachować szczególną ostrożność[25].

Negatywne oddziaływanie na psychikę młodego człowieka, mogą mieć również inne niebezpieczne treści zamieszczone w sieci. W literaturze przedmiotu wyodrębnia się te, które najczęściej mają miejsce[26]. Wśród stosowanych praktyk wymienia się m.in.:

1/ umożliwienie dzieciom łatwego dostępu do treści pornograficznych, bez żadnego ostrzeżenia i zabezpieczeń;
2/ emitowanie treści obrazujących przemoc, obrażenia fizyczne czy okrucieństwo wobec zwierząt;
3/ zamieszczanie materiałów nawołujących do samookaleczeń, samobójstw oraz zachowań szkodliwych dla zdrowia;
4/ propagowanie treści dyskryminacyjnych, nawołujących do wrogości i nienawiści wobec różnych grup społecznych lub jednostek[27].

---

[24] J. Ćwirek, K. Kowalska, *Coraz więcej dzieci odbiera sobie życie. Najmłodsze miało osiem lat*, https://www.rp.pl/spoleczenstwo/art240171-coraz-wiecej-dzieci-odbiera-sobie-zycie-najmlodsze-mialo-osiem-lat (dostęp: 18.03.2022 r.).

[25] B. Godziński, *TikToki z frontu. Ukraińcy pokazują, jak wygląda ich codzienność na wojnie*, https://spidersweb.pl/rozrywka/2022/02/28/tiktok-wojna-ukraina-rosja-relacje-filmiki (dostęp: 18.03.2022 r.).

[26] A. Borkowska, O. Chojnacka, A. Kwaśnik i in., *Niebezpieczne treści*, [w:] *Bezpieczeństwo dzieci i młodzieży online*…, s. 39.

[27] *Ibidem*.

Ponadto dość częstym zjawiskiem wśród młodych osób jest *seksting*, który polega na przesyłaniu za pośrednictwem sieci lub publikowaniu online osobistych materiałów o charakterze erotycznym lub pornograficznym[28]. Jak wskazują autorzy raportu przygotowanego na zlecenie Fundacji Dzieci Niczyje, praktyki te są popularne z powodu chęci rozrywki, początku fascynacji seksem, zainteresowania płcią przeciwną, braku doświadczenia, ciekawości czy nieśmiałości. Co symptomatyczne, konsekwencje tego zjawiska mogą być bardzo poważne. Z pozoru niewinne zachowanie, polegające na przesłaniu znajomemu zdjęcia, stało się powodem wykorzystywania, żartów, ośmieszania czy zemsty. Bardzo często praktykom tym towarzyszy szantaż, mający u osoby poszkodowanej wymóc określone zachowanie[29]. Zjawisko to, w literaturze przedmiotu określane jest mianem *Sextortion* (szantaż emocjonalny). Formułowane żądania sprowadzają się do wymuszania pieniędzy. Najczęściej formułowane groźby dotyczą problemów w pracy i w szkole. Niekiedy zaś sprawca żąda świadczeń seksualnych ze strony ofiary[30].

Dość częstą praktyką występującą w wirtualnej rzeczywistości jest *grooming*, sprowadzający się do uwodzenia dzieci przez dorosłych. Dotyczy on zachowania sprawcy, który roztacza pozorną opiekę nad dzieckiem, by z czasem nakłonić je do relacji seksualnych. Niezdrowe relacje pomiędzy dorosłymi a dzieckiem stały się przedmiotem zainteresowania opinii publicznej w latach 70. XX w. Rozpowszechnienie dostępu do Internetu otworzyło przed przestępcami nowe możliwości[31]. W świetle badań przeprowadzonych przez EU Kids Online z 2018 r., na pytanie dotyczące tego, czy w ostatnim roku otrzymałaś/eś

[28] J. Uliasz, *Prawna ochrona prywatności oraz wolności dzieci w Internecie*, „Zeszyty Naukowe Uniwersytetu Rzeszowskiego" 2020, z. 110, s. 286.

[29] K. Makaruk, Sz. Wójcik, *Seksting wśród polskiej młodzieży. Wyniki badania ilościowego*, Warszawa 2014, s. 4. https://fdds.pl/_Resources/Persistent/c/c/8/f/cc8fee410093693294ae8b7fbf39b2c0d9322b41/Wojcik_Makaruk_Seksting_wsrod_polskiej_mlodziezy.pdf (dostęp: 22.03.2022 r.).

[30] A. Kwaśnik, Z. Polak, O. Chojnacka, M. Różycka, M. Marańda, *Ryzykowne zachowana seksualne i seksualizacja młodych użytkowników Internetu. Zarys Problematyki*, Warszawa 2019, s. 20–22.

[31] M. Dabrowska, *Grooming – wybrane aspekty prawnokarne i kryminologiczne*, Warszawa 2018, s. 12–13.

jakiekolwiek wiadomości związane z seksem, odpowiedzi przedstawiały się dla odpowiednich grup wiekowych w następujący sposób:

1/ 11–12 lat – 5,4% chłopców i 1,1% dziewczynek,

2/ 13–14 lat – 12% chłopców i 9% dziewcząt,

3/ 15–17 lat – 24% chłopców i 23% dziewcząt[32].

Większość użytkowników Internetu, w tym również osoby nieletnie, padają ofiarą działań marketingowych mających na celu wyłudzenie danych osobowych i naruszenie prywatności. Podatne na sugestię dzieci, zalewane są różnorodnymi ofertami handlowymi, które często kończą się zakupem drogich i niepotrzebnych towarów. Wyłudzenie danych najczęściej związane jest z instalowaniem złośliwego oprogramowania na urządzeniach mobilnych. W badaniach przeprowadzonych przez EU Kids, aż 20% respondentów wskazało, że w ciągu roku miało kontakt z tego typu nadużyciami. 9% respondentów wskazało, że ich dane są wykorzystywane w sposób niezgodny z ich intencją. 70% badanych nie zadeklarowało jednoznacznie czy miało do czynienia z powyższymi zagrożeniami. Wynikać to może z braku wiedzy na temat praktyk, których dopuszczają się sprawcy albo z coraz doskonalszych metod pozyskiwania danych. Jak wskazują autorzy raportu, udział osób, które doświadczyły zagrożeń prywatności i oszustw internetowych, wzrasta wraz z wiekiem. Wyniki przedstawiają się następująco: ok. 20% dzieci do 10. roku życia, 26% osób w wieku 11–12 lat, 35% nastolatków w wieku 13–14 lat i 39% najstarszych respondentów, doświadczyło naruszenia prywatności w Internecie[33].

Nierzadko niepożądanych praktyk wobec dziecka dopuszczają się nieświadomi tego rodzice bądź opiekunowie prawni. Związane jest to ze sferą prywatności dziecka i w literaturze przedmiotu określane jest mianem *sharentingu* albo *parental trollingu*[34].

Termin *sharenting* pochodzi z połączenia dwóch angielskich słów *parenting* – rodzicielstwo oraz *sharing*, oznaczający czynność rozpowszechniania. Zjawisko to polega na zaangażowaniu się rodziców w mediach społecznościowych,

---

[32] J. Pyżalski. A. Zdrodowska, Ł. Tomczyk, K. Abramczuk, *Polskie badania EU Kids Online 2018 r. Najważniejsze wyniki i wnioski*, Poznań 2019, s. 146.

[33] *Ibidem*, s. 83.

[34] J. Uliasz, *op. cit.*, s. 287.

objawiające się regularnym zamieszczaniem szczegółowych informacji o swoich dzieciach. Jak zauważa P. Forma, *shareting* jest zjawiskiem masowym. Powołując się na badania przeprowadzone na Uniwersytecie Michigan, podkreśla, że 74% respondentów wskazało, iż ich znajomi rodzice udostępniają w Internecie zbyt wiele informacji na temat swoich dzieci. Niepokój budzi jednakże okoliczność, że większość rodziców nie dostrzega zagrożeń wynikających z udostępniania informacji o swoich dzieciach i o swoich rolach rodzicielskich[35]. Aktywność rodziców bardzo często zaczyna się jeszcze przed narodzeniem dziecka, kiedy to w sieci pojawiają się zdjęcia z badań prenatalnych. Radość z narodzin dziecka łączy się z brakiem zdroworozsądkowego podejścia i może doprowadzić do niepożądanych sytuacji.

Parental trolling to zachowanie rodziców, polegające na wykorzystaniu wizerunku swojego dziecka, utrwalonego w sytuacjach kompromitujących lub ośmieszających osobę nieletnią. W celu publikacji zdjęcia wykorzystywany jest Internet, co ma skutkować zdobyciem „popularności" przez rodziców[36]. W dniu 25 stycznia 2016 r. Sąd Okręgowy Warszawa-Praga w Warszawie skazał ojca na 3 miesiące ograniczenia wolności za publikację nagiego wizerunku syna[37].

Większość z prezentowanych zachowań doczekała się penalizacji ze strony prawodawcy, oraz stygmatyzacji w działaniach organów krajowych i międzynarodowych. Identyfikacja zagrożeń, jakie mogą spotkać osobę nieletnią w cyberprzestrzeni, dokonuje się również za sprawą działalności Komitetu Praw Dziecka (ang. *Committee on the Rights of the Child* – CRC). Jest to organ monitorujący wypełnienie przez państwa postanowień Konwencji o Prawach Dziecka. Państwa, które ratyfikowały KoPD, zobowiązały się do przysyłania Komitetowi raportów opisujących wprowadzenie Konwencji w życie. Komitet dokonuje również wykładni treści klauzul prawnych z zakresu praw człowieka

---

[35] P. Forma, *Sharenting, czyli internetowa wizualizacja życia rodzinnego* (*prezentacja*), https://www.scdn.pl/images/stories/projekty/chmura19/SHARENTING.pdf (dostęp: 22.03.2022 r.).

[36] A. Drapała, *Parental trolling w świetle uregulowań polskiej ustawy karnej*, „Problemy Prawa Prywatnego Międzynarodowego" 2018, nr 23, s. 79–80.

[37] Wyrok SO Warszawa-Praga w Warszawie z dnia 25 stycznia 2016 r., VI Ka 1206/16. niepubl.; szerzej na ten temat: M. Pająk, F. Sztandera, *Wybrane aspekty parental trollingu w sieci Internet*, „Problemy Nauk Prawnych" 2019, t. 12, s. 27–38.

pod względem merytorycznym i metodologicznym. Wykładnia ta jest publikowana w postaci Ogólnych Komentarzy i Ogólnych Zaleceń[38]. W Komentarzu Ogólnym nr 7 z 2005 r. CRC zwraca uwagę na to, że szczególne problemy wiążą się z szybkim wzrostem różnorodności i dostępności nowoczesnych rozwiązań technicznych m.in. tych, które wykorzystują Internet. Na oddziaływanie nieodpowiednich i drastycznych treści szczególnie narażone są małe dzieci (pkt 35)[39]. Komentarz nr 13 z 2011 r. dotyczy praktyk polegających na stosowaniu przemocy wobec dzieci[40]. Niedozwoloną praktyką, stosowaną wobec niepełnoletnich, jest przemoc psychiczna, określana jako psychiczne maltretowanie, nadużycia psychiczne, nadużycia słowne oraz emocjonalne, która dokonuje się przez technologie informacyjne i komunikacyjne (pkt 21). W świetle dokumentu zagrożenia związane z ochroną dzieci przed szkodliwym oddziaływaniem technologii informacyjno-komunikacyjnych obejmuje następujące obszary:

1/ wykorzystywanie dzieci na tle seksualnym poprzez przedstawianie obrazów dzieci w wersji audio–video udostępnianych w Internecie i innych narzędziach;
2/ produkowanie, tworzenie, zezwalanie na robienie, dystrybuowanie, pokazywanie, posiadanie lub reklamowanie niemoralnych zdjęć lub filmów video z dziećmi;
3/ prezentowania dzieciom szkodliwych informacji w postaci: reklam, spamu, materiałów sponsorowanych, informacji osobistych, treści przepełnionych przemocą, nienawiścią, stereotypami, rasizmem, pornografią, materiałów wprowadzających w błąd;
4/ wyszydzanie, dręczenie , prześladowane, przymuszane, oszukiwanie lub zachęcanie do spotkań z obcymi poza Internetem;

---

[38] Komitet Praw Dziecka (ang. *Committee on the Rights of the Child*, CRC), http://www.unic.un.org.pl/dyskryminacja/ct_crc.php (dostęp: 22.03.2022 r.).

[39] Komitet Praw Dziecka. Czterdziesta Sesja Genewa 12–30 września 2005 r. Komentarz Ogólny nr 7 (2005). *Realizacja praw dziecka w okresie wczesnego dzieciństwa*, [w:] *Prawa dziecka. Dokumenty Organizacji Narodów Zjednoczonych. Zbiór i opracowanie*, red. P.J. Jaros, M. Michalak, Warszawa 2015, s. 505.

[40] Komitet Praw Dziecka. Komentarz Ogólny nr 13 (2011). *Prawo dziecka do wolności od wszelkich form przemocy*, [w:] *Prawa dziecka*.., s. 639–680.

5/ wyszukiwane dzieci w celach angażowania ich w czynności seksualne oraz/lub dostarczanie im informacji o charakterze osobistym obejmujące szkodliwe treści;
6/ Zachęcanie do uprawiania hazardu, włamywania się do komputerów, wyłudzania pieniędzy oraz/lub angażowanie nieletnich w terroryzm (pkt 31).

Komentarz Ogólny nr 16 z 2013 r., porusza problem seksualnego wykorzystywania osób nieletnich[41]. Podkreśla się tu m.in., że dzieci mogą stać się ofiarami przemocy takiej jak: zastraszanie w sieci, handel lub wykorzystywanie seksualne, turystyka seksualna czy pornografia dziecięca. W związku z tym zaleca się państwom, aby prowadziły działania skoordynowane z przemysłem technologii informacyjnej i komunikacyjnej. Ponadto na poziomie centralnym należy stworzyć regulacje służące ochronie dzieci przed przemocą i materiałami zawierającymi niestosowną treść (pkt 60).

Szkodliwy wpływ gier komputerowych na psychikę nieletnich podkreśla CRC w Komentarzu Ogólnym nr 17. Stwierdza się tam m.in., że coraz większe zainteresowanie grami komputerowymi pełnymi przemocy, szczególnie ze strony chłopców, zdaje się wiązać z ich agresywnym zachowaniem. Dzieje się tak dlatego, że długotrwałe zaangażowanie w grę tworzy silną interakcję i wzmacnia negatywne bodźce, co może prowadzić do osłabienia wrażliwości na ból i cierpienie innych (pkt 46).

O szkodliwym wpływie jaki mogą wywierać na osobę nieletnią treści zamieszczane w Internecie, wspomina się również w rezolucji Parlamentu Europejskiego z dnia 20 listopada 2012 r.[42] W dokumencie podkreśla się fakt, że Internet stanowi zagrożenie dla dzieci ze względu na zjawiska takie jak pornografia dziecięca, wymiana materiałów przedstawiających przemoc, cyberprzestępczość, zastraszanie, terroryzowanie, uwodzenie, możliwość dostępu do towarów i usług lub zakupu przez dzieci takich produktów, które są prawnie

[41] Komitet Praw Dziecka. Sześćdziesiąta Druga Sesja. Genewa 14 stycznia – 1 lutego 2013. *Komentarz Ogólny nr 16* (*2013*) *dotyczący zobowiązań Państw – Stron w zakresie wpływu sektora biznesowego na prawa dzieci*, [w:] *Prawa dziecka*…, s. 737–764.

[42] Rezolucja Parlamentu Europejskiego z dnia 20 listopada 2012 r. w sprawie ochrony dzieci w świecie cyfrowym – 2012/2068(INI) (Dz.Urz. UE C Nr 419, s. 33).

ograniczone lub niestosowne do wieku, kontakt z reklamami niestosownymi do wieku, agresywnymi lub wprowadzającymi w błąd, ryzyko wyłudzenia pieniędzy, kradzieży tożsamości, oszustw i podobnych zagrożeń dotyczących finansów, które mogą stać się traumatycznym doświadczeniem (pkt 13).

Powyższy katalog zagrożeń, które mogą napotkać dziecko w Internecie, z całą pewnością nie jest kompletny. Wirtualna rzeczywistość przyjmuje wszystkie zachowania, które mają miejsce w realnym świecie Dlatego też istnieje wiele płaszczyzn, na których może dojść do ingerencji w dobro dziecka. Znaczna część zidentyfikowanych praktyk dotyczy sfery seksualnej jednostki. Niemniej jednak bardzo trudno jest przeciwdziałać działalności podmiotów, które z cyberprzestrzeni uczyniły swoje źródła dochodów. Lobby reprezentujące producentów filmów porno jest bardzo silne i pod pozorem swobód gospodarczych, stara się torpedować wszelkie formy ograniczeń. Dlatego tak ważne jest, aby zapewnić systemową opiekę psychologiczną na poziomie każdej placówki edukacyjnej. Z aprobatą należy odnotować fakt, że na skutek licznych postulatów kierowanych przez organizacje pozarządowe, jak również w oparciu o stały monitoring sytuacji panującej w polskich szkołach, 11 marca 2021 r. Ministerstwo Edukacji i Nauki przyjęło program wsparcia psychologiczno-pedagogicznego uczniów i nauczycieli. Jako powód jego wprowadzenia podano fakt, że wskutek zdalnej nauki uczniowie stali się zmęczeni, apatyczni, odizolowani od bezpośrednich kontaktów rówieśniczych. Skutkuje to trudnościami w nauce, a także wzrostem zachowań ryzykownych[43]. Wypada mieć tylko nadzieje, że efekty powyższych działań przyniosą wymierne efekty i poprawią kondycję polskich uczniów.

4. Gwarancje formalne

Ochrona normatywna dziecka przed szkodliwym oddziaływaniem publikacji internetowych dokonuje się na wielu płaszczyznach, obejmując swym zakresem zarówno regulacje krajowe jak i międzynarodowe. Ponadto istotną rolę

[43] *Program wsparcia psychologiczno-pedagogicznego dla uczniów i nauczycieli w pandemii*, https://www.gov.pl/web/edukacja-i-nauka/program-wsparcia-psychologiczno-pedagogicznego-dla-uczniow-i-nauczycieli-w-pandemii (dostęp: 18.03.2022 r.).

w egzekwowaniu praw przysługujących osobom nieletnim odgrywa wymiar sprawiedliwości. Na wstępie należy zaznaczyć, że w obrębie aktów normatywnych o zasięgu międzynarodowym mieszczą się zarówno rozwiązania o charakterze uniwersalnym jak i regionalnym. Z racji konieczności aplikowania rozwiązań międzynarodowych do krajowego systemu prawnego, istnieje ścisła koherencja pomiędzy istniejącymi regulacjami. Znaczna ich część związana jest ze sferą seksualności młodego człowieka. Dominuje w nich zjawisko dziecięcej pornografii, ale także regulowane są inne formy negatywnego oddziaływania na integralność cielesną i duchową małoletnich.

Konwencja o Prawach Dziecka, która stanowi punkt odniesienia dla wszelkich rozwiązań normatywnych, regulujących sytuację osób nieletnich, nie zawiera w swej treść reguł, które wprost nawiązywałyby do publikacji zamieszczanych w Internecie. Niemniej jednak zawarte w niej rozwiązania mogą mieć bezpośredni związek z tą sferą aktywności dziecka. Podstawowym celem KoPD jest ochrona dziecka, co wyraża art. 3 ust. 1, który stanowi, że we wszystkich działaniach dotyczących dzieci, podejmowanych przez publiczne lub prywatne instytucje opieki społecznej, sądy, władze administracyjne lub ciała ustawodawcze, sprawą nadrzędną jest najlepsze zabezpieczenie interesów dziecka. Dla ochrony prawidłowego rozwoju dzieci w art. 19 KPD państwa-strony zobowiązują się podejmować wszelkie właściwe kroki w dziedzinie ustawodawczej, administracyjnej, społecznej oraz wychowawczej dla ochrony dziecka przed wszelkimi formami przemocy fizycznej bądź psychicznej, krzywdy lub zaniedbania bądź złego traktowania lub wyzysku, w tym wykorzystywania w celach seksualnych. Z kolei w art. 34 KPD już wyraźnie zobowiązuje do ochrony dzieci przed wszelkimi formami wyzysku seksualnego i nadużyć seksualnych[44]. W dniu 25 maja 2000 r., został przyjęty Protokół fakultatywny do KoPD w sprawie handlu dziećmi, dziecięcej prostytucji i dziecięcej pornografii[45]. W świetle dokumentu dziecięca

[44] Szerzej na ten temat: P. Mostowik, *Kwestia regulacji dostępu dzieci do internetowej pornografii na tle prawa międzynarodowego i unijnego. Uwagi na tle niekontynuowanej inicjatywy legislacyjnej*, s. 30 (maszynopis w posiadaniu autora).

[45] Protokół Fakultatywny do Konwencji o prawach dziecka w sprawie handlu dziećmi, dziecięcej prostytucji i dziecięcej pornografii, przyjęty w Nowym Jorku dnia 25 maja 2000 r. (Dz.U. z 2007 r. Nr 76, poz. 494).

pornografia oznacza jakiekolwiek pokazywanie za pomocą dowolnych środków, dziecka uczestniczącego w rzeczywistych lub symulowanych ewidentnie czynnościach seksualnych lub też jakiekolwiek pokazywanie organów płciowych w celach przede wszystkim seksualnych (art. 2 lit. c). Państwa, które podpisały Protokół, zobowiązały się objąć swoim prawem kryminalnym praktyki polegające m.in. na: produkcji, dystrybucji, rozpowszechnianiu, imporcie, eksporcie, oferowaniu, handlu lub posiadaniu materiałów zawierających dziecięcą pornografię (art. 3 ust. 1 lit. c).

Społeczność międzynarodowa podejmowała szereg inicjatyw o różnym charakterze, mających na celu ochronę dzieci przed różnymi formami seksualnego wykorzystywania[46]. Część z przyjętych rozwiązań dotyka problemu szkodliwego oddziaływania Internetu na fizyczny i emocjonalny rozwój dziecka. W Konwencji Rady Europy z dnia 23 listopada 2001 r. o cyberprzestępczości, dużo uwagi poświęcono zjawisku pornografii dziecięcej. Państwa – strony zostały zobowiązane do podjęcia odpowiednich środków prawnych, aby objąć karalnością czyny polegające na: produkowaniu pornografii dziecięcej dla celów jej rozpowszechniania za pomocą systemu informatycznego; oferowaniu lub udostępnianiu pornografii dziecięcej za pomocą systemu informatycznego; rozpowszechnianiu lub transmitowaniu pornografii dziecięcej za pomocą systemu

[46] Plan Działań przyjęty na trzecim Szczycie Głów Państw i Rządów Rady Europy (Warszawa, dnia 16–17 maja 2005 r.) wzywający do opracowania środków mających na celu zwalczanie seksualnego wykorzystywania dzieci; Rekomendacja Komitetu Ministrów Nr R (91) 11 w sprawie seksualnego wykorzystywania, pornografii, prostytucji oraz handlu dziećmi i młodzieżą, Rekomendacja (2001) 16 w sprawie ochrony dzieci przed seksualnym wykorzystywaniem, Konwencja Rady Europy o cyberprzestępczości (ETS Nr 185), a zwłaszcza jej art. 9, a także Konwencję Rady Europy w sprawie działań przeciwko handlowi ludźmi (ETS Nr 197); Deklaracja Sztokholmska i Agenda Działania, przyjęte na I Światowym Kongresie przeciwko Seksualnemu Wykorzystywaniu Dzieci w Celach Komercyjnych (27–31 sierpnia 1996 r.), Globalne Porozumienie przyjęte na II Światowym Kongresie przeciwko Seksualnemu Wykorzystywaniu Dzieci w Celach Komercyjnych w Jokohamie (17–20 grudnia 2001 r.), Porozumienie Budapeszteńskie i Plan Działania przyjęte na Konferencji przygotowawczej do II Światowego Kongresu przeciwko Seksualnemu Wykorzystywaniu Dzieci w Celach Komercyjnych (20–21 listopada 2001 r.), Rezolucję Zgromadzenia Ogólnego Organizacji Narodów Zjednoczonych S-27/2 „Świat pasujący do dzieci" oraz trzyletni program „Budowanie Europy dla dzieci i z dziećmi", przyjęty w efekcie trzeciego Szczytu i zapoczątkowany Konferencją w Monako (4–5 kwietnia 2006 r.) – Preambuła do Konwencji Rady Europy o ochronie dzieci przed seksualnym wykorzystywaniem i niegodziwym traktowaniem w celach seksualnych, sporządzona w Lanzarote dnia 25 października 2007 r. (Dz.U. z 2015 r. poz. 608).

informatycznego; pozyskiwaniu pornografii dziecięcej za pomocą systemu informatycznego dla siebie lub innej osoby oraz posiadaniu pornografii dziecięcej w ramach systemu informatycznego lub na środkach do przechowywania danych informatycznych.

Podobna problematyka została również uregulowana w przyjętej w dniu 25 października 2007 r., Konwencji Rady Europy o ochronie dzieci przed seksualnym wykorzystywaniem i niegodziwym traktowaniem w celach seksualnych. Niektóre z stypizowanych w niej czynów mogą mieć związek z aktywnością osoby nieletniej w Internecie. Na państwa – strony został nałożony obowiązek przyjęcia koniecznych środków ustawodawczych w celu zapewnienia karalności zachowania umyślnego, polegającego m.in. na rekrutacji dziecka do prostytucji (art. 19 ust. 1 lit. a). Ponadto strony Konwencji zobowiązały się przyjąć konieczne środki ustawodawcze, penalizujące umyślne czyny sprowadzające się do: produkowania pornografii dziecięcej, oferowaniu pornografii, dystrybucji czy też świadomego pozyskiwania dostępu do pornografii dziecięcej za pośrednictwem technologii informacyjnych i telekomunikacyjnych (art. 20 ust. 1). Przestępczym działaniem w rozumieniu Konwencji jest także rekrutacja dziecka do udziału w prezentacjach pornograficznych (art. 21 ust. 1 lit. a). Art. 22 ma chronić dziecko przed demoralizacją. Zakazuje się tu zachowania polegającego na umożliwieniu dziecku uczestniczenia jako świadek przy obcowaniu seksualnym lub innej czynności seksualnej, nawet w sytuacji, gdy dziecko nie jest zmuszane do uczestniczenia w tychże praktykach. Do nagabywania dzieci dla celów seksualnych za pośrednictwem Internetu wprost odnosi się dyspozycja wyrażona w art. 23. Zgodnie z treścią owego przepisu, należy zabezpieczyć karalność zachowania, polegającego na umyślnym składania dziecku przez osobę dorosłą za pośrednictwem technologii informacyjnych i telekomunikacyjnych propozycji spotkania w celu popełnienia przeciwko dziecku któregokolwiek z przestępstw o charakterze seksualnym, w sytuacji, gdy za taką propozycją idą faktyczne działania, mające na celu doprowadzenie do takiego spotkania.

Dużą aktywnością, mającą na celu kryminalizację zachowań związanych z seksualnym wykorzystaniem osób nieletnich za pośrednictwem nowoczesnych technologii, wykazuje się również UE. W dyrektywie Parlamentu Europejskiego i Rady 2010/13/UE, podniesiono m.in. kwestie przeciwdziałania

przez krajowego prawodawcę, treściom mogącym naruszać fizyczny, umysłowy i moralny rozwój małoletnich[47]. W związku z tym należy zastosować odpowiednie środki w celu zapewnienia, by audiowizualne usługi medialne świadczone przez dostawców usług medialnych podlegających ich jurysdykcji, które mogą zaszkodzić fizycznemu, psychicznemu lub moralnemu rozwojowi małoletnich, były udostępniane jedynie w taki sposób, by małoletni w zwykłych okolicznościach nie mogli ich słuchać ani oglądać. Środki te mogą obejmować wybór godzin nadawania, narzędzia weryfikacji wieku lub inne rozwiązania techniczne. Muszą być też proporcjonalne do potencjalnej szkodliwości audycji. W dokumencie podkreśla się jednocześnie, że najbardziej szkodliwe treści, takie jak nieuzasadniona przemoc i pornografia, maja podlegać najsurowszym środkom (art. 6a ust. 1). Dokumentem o szczególnym znaczeniu dla ochrony praw dziecka w sferze jest dyrektywa 2011/93/UE Parlamentu Europejskiego i Rady z dnia 13 grudnia 2011 r.[48] Zgodnie z wyrażoną tam dyspozycją powinno być kryminalizowane świadome uzyskiwanie dostępu do pornografii dziecięcej za pomocą technologii informacyjno-komunikacyjnych. Daną osobę można pociągnąć do odpowiedzialności, jeżeli zamierza ona wejść na stronę zawierającą pornografię dziecięcą, wiedząc, że takie treści się tam znajdują. Zastrzega się jednakże, iż nie należy nakładać sankcji na osoby, które nieumyślnie wejdą na strony zawierające pornografię dziecięcą. Umyślność przestępstwa można ustalić w szczególności, na podstawie stwierdzenia, że ma ono charakter powtarzalny lub popełnione zostało za pośrednictwem płatnego serwisu (pkt 18). Podkreśla się również fakt, że w kontekście korzystania z Internetu, nagabywanie dzieci w celach seksualnych jest zagrożeniem o specjalnym charakterze. Dzieje się tak z uwagi na anonimowość użytkowników mogących ukryć własną tożsamość i dane osobowe (pkt 19). Problem stanowi usuwanie treści zawierających pornografię

[47] Dyrektywa Parlamentu Europejskiego i Rady z dnia 10 marca 2010 r. 2010/13/UE w sprawie koordynacji niektórych przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich dotyczących świadczenia audiowizualnych usług medialnych (Dz.Urz. UE L Nr 95, s. 1).

[48] Dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW (Dz.Urz. UE L Nr 335, s. 1).

dziecięcą w przypadku, gdy oryginalne materiały znajdują się poza terytorium Unii. Poleca się w związku z tym ustanowienie mechanizmów blokowania dostępu z terytorium Unii do stron internetowych, w odniesieniu do których ustalono, że zawierają pornografię dziecięcą lub służą do jej rozpowszechniania (pkt 47). Państwa członkowskie Unii Europejskiej zostały zobowiązane do podjęcia niezbędnych środków zmierzających do usunięcia stron internetowych zawierających lub rozpowszechniających pornografię dziecięcą utrzymywanych na ich terytorium oraz do tego, by dążyły do zapewnienia usunięcia takich stron utrzymywanych poza ich terytorium. Należy ponadto blokować strony internetowe zawierające lub rozpowszechniające pornografię dziecięcą. Wprowadzane rozwiązania mogą również przewidywać możliwość uzyskania zadośćuczynienia sądowego (art. 25). W polskich realiach normą o charakterze ogólnym jest analizowany już 72 Konstytucji RP, który nakłada na szeroko pojmowaną władzę obowiązek zapewnienia ochrony praw dziecka. Ponadto każdy ma prawo żądać od organów władzy publicznej ochrony dziecka przed przemocą, okrucieństwem, wyzyskiem i demoralizacją. Ochrona przed zachowaniami sprawców przestępstw związanych ze sferą seksualności osób nieletnich została zapewniona na gruncie regulacji przyjętych przez polskiego prawodawcę. Naganne czyny zostały stypizowane m.in. w Kodeksie karnym (k.k.)[49]. Zgodnie z dyspozycją wyrażoną w art. 191a k.k., karane jest zachowanie, mające na celu utrwalanie wizerunku nagiej osoby lub osoby w trakcie czynności seksualnej, używając w tym celu wobec niej przemocy, groźby bezprawnej lub podstępu, albo rozpowszechnianie wizerunku nagiej osoby lub osoby w trakcie czynności seksualnej bez jej zgody. Ściganie przestępstwa dokonuje się na wniosek osoby pokrzywdzonej. Jak zauważa Sąd Najwyższy, rozpowszechnianie wizerunku, stanowiące znamię przestępstwa z art. 191a. k.k. w praktyce następuje wyłącznie za pomocą mediów elektronicznych, co samo w sobie w najmniejszym stopniu nie obniża stopnia szkodliwości społecznej takiego czynu[50]. Penalizacja zachowań wypełniających dyspozycję art. 191a k.k., dokonała się za sprawą

[49] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. Dz.U. z 2021 r. poz. 2345 z późn. zm.).

[50] Wyrok SN z dnia 13 kwietnia 2016 r., II KK 304/15, LEX nr 2019608.

nowelizacji Kodeksu karnego ustawą z dnia 15 grudnia 2009 r.[51] Przed datą wejścia jej w życie (8 czerwca 2010 r.), pokrzywdzony takim czynem mógł skorzystać jedynie z ochrony cywilnoprawnej. Jednakże nagminność tego typu zachowań, w szczególności dokonywanych za pośrednictwem Internetu, spowodowała konieczność przeciwdziałania temu zjawisku[52]. Jak pokazują policyjne statystyki, na przełomie lat 2010–2020 liczba stwierdzonych przestępstw z art. 191a k.k., wzrosła z 11 do 360. Najwięcej jednak, bo aż 400, odnotowano w 2019 r.[53] Wynika to zapewne z coraz bardziej powszechnej dostępności do usług internetowych, jak również ze zwiększającej się świadomości samych poszkodowanych. Kodeks karny penalizuje również zachowanie, polegające na prezentowaniu małoletniemu poniżej 15. roku życia treści pornograficznych lub udostępnianie mu przedmiotów mających taki charakter. Ponadto zakazuje się rozpowszechniania treści pornograficznych w sposób umożliwiający małoletniemu zapoznanie się z nimi. Karana jest także reklama lub promocja działalności, polegająca na rozpowszechnianiu treści pornograficznych w sposób umożliwiający zapoznanie się z nimi małoletniemu poniżej lat 15 (art. 200 § 3 i 5 k.k.). Czyny karalne dokonywane za pomocą narzędzi elektronicznych zostały stypizowane w art. 200a k.k. (przepis dodany na mocy nowelizacji z dnia 15 grudnia 2009 r.). Zgodnie z dyspozycją wyrażoną w powyższej normie, kto w celu popełnienia przestępstwa gwałtu wobec małoletniego poniżej 15. roku życia lub innych form wykorzystywania seksualnego osoby poniżej 15 lat, dookreślonych w art. 200 k.k., jak również produkowania lub utrwalania treści pornograficznych, za pośrednictwem systemu teleinformatycznego lub sieci telekomunikacyjnej nawiązuje kontakt z małoletnim poniżej lat 15, zmierzając, za pomocą wprowadzenia go w błąd, wyzyskania błędu lub niezdolności do

[51] Ustawa z dnia 5 listopada 2009 r. o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego, ustawy – Kodeks karny wykonawczy, ustawy – Kodeks karny skarbowy oraz niektórych innych ustaw (Dz.U. z 2009 r. Nr 26, poz. 1589) – art. 21 ust. 23.

[52] M. Mozgawa, K. Nazar-Gutowska, *Utrwalanie lub rozpowszechnianie wizerunku nagiej osoby – art. 191 a k.k.* (*analiza prawnokarna i praktyka ścigania*), „Prawo w Działaniu" 2014, nr 19, s. 28.

[53] *Utrwalenie wizerunku bez jej zgody* (*art. 191a*), https://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-4/48035,Utrwalanie-wizerunku-nagiej-osoby-bez-jej-zgody-art-191a.html (dostęp: 24.03.2022 r.).

należytego pojmowania sytuacji albo przy użyciu groźby bezprawnej, do spotkania z nim, podlega karze pozbawienia wolności do lat 3. Karze grzywny, ograniczeniu wolności albo pozbawieniu wolności do lat 12, podlega także ten, kto za pośrednictwem systemu teleinformatycznego lub sieci telekomunikacyjnej małoletniemu poniżej lat 15 składa propozycję obcowania płciowego, poddania się lub wykonania innej czynności seksualnej lub udziału w produkowaniu lub utrwalaniu treści pornograficznych i zmierza do jej realizacji (art. 200 a § 2 k.k.). Zgodnie ze stanowiskiem SN:

> odpowiedzialności karnej za przestępstwo tzw. groomingu w postaci wskazanej w art. 200a § 2 k.k. podlega ten, „kto za pośrednictwem systemu teleinformatycznego lub sieci telekomunikacyjnej małoletniemu poniżej lat 15 składa propozycję obcowania płciowego, poddania się lub wykonania innej czynności seksualnej lub udziału w produkowaniu lub utrwalaniu treści pornograficznych, i zmierza do jej realizacji". Realizacja znamion tego typu czynu zabronionego wymaga podjęcia przez sprawcę dwóch powiązanych ze sobą ściśle zachowań sprawczych. Po pierwsze, ma to być zachowanie sprawcy polegające na złożeniu za pośrednictwem systemu teleinformatycznego lub sieci telekomunikacyjnej małoletniemu poniżej lat 15 propozycji obcowania płciowego, poddania się lub wykonania innej czynności seksualnej lub udziału w produkowaniu lub utrwalaniu treści pornograficznych. Po drugie, sprawca w związku z tą propozycją musi podjąć zachowania zmierzające do realizacji tej propozycji[54].

W innym ze swoich orzeczeń SN doprecyzował, że:

> doprowadzenie małoletniego poniżej lat 15 do wykonania czynności seksualnej i do przesłania jej zapisu na profil internetowy sprawcy, który uprzednio złożył pokrzywdzonemu za pośrednictwem systemu teleinformatycznego propozycję w tym zakresie i zmierzał do jej realizacji, w konsekwencji

[54] Wyrok SN z dnia 23 lipca 2020 r., III KK 281/19, LEX nr 3126968.

> czego uzyskał dostęp do treści pornograficznej z udziałem dziecka – stanowi przestępstwo określone w art. 200a § 2 k.k. […][55].

W świetle danych prezentowanych przez Policję liczba stwierdzonych przestępstw dookreślonych w art. 200a k.k., wzrosła na przestrzeni lat 2010–2020 z 6 do 456[56].

W art. 202 k.k. zostały uregulowane przestępstwa związane z publicznym prezentowaniem treści pornograficznych. Czyny wobec nieletnich dotyczą m.in. rozpowszechniania, prezentowania, produkcji, utrwalania, przechowywania treści pornograficznych z ich udziałem.

Obok regulacji zawartych w Kodeksie karnym, normy dotyczące ochrony małoletnich przed wykorzystywaniem seksualnym za pomocą przekazów elektronicznych zostały zawarte w szeregu innych aktów normatywnych. Ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (u.k.s.c.)[57], przyjęto w celu implementacji do prawa polskiego dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (tzw. dyrektywę NIS)[58]. Role CSIRT (ang. *Computer Security Incident Response Team*) poziomu krajowego przyjęły na siebie Agencja Bezpieczeństwa Wewnętrznego (CSIRT GOV), NASK – Państwowy Instytut Badawczy (CSIRT NASK) oraz resort obrony narodowej (CSIRT MON). Do zadań CSIRT NASK należy m.in. zapewnienie obsługi linii telefonicznej lub serwisu internetowego prowadzących działalność w zakresie zgłaszania i analizy przypadków dystrybucji, rozpowszechniania lub przesyłania pornografii dziecięcej za pośrednictwem technologii informacyjno-komunikacyjnych, o których mowa w dyrektywie Parlamentu Europejskiego i Rady 2011/92/UE

[55] Postanowienie SN z dnia 4 lipca 2019 r., III KK 166/18, OSNKW 2019, nr 9, poz. 55.

[56] Uwodzenie małoletniego poniżej 15 lat z wykorzystaniem systemu teleinformatycznego lub sieci telekomunikacyjnej (art. 200a), https://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-6/64005,uwodzenie-maloletniego-ponizej-lat-15-z-wykorzystaniem-systemu-teleinformatyczne.html (dostęp: 24.03.2022 r.).

[57] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2020 r., poz. 1369).

[58] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. UE L Nr 194, s. 1).

z dnia 13 grudnia 2011 r. (art. 26 ust. 6 p. 3 u.k.s.c.). Zadanie to realizowane jest przez CSIRT NASK w ramach Dyżurnet.pl, zespołu ekspertów Naukowej i Akademickiej Sieci Komputerowej, działającego jako punkt kontaktowy do zgłaszania nielegalnych treści w Internecie, szczególnie związanych z seksualnym wykorzystywaniem dzieci[59].

Dostęp osób nieletnich do treści zagrażających fizycznemu, psychicznemu lub moralnemu rozwojowi został również ograniczony w ustawie o radiofonii i telewizji (u.r.t.)[60]. Z uwagi zaś na to, że większość stacji radiowych i telewizyjnych nadaje swoje programy w Internecie, zasady zawarte w ustawie mają bezpośrednie przełożenie do kwestii poruszanych w niniejszym opracowaniu. Prawodawca uznał m.in., że szczególnie negatywny wpływ na rozwój dziecka mają treści pornograficzne lub te, które w nieuzasadniony sposób eksponują przemoc (art. 18 ust. 4 u.r.t.). Szczegóły dotyczące treści zawierających sceny seksu prezentowane osobom nieletnim zostały dookreślone w rozporządzeniu Krajowej Rady Radiofonii i Telewizji (KRRiT) z dnia 23 czerwca 2005 r.[61] Na straży przestrzegania przepisów u.r.t. stoi Przewodniczący KRRiT. Do jego kompetencji należy m.in. nakładanie kar pieniężnych określonych w art. 53 u.r.t.[62].

W związku z ochroną małoletnich przed treściami pornograficznymi w literaturze przedmiotu analizowany jest aspekt ewentualnego zakazu ich publikowania, który może zostać nałożony na producentów takowych materiałów. Jak podkreśla M. Niedźwiedź, ewentualna decyzja o blokowaniu dzieciom dostępu

---

[59] K. Prusak-Górniak, K. Ślicki, [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. K. Czaplicki, A. Gryszczyńska, G. Szpor, Warszawa 2019, art. 26.

[60] Ustawa z dnia 29 grudnia 1992 r. o radiofonii i telewizji (t.j. Dz.U. z 2017 r. poz. 1414 z późn. zm.).

[61] Rozporządzenie Krajowej Rady Radiofonii i Telewizji z dnia 23 czerwca 2005 r. w sprawie kwalifikowania audycji lub innych przekazów mogących mieć negatywny wpływ na prawidłowy fizyczny, psychiczny lub moralny rozwój małoletnich oraz audycji lub innych przekazów przeznaczonych dla danej kategorii wiekowej małoletnich, stosowania wzorów symboli graficznych i formuł zapowiedzi (t.j. Dz.U. z 2014 r. poz. 311).

[62] Szerzej na ten temat: Stowarzyszenie Twoja Sprawa, Analiza istniejących przepisów prawnych pod kątem ochrony dzieci i młodzieży przed zbyt łatwym dostępem do treści seksualizujących i pornograficznych, Warszawa 2016, https://twojasprawa.org.pl/files/attachments/9f4d9607-6a88-11e9-a494-00163e34cb38/analiza-prawna-sts.pdf (dostęp: 25.03.2022 r.).

do treści o charakterze pornograficznym wiąże się z szeregiem problemów[63]. Po pierwsze, należy dookreślić, czy ograniczenia trzeba wprowadzać w formie źródeł prawa powszechnie obowiązującego, czy też poprzez regulacje wewnętrzne przyjmowane przez poszczególnych przedsiębiorców. Po drugie, istnieje możliwość zaistnienia kolizji praw człowieka i praw ekonomicznych. Trzecią kwestię stanowi problem precyzyjnego definiowania treści podlegających filtrowaniu i blokowaniu. Po czwarte, mogą zaistnieć ewentualne trudności techniczne w blokowaniu stron nieodpowiednich dla nieletnich. Po piąte, oczywistą sprawą będzie opór niektórych środowisk biznesowych oraz części społeczeństwa[64]. Prezentowane powyżej regulacje, przyjęte na poziomie Unii Europejskiej, zakładają, że to państwa winny przyjąć odpowiednie rozwiązania ograniczające ewentualny dostęp nieletnich do treści pornograficznych. Dzieje się tak dlatego, że sama UE nie wypracowała dotąd uniwersalnego modelu akceptowanego przez poszczególne państwa członkowskie. W Polsce w 2013 r. podjęto działania, mające na celu przyjęcie ustawy gwarantującej rodzicom prawo do Internetu bez pornografii. W projekcie uchwały sejmowej skierowanej do Ministra Cyfryzacji i Administracji podkreślono konieczność przyjęcia takich reguł, które pozwalałyby każdej osobie żądania od dostawcy usług internetowych blokowania przesyłania treści o charakterze pornograficznym. Ponadto, dostawcy usług internetowych powinni opracować skuteczne filtry, umożliwiające blokowanie treści o charakterze pornograficznym[65]. Niestety inicjatywa upadła i prace nad ustawą zostały zatrzymane. Głównym argumentem podnoszonym przeciw możliwości przyjęcia odpowiednich regulacji są rozwiązania przyjęte w dyrektywie 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r.[66], które zostały implementowane do ustawy

[63] M. Niedźwiedź, *Problematyka prawna ograniczenia dostępu do treści pornograficznych w Internecie ze względu na ochronę dzieci z perspektywy prawa unijnego*, „Problemy Współczesnego Prawa Międzynarodowego, Europejskiego i Porównawczego" 2018, t. XV, s. 102.

[64] *Ibidem*, s. 102–103.

[65] Druk sejmowy nr 1664 z dnia 29 lipca 2013 r., http://orka.sejm.gov.pl/Druki7ka.nsf/0/107F92BAF489D5EAC1257BD500319B54/$File/1664.pdf (dostęp: 25.03.2022 r.).

[66] Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (Dz.Urz. UE L Nr 178, s. 1).

z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (art. 14 i 15)[67]. Kluczowe znaczenie ma art. 15 dyrektywy, który stanowi, że:

> Państwa Członkowskie nie nakładają na usługodawców świadczących usługi określone w art. 12, 13 i 14 ogólnego obowiązku nadzorowania informacji, które przekazują lub przechowują ani ogólnego obowiązku aktywnego poszukiwania faktów i okoliczności wskazujących na bezprawną działalność.

Warto zauważyć, że nie ma zgodności co do interpretowania powyższej normy nawet w orzecznictwie TSUE. W sprawie C-70/10, *Scarlet v. SABAM*, Trybunał wskazał, że zakaz, o którym mowa w art. 15, obejmuje przepisy krajowe, które zobowiązywałyby usługodawcę do prowadzenia aktywnego nadzoru nad wszystkimi danymi każdego z jego klientów celem realizacji wskazanego celu[68]. Podobnie w wyroku z dnia 16 lutego 2012 r., TSUE podkreśla m.in., że dyrektywa 2000/31/WE, 2001/29/WE oraz 2004/48/WE, pozostające w związku i interpretowane w świetle wymogów wynikających z ochrony mających zastosowanie praw podstawowych, należy rozumieć w ten sposób, że stoją one na przeszkodzie skierowanemu przez sąd krajowy do podmiotu świadczącego usługi hostingowe nakazowi wprowadzenia systemu filtrowania informacji przechowywanych na serwerach przez użytkowników tych usług[69].

Bardziej jednak przekonuje stanowisko, jakie wyraził TSUE w wyroku z dnia 3 października 2019 r.[70] Zgodnie z jego treścią, dyrektywę 2000/31/WE, a w szczególności jej art. 15 ust. 1, należy interpretować w ten sposób, że nie stoi ona na przeszkodzie temu, aby sąd państwa członkowskiego mógł m.in. nakazać dostawcy usług hostingowych usunięcie informacji, które dostawca ten przechowuje i których treść jest identyczna z treścią informacji uprzednio uznanej za mającą bezprawny charakter lub zablokowanie dostępu do tych informacji, niezależnie od tego, kto wnioskował o przechowywanie tych informacji. Sąd

---

[67] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz.U. z 2020 r. poz. 344).

[68] Wyrok TSUE z dnia 24 listopada 2011 r., C-70/10, LEX nr 1064166.

[69] Wyrok TSUE z dnia 16 lutego 2021 r., C-360/10, LEX nr 1108635.

[70] Wyrok TSUE z dnia 3 października 2021 r., C-360/10, LEX nr 2723800.

krajowy może również nakazać dostawcy usług hostingowych usunięcie informacji, których dotyczy nakaz lub zablokowanie dostępu do tych informacji na całym świecie, w ramach właściwego prawa międzynarodowego. Z powyższym stanowiskiem koresponduje również wyrok SN, w którym podkreśla się, iż to, że na gruncie art. 15 ust. 1 dyrektywy 2000/31/WE i art. 15 ustawy z 2002 r. o świadczeniu usług drogą elektroniczną usługodawcy nie mają obowiązku monitorowania, filtrowania danych czy ich sprawdzania, nie oznacza, iż nie mogą i nie powinni reagować na informacje o wykorzystywaniu prowadzonego portalu. Wprawdzie orzeczenie to dotyczy treści o charakterze totalitarnym, niemniej jednak ma ono również zastosowanie w stosunku do innych informacji. Zgodzić się należy ze stanowiskiem, że w świetle przepisów dyrektywy 2000/31/WE dostawca usług internetowych nie może ponosić odpowiedzialności za treść przekazu ani też nie może być zobowiązany do ogólnego obowiązku nadzorowania informacji. Zwolnienie to ma jednak charakter warunkowy i dostawca nie jest zwolniony z odpowiedzialności za udostępniane treści w sytuacji, gdy był w posiadaniu wiarygodnych informacji o ich bezprawnym charakterze[71].

Obok zachowań związanych ze sferą seksualności nieletniego, prawodawca penalizuje również inne czyny, które mogą być dokonywane za sprawą mediów elektronicznych. Zgodnie z art. 190 § 1 k.k. zakazane jest zachowanie polegające na grożeniu innej osobie popełnieniem przestępstwa na jej szkodę lub szkodę osoby najbliższej, jeżeli groźba wzbudza w zagrożonym uzasadnioną obawę, że będzie spełniona. Jak podkreśla się w doktrynie, forma groźby nie ma znaczenia[72]. Może być więc wyrażona również poprzez Internet. Jak podkreślił SN w jednym ze swoich wyroków, groźba bezprawna może nie być wyrażona słowami, lecz i gestem, wyrazem twarzy, w ogóle zachowaniem się grożącego, byle tylko w sposób zrozumiały dla pokrzywdzonego dawała im poznać swoją treść[73].

---

71 M. Niedźwiedź, *op. cit.*, s. 110–111.

72 M. Mozgawa, [w:] *Kodeks karny. Komentarz*, red. M. Mozgawa, LEX/el. 2022, art. 190.

73 Wyrok SN z dnia 18 stycznia 1934 r., I K 927/33, OSNK 1934, nr 6, poz. 110.

5. Wnioski

Powszechny dostęp do Internetu sprawia, że obserwuje się systematycznie wzrastającą liczbę przestępstw. Dzieci szczególnie narażone są na zachowanie godzące w ich rozwój fizyczny, duchowy czy emocjonalny. Zdecydowana większość przestępstw popełnianych na szkodę osób nieletnich związana jest z intymną sferą ich życia. Dotyczy w głównej mierze zachowań o charakterze seksualnym, czyniących dziecko czynnym bądź biernym podmiotem agresji. Podsumowując ustalenia zawarte w niniejszym opracowaniu, można sformułować następujące wnioski:

1/ Dziecko z uwagi na swą niedojrzałość fizyczną i psychiczną jest szczególnie narażone na różnorodne ataki, skierowane wobec jego osoby. Płaszczyzną zaś, gdzie dochodzi do szczególnej ingerencji w dobro małoletniego jest Internet.
2/ Ponad połowę aktywnego czasu dziecko spędza w sieci, co powoduje, że wirtualna rzeczywistość dominuje w kształtowaniu jego osobowości.
3/ Żadna dziedzina życia nie rozwija się tak dynamicznie jak wirtualna rzeczywistość. W związku z tym ogromne wyzwanie ciąży na prawodawcy, aby adekwatnie reagować w zależności od pojawiania się nowych zagrożeń.
4/ Obowiązek troski o prawa dziecka jest klauzulą powszechną, obejmującą nieograniczony zakres adresatów, a zasada konieczności kierowania się jego dobrem jest naczelną wartością w procesie sprawowania opieki przez rodziców i opiekunów prawnych.
5/ Sfera ochrony prywatności dziecka dotyczy nie tylko jego rodziców i opiekunów prawnych, ale obejmuje nieograniczony zakres podmiotów, które mogą ingerować w owe uprawnienia.
6/ Nie można wykluczyć ewentualności, iż dziecko powołując się na swe prawo do prywatności będzie oponować przeciwko zdaniu rodziców. Nie można również kategorycznie stwierdzić, że w każdej sytuacji wola rodziców będzie miała decydujące znaczenie, dlatego też sporne zagadnienia mogą być przedmiotem rozstrzygnięcia wymiaru sprawiedliwości.

7/ Na gruncie rozwiązań normatywnych można wskazać granice temporalne (13–16 lat), po przekroczeniu których, prawodawca uznaje skuteczność woli wyrażonej przez osobę nieletnią.

8/ W polskich realiach wiele rozwiązań normatywnych daje rodzicom narzędzie do tego, aby wiążąco wpływać na zachowanie ich dzieci. Przykładem jest norma zawarta w art. 48 ust. 1, przyznająca rodzicom prawo do wychowania dziecka zgodnie z ich przekonaniami.

9/ Interesem rodziców w sytuacjach, gdy ingerują w prywatność swoich dzieci będzie obowiązek troszczenia się o ich fizyczny i duchowy rozwój (art. 96 § 1 k.r.o.).

10/ Ewentualna opcja zanegowania zdania rodziców w procesie wychowania powinna być brana pod uwagę w wyjątkowych sytuacjach, gdy ingerowanie w prawa dziecka jest oczywiście bezzasadne.

11/ Jak alarmują psychologowie, stany depresyjne, doprowadzające do samobójstw wśród nieletnich, spowodowane są m.in. tym, że w okresie pandemii całe życie dziecka – szkolne i towarzyskie – toczy się w systemie online.

12/ Według danych Komendy Głównej Policji, w 2020 r. targnęło się na własne życie 116 osób poniżej 18. roku życia. Wśród nich było ośmioletnie dziecko. Jest to wzrost na poziomie ok. 20% w stosunku do trzech poprzednich lat.

13/ Ochrona normatywna dziecka przed szkodliwym oddziaływaniem publikacji internetowych dokonuje się na wielu płaszczyznach, obejmując swym zakresem zarówno regulacje krajowe jak i międzynarodowe. Ponadto istotną rolę w egzekwowaniu praw przysługujących osobom nieletnim odgrywa wymiar sprawiedliwości.

14/ Z racji konieczności aplikowania rozwiązań międzynarodowych do krajowego systemu prawnego, istnieje ścisła koherencja pomiędzy istniejącymi regulacjami. Znaczna ich część związana jest ze sferą seksualności młodego człowieka. Dominuje w nich zjawisko dziecięcej pornografii, ale także regulowane są inne formy negatywnego oddziaływania Internetu na integralność cielesną i duchową małoletnich.

15/ W świetle obowiązujących regulacji dostawca usług internetowych nie może ponosić odpowiedzialności za treść przekazu ani też nie może być

zobowiązany do ogólnego obowiązku nadzorowania informacji. Zwolnienie to ma jednak charakter warunkowy i dostawca nie jest zwolniony z odpowiedzialności za udostępniane treści w sytuacji, gdy był w posiadaniu wiarygodnych informacji o ich bezprawnym charakterze.

Bibliografia

Bezpieczeństwo dzieci i młodzieży online. Kompendium dla rodziców i profesjonalistów, red. A. Rywczyńska, Sz. Wójcik, Warszawa 2018.

Bielecki M., *Ochrona rodziny i życia rodzinnego w kontekście wychowywania zgodnie z przekonaniami rodziców*, Warszawa 2020.

Brynat P.E., Coleman A.M., *Psychologia rozwojowa*, Poznań 1997.

Dabrowska M., *Grooming – wybrane aspekty prawnokarne i kryminologiczne*, Warszawa 2018.

Drapała A., *Parental trolling w świetle uregulowań polskiej ustawy karnej*, „Problemy Prawa Prywatnego Międzynarodowego" 2018, nr 23.

Kwaśnik A., Polak Z., Chojnacka O., Różycka M., Marańda M., *Ryzykowne zachowana seksualne i seksualizacja młodych użytkowników Internetu. Zarys Problematyki*, Warszawa 2019.

Magda M., *Wrażliwość moralna, a rozwój moralny człowieka*, „Wychowanie Na Co Dzień" 2000, nr 1.

Mostowik P., *Kwestia regulacji dostępu dzieci do internetowej pornografii na tle prawa międzynarodowego i unijnego Uwagi na tle niekontynuowanej inicjatywy legislacyjnej*, maszynopis w posiadaniu autora.

Mozgawa M., [w:] *Kodeks karny. Komentarz*, red. M. Mozgawa, LEX/el 2022.

Mozgawa M., Nazar-Gutowska K., *Utrwalanie lub rozpowszechnianie wizerunku nagiej osoby – art. 191 a k.k.* (*analiza prawnokarna i praktyka ścigania*), „Prawo w Działaniu" 2014, nr 19.

Niedźwiedź M., *Problematyka prawna ograniczenia dostępu do treści pornograficznych w Internecie ze względu na ochronę dzieci z perspektywy prawa unijnego*, „Problemy Współczesnego Prawa Międzynarodowego, Europejskiego i Porównawczego" 2018, t. XV.

Pająk M., Sztandera F., *Wybrane aspekty parental trollingu w sieci Internet*, „Problemy Nauk Prawnych" 2019, t. 12.

Program wsparcia psychologiczno-pedagogicznego dla uczniów i nauczycieli w pandemii – https://www.gov.pl/web/edukacja-i-nauka/program-wsparcia-psychologiczno-pedagogicznego-dla-uczniow-i-nauczycieli-w-pandemii (dostęp: 18.03.2022).

Prusak-Górniak K., Ślicki K., [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. K. Czaplicki, A. Gryszczyńska, G. Szpor, Warszawa 2019.
Pryciak M., *Prawo do prywatności*, „Studia Erasmiana Wratislaviensia" 2010, nr 4.
Pyżalski J., Zdrodowska A., Tomczyk Ł., Abramczuk K., *Polskie badania EU Kids Online 2018 r. Najważniejsze wyniki i wnioski*, Poznań 2019.
Rodzik E., *Prawo do prywatności dziecka a rodzicielska kontrola jego aktywności w Internecie*, [w:] *Prawo do prywatności – współczesne wyzwania*, red. M. Wiącek, Warszawa 2019.
Uliasz J., *Prawna ochrona prywatności oraz wolności dzieci w Internecie*, „Zeszyty Naukowe Uniwersytetu Rzeszowskiego" 2020, z. 110.

Akty prawne i inne regulacje

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r., Nr 78, poz. 483 z późn. zm.).
Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności z dnia 4 listopada 1950 r. (Dz.U. z 1993 r., Nr 61, poz. 284).
Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (Dz.U. z 1977 r. Nr 38, poz. 167).
Protokół Fakultatywny do Konwencji o prawach dziecka w sprawie handlu dziećmi, dziecięcej prostytucji i dziecięcej pornografii, przyjęty w Nowym Jorku dnia 25 maja 2000 r. (Dz.U. z 2007 r. Nr 76, poz. 494).
Konwencja Rady Europy o ochronie dzieci przed seksualnym wykorzystywaniem i niegodziwym traktowaniem w celach seksualnych, sporządzona w Lanzarote dnia 25 października 2007 r. (Dz.U. z 2015 r. poz. 608).
Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (Dz.Urz. UE L Nr 178, s. 1).
Dyrektywa Parlamentu Europejskiego i Rady z dnia 10 marca 2010 r. 2010/13/UE w sprawie koordynacji niektórych przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich dotyczących świadczenia audiowizualnych usług medialnych (Dz.Urz. UE L Nr 95, s. 1).
Dyrektywa Parlamentu Europejskiego i Rady z dnia 13 grudnia 2011 r. (2011/93/UE) w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW (Dz.Urz. UE L Nr 335, s. 1).
Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. UE L Nr 194, s. 1).

Konwencja o prawach dziecka z dnia 20 listopada 1989 r. (Dz.U. z 1991 r. Nr 120, poz. 526).
Karta Praw Podstawowych Unii Europejskiej 2007 r. (Dz.Urz. UE C Nr 303, s. 1).
Ustawa z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (Dz.U. z 2020 r. poz. 1575);
Ustawa z dnia 26 października 1982 r. Postępowanie w sprawach nieletnich (t.j. Dz.U. z 2018 r. poz. 969 z późn. zm.).
Ustawa z dnia 29 grudnia 1992 r. o radiofonii i telewizji (t.j. Dz.U. z 2017 r. poz. 1414 z późn. zm.).
Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz.U. z 2021 r. poz. 2345 z późn. zm.).
Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz.U. z 2020 r. poz. 344).
Ustawa z dnia 5 listopada 2009 r. o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego, ustawy – Kodeks karny wykonawczy, ustawy – Kodeks karny skarbowy oraz niektórych innych ustaw (Dz.U. z 2009 r. Nr 26, poz. 1589).
Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2020 r. poz. 1369).
Rozporządzenie Krajowej Rady Radiofonii i Telewizji z dnia 23 czerwca 2005 r. w sprawie kwalifikowania audycji lub innych przekazów mogących mieć negatywny wpływ na prawidłowy fizyczny, psychiczny lub moralny rozwój małoletnich oraz audycji lub innych przekazów przeznaczonych dla danej kategorii wiekowej małoletnich, stosowania wzorów symboli graficznych i formuł zapowiedzi (t.j. Dz.U. z 2014 r. poz. 311).
Powszechna Deklaracja Praw Człowieka z dnia 10 grudnia 1948 r.
Komitet Praw Dziecka. Czterdziesta Sesja Genewa 12-30 września 2005 r. Komentarz Ogólny nr 7 (2005). Komitet Praw Dziecka. Komentarz Ogólny nr 13 (2011).
Komitet Praw Dziecka. Sześćdziesiąta Druga Sesja. Genewa 14 stycznia – 1 lutego 2013. Komentarz Ogólny nr 16 (2013)dotyczący zobowiązań Państw – Stron w zakresie wpływu sektora biznesowego na prawa dzieci.
Rezolucja Parlamentu Europejskiego z dnia 20 listopada 2012 r. w sprawie ochrony dzieci w świecie cyfrowym – 2012/2068(INI) (Dz.U. UE.C. 2015.419.33).

Orzecznictwo

Wyrok TK z dnia 16 grudnia 2020 r., SK 26/16, OTK-A 2020, poz. 69.
Wyrok ETPCz z dnia 29 kwietnia 2002 r., skarga nr 2346/02, HUDOC.
Wyrok ETPCz z dnia 2 grudnia 2008 r., skarga nr 2872/02, LEX nr 468377.
Wyrok TSUE z dnia 24 listopada 2011 r., C-70/10, LEX nr 1064166.
Wyrok TSUE z dnia 16 lutego 2021 r., C-360/10, LEX nr 1108635.
Wyrok TSUE z dnia 3 października 2021 r., C-360/10, LEX nr 2723800.

Wyrok SN z dnia 18 stycznia 1934 r., I K 927/33, OSNK 1934, nr 6, poz. 110.
Wyrok SN z dnia 5 maja 2000 r., II CKN 765/00, LEX nr 51981.
Wyrok SN z dnia 13 kwietnia 2016 r., II KK 304/15, LEX nr 2019608.
Postanowienie SN z dnia 4 lipca 2019 r., III KK 166/18, OSNKW 2019, nr 9, poz. 55.
Wyrok SN z dnia 23 lipca 2020 r., III KK 281/19, LEX nr 3126968.
Wyrok NSA z dnia 29 sierpnia 2018 r., II OSK 1041/18, LEX nr 2553581.
Wyrok SO Warszawa-Praga w Warszawie z dnia 25 stycznia 2016 r., VI Ka 1206/16, niepubl.

Netografia

Ćwirek J., Kowalska K., *Coraz więcej dzieci odbiera sobie życie. Najmłodsze miało osiem lat*, https://www.rp.pl/spoleczenstwo/art240171-coraz-wiecej-dzieci-odbiera-sobie-zycie-najmlodsze-mialo-osiem-lat (dostęp: 18.03.2022 r.).
Forma P., *Sharenting czyli internetowa wizualizacja życia rodzinnego* (*prezentacja*), https://www.scdn.pl/images/stories/projekty/chmura19/SHARENTING.pdf (dostęp: 22.03.2022 r.).
Godziński B., *TikToki z frontu. Ukraińcy pokazują, jak wygląda ich codzienność na wojnie*, https://spidersweb.pl/rozrywka/2022/02/28/tiktok-wojna-ukraina-rosja-relacje-filmiki (dostęp: 18.03.2022 r.).
Komitet Praw Dziecka (*Committee on the Rights of the Child*) – CRC, http://www.unic.un.org.pl/dyskryminacja/ct_crc.php (dostęp: 22.03.2022 r.). Utrwalenie wizerunku bez jej zgody (art. 191a), https://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-4/48035,Utrwalanie-wizerunku-nagiej-osoby-bez-jej-zgody-art-191a.html (dostęp 24.03.2022 r.).
Uwodzenie małoletniego poniżej 15 lat z wykorzystaniem systemu teleinformatycznego lub sieci telekomunikacyjnej (art. 200a), https://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-6/64005,uwodzenie-maloletniego-ponizej-lat-15-z-wykorzystaniem-systemu-teleinformatyczne.html (dostęp 24.03.2022 r.).

Emilia Smolak-Lozano, Víctor Serrano Suárez

Cybercrimes in the Spanish legal system. Jurisdiction, evolution, the present state, and online popularity scan

1. Introduction and state of art

1.1. The evolution from "analogue human" towards "digital human"

Currently, the humanity is facing a moment in which digital disruption seems to impose itself day by day on technological accelerating pace, since we are facing the right "technological momentum", as Hughes[1] stated. According to Williams[2], technology can manifest itself as a force that creates habits and new ways of life, or as a force that provides the necessary elements for the creation of those habits and ways of life, as it can be observed with the new communication technologies. Consequently, the forms of communication have been evolving and adapting to this new reality, thus the traditional forms of communication have been replaced by others that are practiced through the tools provided by the new technologies. Chambat[3] noticed that these new technologies have come to spread in all daily activities, from work to leisure activities. As such, those activities that are not incorporated in time into the new technologies mechanisms will become what Rogers[4], in his diffusionist theory, described as "laggard".

---

[1] T.P. Hughes, *Technological momentum En M.R. Smith, & L. Marx* (*Eds.*). *Does Technology Drive History? The Dilemma of Technological Determinism*, MIT Press 2019, *passim*.

[2] R. Williams, *Television, technology and cultural form*, Schocken Books 1975, *passim*.

[3] P. Chambat, *Usages des technologies de l'information et de la communication* (*TIC*): *évolution des problématiques*, "Technologies de l'information et société" 1994, vol. 6, 3. Dunod.

[4] E.M. Rogers, *Diffusion of Innovations*, The Free Press 1983, *passim*.

These new means of communication have countless advantages, including ease of use, the possibility of automating processes and reduced costs, making the transition to the implementation of the innovative ways of communicating not only attractive, but inevitable.

However, it is not all advantages. We are immersed in a change of era, from analogue to digital, thus, at the moment, there coexist the generations born and raised in the previous analogue era with the new "digital humans", born already immersed in the digital era. For the latter, the analogue media are nothing more than echoes of a remote and archaic past.

In this sense, those born in the digital era not only see the use of these new technologies as normal, as it could not be otherwise, but also they have grown up surrounded by them, and apply them with the same naturalness and agility as the "analogue humans" coped with the previous technologies (letters, phone calls, SMS, etc.).

It can be assumed that these new generations master and understand the new tools more easily and, in general, they really do. However, it would be a mistake to assume that just because the modern generations are familiar with the new technologies, they know the legal limits and the dangers they may entail. This happens because new digital generation do not feel the necessity to know how these computer-based technologies work, they just use them on daily basis[5].

Therefore, the rapid growth of the new technologies entails two main problems for all users, regardless to their age: ignorance of the safety risks when applying modern communication tools and the limits that the legal system establishes for their use. Hence the purpose of the study to examine the state of Spanish legislation in the field of cybercrime, the corresponding statistics, its evolution alongside the Internet development, and finally the scan of the online popularity of certain computer-based crimes in online environment.

[5] N. Bilbeny, *La revolución en la ética. Hábitos y creencias en la sociedad digital*, Anagrama 1997, *passim*.

1.2. Transition towards the use of digital communication tools and the possible issues

As mentioned before, there has been a transformation of the communication tools applied by different users, among which we find, for example, and without wishing to include a *numerus clauses*, the different paths of transition. Among them there can be found as follows: transition from the use of fixed telephony to cell phones; from SMS to instant messaging apps or the use of social networks; from telephone calls to IP calls, video calls or social networks; from traditional letters to e-mails; from fax to e-mail with acknowledgment of sending and receiving; or from bureaufax to electronic bureaufax.

The current trend is marked by concept of "being paperless", and the adoption of web-based means of communication, as far as possible.

Among all the prevailing newly emerging means of communication via online technologies, we can observe the extraordinary importance of social networks that can be used for practically any kind of communication purpose, whether it is person-to-person flow or the message is addressed to a multitude of audiences.

However, the use of social networks as a predominant tool of communication by all types of users, regardless of their training, technical skills, age or any other circumstance, can produce behaviours that may arise a conflict with the legal system in various ways.

On one hand, these social networks allow the dissemination of content (images, videos, audios, documents, etc.), which in many cases is done without any kind of filter or review from the social networks themselves (with exceptions such as Youtube, which incorporates an algorithm capable of detecting protected content and suspending it in case of detection of fraud). Therefore, on numerous occasions the content protected by copyright is commonly shared via social networks channels that may violate the honour, privacy or intellectual property rights of other users.

On the other hand, and due to some extent to the type of often confidential content that is uploaded to social networks, or any other private digital media, unauthorized access to these resources becomes an interesting target for

unauthorized users, when trying to access them without permission, by means of illegal techniques and procedures, and for illicit purposes.

1.3. Computer communications security

The standardization of the new technologies usage requires the adoption of ever stronger security and protection systems. Initially, the systems for accessing resources were weak and trivial, but as new technologies have advanced, the means dedicated to their protection have been developed accordingly. Unfortunately, the attack techniques are always ahead of these protection systems. Usually, security breaches, if they happen to be detected, are identified long after they have been exploited by hackers. Therefore, in the field of computer security it is common consideration of the lack thereof.

Nevertheless, there are several systems used for the technological protection by IT tools, such as: the use of "secure" web communication protocols (https), conditional access through username and password, biometric identification means or any other tools intended for this purpose, apart from other additional means that the user can use in addition, such as the use of proxies or VPNs, for example.

1.4. The usual means of computer-based communication hacking

Without delving into purely technical aspects, the data show that, despite the attempts to protect communications, there exist innumerable means that try to obtain unauthorized access. Among them, there can be found the following: brute force crackers of users and passwords (which obtain access data through the trial and error system, trying various alphanumeric combinations starting from one digit, moving on to two digit passwords, three digit passwords and

so on until the correct one is found)[6]. However, with the evolution of CPUs (central computer processors) and GPUs (graphics processors) these processes are becoming faster and easier, turning into child's play as far as the imminent rise of usage of quantum computers is concerned, however still restricted to large corporations. Other examples are: the use of data sniffers in shared networks[7] or the implementation of Trojans (programs generally hidden within the codes, whose purpose is to establish a backdoor to access the infected computer). Other means can be as follows: rootkits (set of tools that are installed on the victim's computer to obtain administrator access privileges), scripts (which are small codes that carry out unwanted actions on the attacked computer), "Man in the Middle" techniques (through unauthorized intrusion between the sender and receiver communications) or the use of Keyloggers (either physical or software, which record all keystrokes).

1.5. Intellectual property protection in Spain

For the purpose of the study, as the research is focused on Spanish legal system, Table 1 presents the names and translations of the different types of law that is subject of the paper and the abbreviations used to denote each type.

Table 1. Abbreviations used in the text

Rule	Abbreviation
Código Penal (Spanish Criminal Code)	CP
Código Civil (Spanish Civil Code)	CC
Ley de Enjuiciamiento Civil (Spanish Civil Procedure Law)	LEC
Constitución Española (Spanish Constitution)	CE

Source: own elaboration

[6] Therefore, the longer and more varied the passwords are, the longer it will take the attacking computer to obtain them.

[7] Those are applications that run on computers connected to a shared network, capturing packets of information sent by the other computers, to obtain those containing the data necessary to establish a connection with them.

The respect of intellectual property is one of the most conflictive aspects of new technologies, due to the ease of incorporating third party contents, which are not copyrighted. The protection of these rights has been in place for decades at the international level. Historically, we can find a division between intellectual and industrial property rights, as it can be observed in the elaboration of specific conventions on each subject. The first one is the Paris Convention for the Protection of Industrial Property, signed on March 20, 1883, applicable to industrial property in an extensive manner, including patents, trademarks, industrial designs, utility models, service marks, trade names, geographical indications and the repression of unfair competition. Second one is the Berne Convention for the Protection of Literary and Artistic Works, signed on September 9, 1886, for the protection of intellectual property. Subsequently, through the Convention establishing the World Intellectual Property Organization, signed in Stockholm on July 14, 1967, the World Intellectual Property Organization (WIPO) was created, which is now part of the United Nations (UN). Later, the Agreement on Trade-Related Aspects of Intellectual Property Rights, signed in Marrakech, on April 15, 1994, of the World Trade Organization (WTO) was created and, within the European Union, both rights have been jointly dealt with by means of Directive 2004/48/EC[8] of the European Parliament and of the Council of April 29, 2004, on the enforcement of intellectual property rights.

Within the Spanish legal system, it can be found both in civil and criminal proceedings. This protection stems from article 20 EC, which defends it as a fundamental right.

This right to intellectual property is protected in Chapter III, Title IV, of the Second Book of the Código Civil (CC), which in Article 428 stipulates that the author of a literary, scientific or artistic work has the right to exploit and dispose of it at will, while the following article adds that the Law on Intellectual Property shall determine the persons to whom this right belongs, the form of its exercise and the time of its duration. The content of this article must be brought into line with article 348, which states that ownership is the right to enjoy and dispose of a thing, with no other limitations than those established

[8] EC stands for European Comission.

by law, and adds that the owner has the right to an action against the holder and possessor of the thing to claim it. The procedure for the defence of this right by civil action is contemplated in articles 249 and following of the Spanish Procedure Law (Ley de Enjuiciamiento Civil- LEC in Spanish).

More specifically, the second final provision of Law 27/1995, of October 11, 1995, transposing into Spanish law the Council Directive 93/98/EEC, of October 29, 1995, harmonizing the term of protection of copyright and certain related rights, gave rise to the creation of the specific law in the field of intellectual property, through the publication of Royal Legislative Decree 1/1996, of April 12, 1996, which approved the Consolidated Text of the Intellectual Property Law.

For its part, the CP includes crimes against intellectual property in Section 1, crimes related to intellectual property, of Chapter XI, crimes related to intellectual and industrial property, the market and consumers, of Title XIII of the crimes against property and against the socioeconomic order. It differentiates between the basic type of article 270 CP, which in its first section defines this crime as the conduct consisting of acting, for profit and to the detriment of a third party, of reproducing, plagiarizing, distributing, publicly communicating or in any other way economically exploiting, in whole or in part, a literary, artistic or scientific work or performance, or its transformation, interpretation or artistic execution fixed in any type of support or communicated by any means, without the authorization of the holders of the corresponding intellectual property rights or their assignees. On the other hand, we also find the aggravated type, in article 271 CP and the privileged type, in section 4 of article 270 CP.

1.6. The right to honour, intimacy and self-image in Spanish legal system

The other aspect that needs to be analysed legally is the respect for honour, privacy and self-image. These are important aspects when using new communication technologies, since it is not difficult to violate the legislation on this matter when adding content to the tools provided by modern online tools. Especially, it takes place when publishing data, images or comments referring

to third parties without their authorization, apart from the possible cases of libel offenses under article 208 and following of the CP (understood as the action or expression that injures the dignity of another person, undermining his reputation or undermining his own esteem). Another example is slander, under article 205 and following of the CP, consisting of the imputation of a crime made with knowledge of its falsity or reckless disregard for the truth. All of aforementioned types of crimes are common in social media and online environment.

This is a fundamental right contained in article 18 of the Spanish Constitution (*Constitución Española-CE*), which establishes in its first paragraph that the right to honour, to personal and family privacy and to one's own image is guaranteed, in accordance with Article 8 of the Convention for the Protection of Fundamental Rights and Freedoms, signed in Rome on November 4, 1950.

These fundamental rights are specifically developed in Spanish Organic Law 1/1982, of May 5, 1982, on the civil protection of the right to honour, to personal and family privacy and to one's own image.

As for their protection from the criminal point of view, these rights are protected in Chapter I of Title X of the CP, relating to crimes against privacy, the right to one's own image and the inviolability of the home, in articles 197 and following.

2. Methodology used in the study

The starting point of the present research is the assumption that the appearance of new communication technologies has given rise to the new typology of cybercrimes, either as an adaptation of existing crimes, or as completely new kind of crimes. Although the technical level of users´ skills has been increasing over time, it is also true that they may not have yet reached a sufficient level of knowledge regarding cyber environment to be able to discern which behaviours can be considered as criminal in online environment. Therefore, presumption for the study states that, we may find actions that border or go beyond the legally established limits since the rise of new technologies, especially in '90s.

The main aim of this research is to determine whether the growth of the computer technologies of communication has led to an increase in the number of criminal offenses, and whether there is really a considerable incidence of cybercrimes in Spain. For that purpose, few specific objectives have been set:

SO1: to describe the evolution of cybercrime in Spain
SO2: to determine the typology of cybercrimes in Criminal Code of Spain and describe the overall jurisdiction for each type
SO3: to determine the overall number of sentences regarding cybercrime in Spain and per type as well as the ruling
SO4: to determine the level of popularity of cybercrimes on Internet

The study applied the content analysis approach of the legal database and IA based tools for online data mining and was conducted in several stages.

To begin with the study, first of all we have examined the evolution of the cybercrimes in Spain and conducted the analysis of the types of cybercrimes existing in the Spanish Criminal Code in relation to online technologies.

As the second step, among all the criminal offenses related to computer-based communication we have found, we attempted to determine which have been newly created, that is to say, which types of offenses did not exist before the development of digital technologies. Subsequently, the study identifies and enumerates the denominations that have been applied to these newly established crimes.

In addition to this, by applying the Tirant lo Blanch Premium Database (www.tirantonline.com), there has been implemented the exhaust analysis of the sentences relating to each type of the criminal offenses regarding new communication technologies that appear in the Spanish CP (Penal Code). This step helped to determine to what extent the legal precepts that regulate the digital crimes are being violated and what particularities they represent.

Once this analysis has been concluded, we have proceeded, through the use of the artificial intelligence tool Tirant Analytics, to determine which are the legal characteristics evidenced in the sentences related to different types of cybercrimes in Spanish legal system and jurisdiction. The date of the data

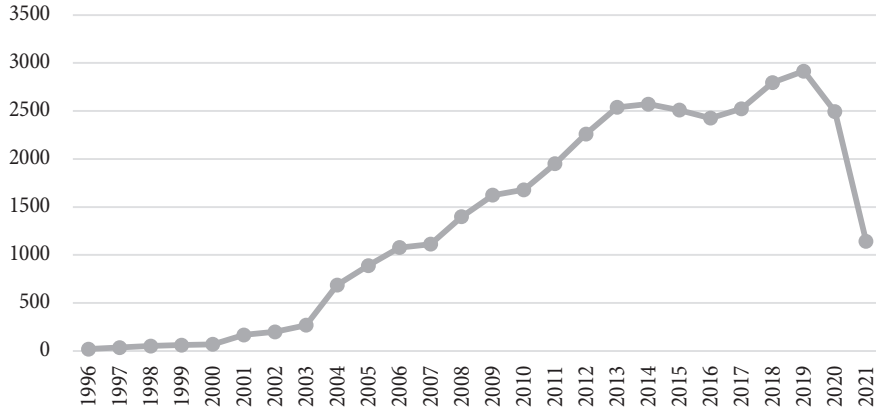
collection was September 11, 2021, and the query range has been the complete content of the database, that is, all the criminal sentences that have been recorded since 1870 (although it must be taken into account that, logically, this type of crime has been observed in a significant way since 1995).

Once these new types of crimes were determined, using the Twitter hashtag analysis tool, Hashtagify (https://hashtagify.me), the research focused on the dissemination and popularity indexes of the new crimes, to determine whether we are really facing new criminal figures in expansion process. The data analyzed were the values obtained on September 11, 2021 referring to popularity, recent popularity, month trend and week trend.

3. Results

As the starting point, there can be observed that, prior to 1995, as is logical due to the still scarce development of these technologies (it must be taken into account that the Internet boom began in 1995, although it comes from the previous Arpanet of 1969), we do not find a significant number of cases related to computer crimes. From 1995 onwards an exponential growth is observed, until reaching the year 2019 in which we appreciate an abrupt drop in this type of cases as represented by Figure 1.

Figure 1. Number of the sentences per year that are related to cybercrimes.

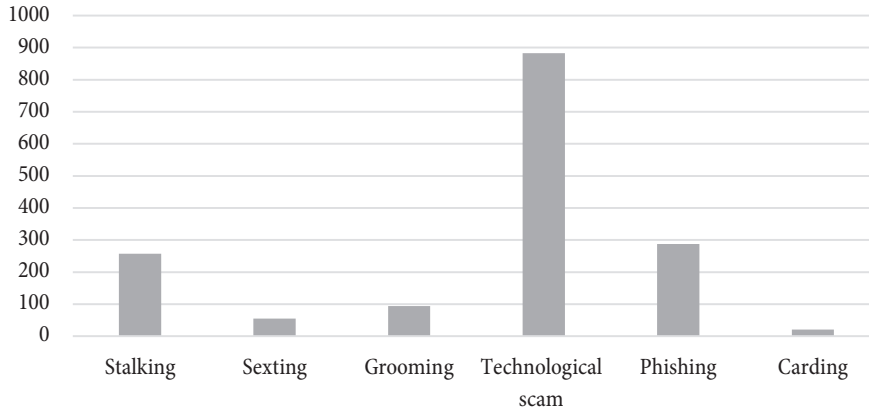


Source: own elaboration on the base of Tirant Analytics data (September 2021).

Regarding the presence of information technologies crimes in Spanish legal system, the variety of existing computer crimes is almost endless, and continues to grow as new technologies evolve. As such, in Spanish CP, there can be found the following crimes: crime of interception of communications (article 197.1 CP), access to confidential data (article 197.2 CP), intrusion into computer equipment (article 197.2 CP), dissemination of illegally obtained data (article 197. 3 CP). Besides there are contemplated the crimes of deleting, damaging, deteriorating, altering, suppressing or making inaccessible data, computer programs or electronic documents of others (article 264 CP). Among the new type of computer-related crimes, there are: Carding (consisting of the use or generation of other people's credit cards in an unlawful manner), the use of Phishing or social engineering techniques. The latter are techniques that try to deceive the victim, such as messages or calls impersonating the operator of the service they wish to access illegitimately, in order to provide them with their access data, bank details or any other data. In addition, those aforementioned examples are only few among many others.

Nevertheless, crimes related to new technologies are not limited to actions of a markedly technical nature such as those mentioned above. In this sense, the new criminal behaviours related to the ever-evolving digital media are appearing constantly. Simultaneously, such behaviours become specialization of everyday crimes in the online environment, such as: stalking (consisting of harassment or stalking of the victim in Internet), the dissemination of content coming from sexting (dissemination of videos or images of erotic or pornographic content) without the consent of the author, or online grooming (which refers to the action of an adult aimed at convincing a minor to engage in sexual relations). The Figure 2 presents the typology of the most common crimes by the number of sentences issued for each type.

Figure 2. The number of sentences that contain the new terms created for the new crimes proceeding from new technology usage.



Source: own elaboration on the base of the judicial data base of Tiran lo Blanch (from 1995 onwards).

As the above figure shows, the technological scam is the type of cybercrime most numerous as it accounts for almost 900 sentences while phishing and stalking for almost 300 sentences, being phishing more common in comparison to stalking as the numbers show.

Apart from all this, we find crimes that, in principle, have nothing to do with the new technologies in their origin; though happen to have a place through them. Those can be the following ones: the crimes against intellectual property (article 270 CP and following), crimes against industrial property (articles 273 CP and following), threats (article 169 CP and following), slander (article 205 CP and following), libel (article 208 CP and following), inducement to prostitution (article 187 and 188 CP) or the recruitment of minors or persons with disabilities in pornographic shows or the distribution or sale of such material (article 189 CP), and computer fraud (article 248. 2 CP). The Table 2 shows the most common crimes and its typology in Spanish Penal Code.

Table 2. The most common crimes related to the new technologies and its typology in CP.

Crime	Article CP	Number of Sentences
Interception of communication	197.1	352.255
Access to protected data	197.2	
Intrusion into IT equipment	197.2	
Diffusion of data obtained illegally	197.3	
IT sabotage	264	13.054
Crimes against intellectual property	270 & ss.	13.157
Crimes against industrial property	273 & ss.	13
Stalking	172 ter & 173.2	403
Sexting	197.7	32.255
Online Grooming	183	1.274
Threats	169	759
Libel	205	113
Slander	208	245
Induction to a prostitution	187 y 188	260
Capturing of the under age or disable people for pornographic show or the distribution thereof	189	731
IT scams (Phishing, Carding, etc…)	248.2	15.106

Source: own elaboration on the base of data obtained from the Tirant lo Blanch legal database (from 1995 onwards).

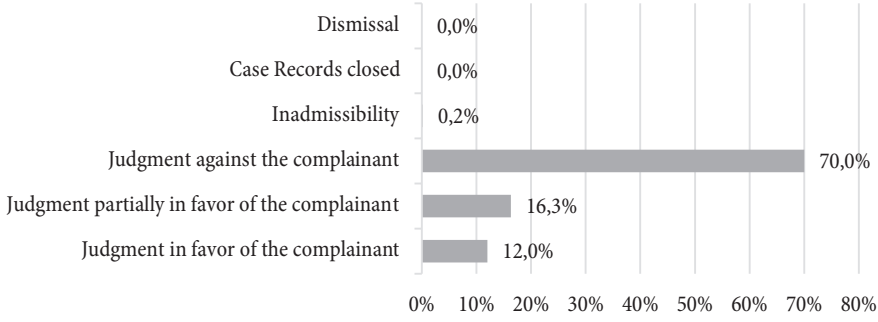
The analysis of the sentences issued in Spain concerning cybercrimes in general concluded with 429,625 sentences in total. The finding show that the crimes of interception of communications, access to confidential data, intrusion of computer equipment, and dissemination of data obtained unlawfully (all regulated in article 197.3 of the CP) account for 82% of the all sentences so far in these cases. The second crime that accumulated a greater number of sentences is sexting, regulated in section seven of article 197 of Spanish CP, which accounts for 8% of all the sentences analysed. Next, there are the crimes related to computer frauds, as regulated in article 248.2 of the CP, which represent 4% of the sentences. Those are followed by the crimes related to intellectual property (from articles 270 and following of the CP), with 3%. The crimes of

computer sabotage, contemplated in article 264 of the CP, also represents 3% of the sentences. Other types of crimes do not reach 1% of the sentences.

Far from these extremes, with an incidence of sentences below 1,000, there can be found crimes of threats made by means of electronic tools, regulated in article 169 CP, with 759 sentences. Next, there are listed the crimes of solicitation of minors or disabled persons for pornographic performances or the distribution of those (article 189 CP, with 731 sentences). Furtherly, numbers of sentences go below 500 sentences in the following order: the crimes of Stalking (regulated in articles 172 ter and 173. 2 CP) with 403 sentences, the crime of inducing prostitution (regulated in articles 187 and 188 CP), with 260 sentences, the crime of slander (as conceptualised in the article 208 CP) numbering 245 sentences, the crime of libel (regulated in articles 205 and following of the CP) presenting 113 sentences, and finally crimes against intellectual property with only 13 sentences.

As per the analysis of the ruling present in cybercrimes sentences, that was carried out with the help of the artificial intelligence tool Tirant Analytics in September 2021, the results obtained have determined the most common type of ruling of the sentences, as Figure 3 demonstrates. These are as follows: rejection, in 70% of the cases, followed by cases with partial estimation, reflected in 16.3% of the cases, judgments with an estimatory ruling, in 12% of the cases, and cases of inadmissibility in 0.2% of the cases. The relevant number of dismissal or dismissal orders have not been found.

Figure 3. Type of the ruling present in the cybercrime sentences.



Source: own elaboration on the base of the results obtained from Tirant Analytics in September 2021.

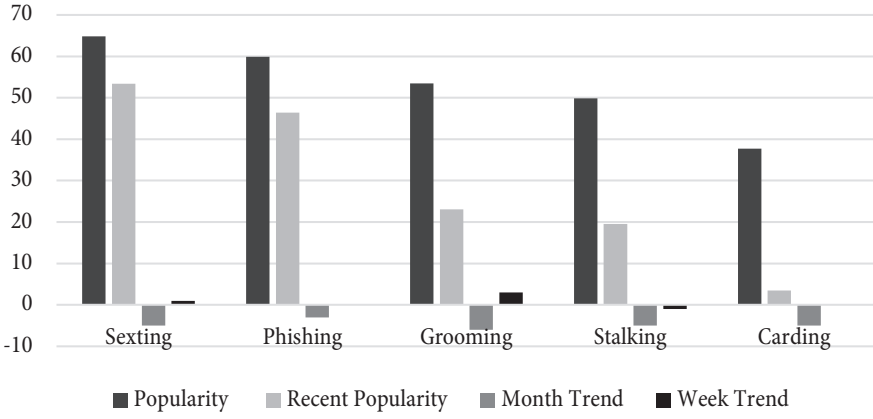
With regard to the modifying circumstances observed in the sentences, the most common was the aggravating circumstance of kinship, alleged in 9% of the cases, followed by the analogous mitigating circumstance of confession, the analogous circumstance of affective relationship, and the mitigating circumstance of undue delay, all of which were observed in 8% of the cases.

As far as the raising of procedural issues are concerned in cybercrimes ruling, the most common were precautionary measures and the poisoned tree theory, which were observed in 11% of the sentences. These were followed with the internal inconsistency, observed in 10% of the sentences. Finally, the prejudicial question, territorial jurisdiction, incidental question, and civil precautionary measures accounted for 9% of the sentences.

Within the elements as per the type, we find the appearance of the element of malice in 11% of the sentences, *animus laedendi*, in 10% of the analysed cases, and recklessness or profit motive, in 8% of sentences.

As far as the analysis applying Hashtagify tool is concerned, aimed to demonstrate the relative popularity of certain cybercrimes in online environment, the results show the most used hashtags related to these new electronic crimes, which are: Stalking, Sexting, Grooming, Phishing and Carding, according to data included in Figure 4.

Figure 4. Hashtags related to the new crimes arisen from new technologies.



Source: own elaboration on the base of the results obtained from Hashtagify (September, 2021).

The results demonstrate that all of these aforementioned types have become significantly popular, both as the current trend and as accumulated number over a certain time range. #Sexting is the most popular among those analysed with 64.8%, followed by #Phishing with 59.9%, #Grooming with 53.5%, #Stalking with 49.9%, and finally #Carding with 37.7%. This leads to the observation that the commission of these new crimes is really widespread and common.

4. Discussion and conclusions

The study confirms the growth and complexity of the criminal offenses in cyber environment, with a considerable incidence of cybercrimes in Spain. Those factors drive the increasing popularity of such types of crimes in online ecosystem, as hashtags analysis showed.

Nevertheless, the discussion within this field of study may be endless. For some authors, such as Velasco Núñez[9], fraud, which is often said to be characteristic of advanced societies where access to the property of others does not require the use of violence, is the computer crime par excellence, the one that occurs the most, reaching a 70% share among cybercrimes. Meanwhile for other authors, such as Gorjón[10], hacking and computer sabotage, can be defined as pure cyber-attacks, where the object of attack are the systems themselves because they refer to attacks that were born with the very development of the Internet and the popularization of the use of new technologies. However, for Domínguez Rocha[11], many criminally reprehensible conducts exclusive to the Internet, such as sexting, stalking, grooming, etc., can be redirected to the figure of insults, insofar as in them appears the intention to injure the honour or good name of the third party, whether in one or another factual form, a criterion is shared only partially.

---

[9] E. Velasco Núñez, *Delincuencia Informática*, Tirant lo Blanch 2019, *passim*.

[10] M.C. Gorjón Barranco, *Ciberterrorismo y Delito de Odio motivado por ideología*, Tirant lo Blanch 2019, *passim*.

[11] D. Domínguez Rocha, *Globalización y lucha contra las nuevas formas de criminalidad transnacional*, Tirant lo Blanch 2019.

The results obtained in the three modes of analysis clearly show that we are obviously facing a significant number of crimes related to new technologies. The development of computer-based communication tools has given rise to about half a million sentences in Spain. Many of offences already existed, before the increasing popularity of Internet from 1995 onwards, but for which there has been an adaptation to the digital format. There can be also found many other crimes, hitherto unpublished, which have been born in the shadow of these new tools, such as, for example, unethical Hacking, Cracking, computer sabotage, Stalking, Sexting, Online Grooming, Phishing, Carding, or Flaming.

The types of offenses that occur most frequently are those regulated in Title X, Book II, of the CP, and more specifically in article 197 CP. However, another important group of cybercrimes can be noticed, which are those related to intellectual property. The phenomenon takes place because, as mentioned above, there may be a lack of knowledge about the legal limits regarding the use of material or content whose authorship belongs to a third party, or simply a lack of concern in this regard.

There are the crimes that raise a particular concern: those of a sexual nature that have a place within the computer-based crimes through criminal figures such as grooming, stalking, or sexting. They are often related to minors, marking a high popularity and topicality, as it could be observed from the analysis carried out with Hashtigify. In this sense, as Ibáñez[12] states, the introduction of the various reforms of the Criminal Code of these criminal behaviours (known as Sexting, Grooming, Cyberbullying, Phishing, Stalking, Hacking, Cracking, etc.) may become an important tool to stop the advance of criminal behaviours arising from technological development. Nevertheless, the legislator, as on other occasions, lags behind the criminal reality and missed the opportunity to regulate the emergence of new risks and threats related to cyber environment.

According to Sánchez[13], many efforts have been made to analyse the dialectic between freedom and security in cyberspace. In any case, when speaking of this type of crime, a diffuse territory lacking in regulation is usually overviewed.

[12] F.L. Ibáñez López-Pozas, *La nueva reforma procesal penal. Derechos fundamentales e innovaciones tecnológicas*, Tirant lo Blanch 2019, *passim*.

[13] A. Sánchez Magro, *Principios de Derecho de Internet*, Tirant lo Blanch 2005, *passim*.

As Velasco San Martín[14] states, when speaking of the terms such as cybercrime or computer crime, just like the term cybersecurity, there is no singular and universally accepted definition. In some countries, the expression computer crime is used, while in others it is referred to as cybercrime or cyber offence or simply crimes committed through computer systems and the Internet. In this sense, it is not even easy to specify the scope these crimes may cover. Such lack of data may be caused, as Ibáñez[15] comments, because we are faced with criminal behaviours that according to the CP affect eight different legal assets that represent at least eighteen different criminal types.

However, its difficult delimitation is not the only complication, since, agreeing with García[16], the truth is that it is a field where the application of the law is particularly complex precisely because of the problems of location of the authors and the computer borders that do not coincide with the state powers for the application of their jurisdictions. In addition to these pitfalls, as defended by Domínguez Pérez[17], the difficulties are centered on the technical issues in accessing the servers that store and distribute the information, which, moreover, in principle, are not responsible for the illicit content of the information they host or contribute to disseminate. In addition, and to further complicate the picture, the current global pandemic situation has led, according to Lopez[18], to the confinement leading to a shift of crime into cyberspace, increasing the quantity and typology of the cybercrimes themselves.

Therefore, the essential conclusions drawn consider cybercrime in Spain as a particularly dynamic and changing field of study, in which the birth of new forms of crime is ahead of the creation of the various regulations. Furthermore, the study of the cybercrime in Spain is complicated even due to the

---

[14] C. Velasco San Martín, *Jurisdicción y competencia penal en relación al acceso transfronterizo en materia de ciberdelitos*, Tirant lo Blanch 2015, *passim*.

[15] F.L. Ibáñez López-Pozas, *op. cit.*, *passim*.

[16] R. García García, *Libertad de Expresión y Prevención de la Violencia y Discriminación por razón de religión*, Tirant lo Blanch 2020, *passim*.

[17] E.M. Domínguez Pérez, *Tutela jurídica de bienes culturales y avances en la lucha contra el tráfico ilícito*, Tirant lo Blanch 2019, *passim*.

[18] J. López Gorostidi, *Los valores tradicionales como bienes jurídicos protegidos también en el ciberespacio: a propósito del confinamiento provocado por la crisis sanitaria del COVID-19*, *Revista Penal*, 47, enero 2021, *passim*.

simple lack of the coherent definition that would manage to conceptualise and delimit its content. Additionally, there exist another difficulty in determining those responsible for the unlawful conduct, which is evidenced by the fact that 70% of the sentences are dismissed. Nevertheless, it must be admitted that this type of crime is already a reality in Spain, having become an important subset within the group of everyday crimes, and is growing exponentially, accelerated even more by the existing pandemic situation.

Bibliography

References

Bilbeny N., *La revolución en la ética. Hábitos y creencias en la sociedad digital*, Anagrama 1997.

Chambat P., *Usages des technologies de l'information et de la communication* (*TIC*): *évolution des problématiques*, "Technologies de l'information et société" 1994, vol. 6, 3. Dunod.

Domínguez Pérez E.M., *Tutela jurídica de bienes culturales y avances en la lucha contra el tráfico ilícito*, Tirant lo Blanch 2019.

Domínguez Rocha D., *Globalización y lucha contra las nuevas formas de criminalidad transnacional*, Tirant lo Blanch 2019.

García García R., *Libertad de Expresión y Prevención de la Violencia y Discriminación por razón de religión*, Tirant lo Blanch 2020.

Gorjón Barranco M.C., *Ciberterrorismo y Delito de Odio motivado por ideología*, Tirant lo Blanch 2019.

Hughes T.P., *Technological momentum En M.R. Smith, & L. Marx* (*Eds.*). *Does Technology Drive History? The Dilemma of Technological Determinism*, MIT Press 2019.

Ibáñez López-Pozas F.L., *La nueva reforma procesal penal. Derechos fundamentales e innovaciones tecnológicas*, Tirant lo Blanch 2019.

López Gorostidi J., *Los valores tradicionales como bienes jurídicos protegidos también en el ciberespacio: a propósito del confinamiento provocado por la crisis sanitaria del COVID-19*, *Revista Penal*, 47, enero 2021.

Rogers E.M., *Diffusion of Innovations*, The Free Press 1983.

Sánchez Magro A., *Principios de Derecho de Internet*, Tirant lo Blanch 2005.

Velasco Núñez E., *Delincuencia Informática*, Tirant lo Blanch 2019.

Velasco San Martín C., *Jurisdicción y competencia penal en relación al acceso transfronterizo en materia de ciberdelitos*, Tirant lo Blanch 2015.

Williams R., *Television, technology and cultural form*, Schocken Books 1975.

Table of legislation

Agreement on Trade Related Aspects of Intellectual Property Rights, Annex 1C to the Marrakesh Agreement establishing the World Trade Organization (WTO), 33 ILM 1197 (1994). https://bit.ly/2YMd6JS

Berne Convention for the Protection of Literary and Artistic Works (1896). *World Intellectual Property Organization*. https://bit.ly/2YMdeJm

Constitución Española, de 27 de diciembre de 1978. (1978). *Boletín Oficial del Estado*, 311, de 29 de diciembre de 1978. https://bit.ly/3DzUtay

Directive of The European Parliament and of the Council 2004/48/EC, [2004] OJ L 157/45. https://bit.ly/3DHFFqm

Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. (2000). *Boletín Oficial del Estado*, 7, de 8 de enero de 2000. https://bit.ly/3AGXPa2

Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. *Boletín Oficial del Estado*, 115, de 14 de mayo de 1982. https://bit.ly/3aA0Ga3

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. (1995). *Boletín Oficial del Estado*, 281, de 24 de noviembre de 1995. https://bit.ly/3DGBhbm

Paris Convention for the Protection of Industrial Property (1883). *World Intellectual Property Organization*. https://bit.ly/3FJBVqd

Real Decreto de 24 de julio de 1889, por el que se publica el Código Civil. (1889). *Gaceta de Madrid*, 206, de 25 de julio de 1889. https://bit.ly/3AFPwv4

Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia. (1996). *Boletín Oficial del Estado*, 97, de 22 de abril de 1996. https://bit.ly/3BJHoMR

Roma Convention for the Protection of Human Rights and Fundamental Freedoms. *European Court of Human Rights* (*1950*). https://bit.ly/3lHADUA

Stockholm Convention Establishing the World Intellectual Property Organization (1967). *World Intellectual Property Organization*. https://bit.ly/3vjyZMo

Maciej Domański, Jerzy Słyk

Bezpieczeństwo dziecka korzystającego z przedmiotów komunikacji elektronicznej a wykonywanie władzy rodzicielskiej

1. Wprowadzenie

Wychowując dziecko, rodzice nieuchronnie napotykają wyzwania związane z rozwojem technologii informatycznych, z których ono korzysta. Niezależnie od przyjętego modelu wychowawczego nie jest możliwe (a w dzisiejszych czasach raczej również nie jest wskazane) całkowite odcięcie dziecka od elektronicznych narzędzi komunikacji. Zwłaszcza w okresie pandemii COVID-19 formy kontaktu służące pracy zdalnej z wykorzystaniem narzędzi informatycznych stały się standardem komunikacji. Praktycznie nie istnieją telefony niewyposażone w rozbudowane funkcje. Presja środowiska rówieśniczego determinuje pragnienia dziecka posiadania określonych urządzeń i oprogramowania. Jest oczywiste, że korzystanie przez dziecko z narzędzi informatycznych generuje zagrożenia, którym powinni przeciwdziałać rodzice odpowiedzialni za jego wychowanie.

W niniejszym artykule podjęto próbę określenia uwarunkowań i konsekwencji wykonywania przez rodziców władzy rodzicielskiej w aspekcie zagwarantowania bezpieczeństwa dziecku korzystającemu ze środków komunikacji elektronicznej na gruncie polskiego prawa rodzinnego. W pierwszej części omówione zostaną podstawowe założenia konstrukcyjne instytucji władzy rodzicielskiej oraz wybrane uwarunkowania tej instytucji prawami człowieka. W części drugiej podjęte zostaną zagadnienia cywilnoprawne związane z wykonywaniem zarządu majątkiem dziecka oraz posługiwaniem się przez dziecko przedmiotami służącymi komunikacji elektronicznej.

2. Władza rodzicielska – konstrukcja normatywna a bezpieczeństwo dziecka w cyberprzestrzeni

Najczęściej przywoływana w piśmiennictwie definicja „władzy rodzicielskiej" ujmuje ją jako **ogół obowiązków i praw rodziców względem dziecka, służących zapewnieniu mu należytej pieczy i strzeżeniu jego interesów**[1]. W podobnym ujęciu władzę rodzicielską określono jako **całokształt uprawnień i obowiązków rodziców względem małoletniego dziecka w celu zapewnienia pieczy nad jego osobą i majątkiem**[2]. J. Strzebińczyk wskazuje, że **władza rodzicielska jest instrumentem prawnym umożliwiającym rodzicom przede wszystkim ostateczne psychofizyczne ukształtowanie dziecka**[3]. Omawianą instytucję prawną definiować można również przez wskazanie elementów jej treści. Mimo pewnych niekonsekwencji konstrukcyjnych w treści przepisów kodeksowych[4], zazwyczaj wskazuje się, że elementami władzy rodzicielskiej są: **piecza nad osobą** dziecka, **piecza nad majątkiem** dziecka oraz **reprezentacja** (przedstawicielstwo ustawowe)[5]. Rekonstrukcja zakresu znaczeniowego elementu osobowego władzy rodzicielskiej jest w doktrynie prawa rodzinnego dokonywana w różny sposób. Szczegółowe omówienie tych różnic przekracza ramy niniejszego artykułu[6]. Dla jego celów wskazać można, że np. zdaniem J. Ignatowicza, piecza nad osobą dziecka obejmuje obowiązek jego wychowania, kierowania dzieckiem, troskę o zapewnienie mu odpowiednich warunków egzystencji

---

[1] J. Ignatowicz, [w:] *System prawa rodzinnego i opiekuńczego*, red. J.S. Piątowski, Wrocław 1985, s. 804.

[2] T. Smyczyński, M. Andrzejewski, *Prawo rodzinne i opiekuńcze*, Warszawa 2020, s. 258.

[3] J. Strzebińczyk, [w:] *System Prawa Prywatnego. Tom 12. Prawo rodzinne i opiekuńcze*, red. T. Smyczyński, Warszawa 2011, s. 235.

[4] Zgodnie z art. 95 Kodeksu rodzinnego i opiekuńczego (ustawa z dnia 25 lutego 1964 r., Dz.U. z 1964 r. Nr 9, poz. 59 z późn. zm., dalej: k.r.o.), władza rodzicielska obejmuje w szczególności obowiązek i prawo rodziców do wykonywania pieczy nad osobą i majątkiem dziecka oraz do wychowania dziecka, zaś art. 96 k.r.o., określający elementy pieczy nad osobą dziecka, wymienia jego wychowanie i kierowanie nim oraz troskę o fizyczny i duchowy rozwój dziecka.

[5] Por. np. K. Jagielski, *Istota i treść władzy rodzicielskiej*, „Studia Cywilistyczne" 1963, t. III, s. 122–123.

[6] Por. np. zestawienie poglądów przedstawionych w doktrynie: J. Słyk, [w:] *Kodeks rodzinny i opiekuńczy. Komentarz Przepisy wprowadzające KRO*, red. K. Osajda, Warszawa 2017, s. 1210–1212.

oraz **bezpieczeństwa**[7]. Element pieczy nad majątkiem dziecka obejmuje zarząd majątkiem dziecka. Posłużenie się przez ustawodawcę terminem „piecza nad majątkiem" sugeruje szerszy zakres tego obowiązku, obejmujący troskę o dobro dziecka a więc o jego bezpieczeństwo[8].

Kształtując stosunek prawny władzy rodzicielskiej[9], ustawodawca konsekwentnie na plan pierwszy wysuwa kategorię **obowiązku** ciążącego na rodzicach. Takie podejście znalazło odzwierciedlenie również w orzecznictwie Sądu Najwyższego, który w fundamentalnej uchwale z 9 czerwca 1976 r.[10] wskazał, że władza rodzicielska to przede wszystkim zespół obowiązków względem dziecka, a uprawnienia rodziców w stosunku do dziecka są niejako wtórnym składnikiem tej władzy. Stanowisku temu nie przeczy inny pogląd zawarty w uchwale SN z 26 stycznia 1973 r., III CZP 101/71, OSNCP 1973, nr 7–8, poz. 118, zgodnie z którym władza rodzicielska oznacza stosunek prawny szczególnego rodzaju, w którym dzieci są **podporządkowane** rodzicom.

Najważniejszą dyrektywą determinującą sposób wykonywania władzy rodzicielskiej w polskim prawie rodzinnym jest zasada dobra dziecka. Stanowi ona jednocześnie naczelną zasadę całego prawa rodzinnego, a w odniesieniu do władzy rodzicielskiej wynika wprost z treści art. 95 § 3 k.r.o.

Podsumowując powyższe uwagi, należy wskazać, że w kontekście głównego problemu niniejszego opracowania, tj. wykonywania władzy rodzicielskiej w związku z korzystaniem przez dziecko ze środków komunikacji elektronicznej, istotne są następujące stwierdzenia:

---

[7] J. Ignatowicz, [w:] *System*…, s. 813.

[8] Relacja znaczeniowa pojęć „pieczy nad majątkiem" i „zarządu majątkiem dziecka" również jest przedmiotem kontrowersji w piśmiennictwie; por. na ten temat np. J. Słyk, *op. cit.*, s. 1212; co do samego pojęcia „zarządu majątkiem dziecka" por. np. K. Gołębiowski, *Uwagi dotyczące zarządu majątkiem dziecka pozostającego pod władzą rodzicielską*, [w:] *Wybrane zagadnienia polskiego prawa prywatnego. Księga pamiątkowa ku czci Doktora Józefa Kremisa i Doktora Jerzego Strzebińczyka*, red. J. Jezioro, K. Zagrobelny, Wrocław 2019, s. 125 i n.

[9] Poza zakresem niniejszego artykułu pozostaje rozważanie różnic poglądów doktryny definiujących władzę rodzicielską w kategoriach prawa podmiotowego lub sprzeciwiających się takiemu ujęciu; por. zestawienie tych ujęć: J. Słyk, *op. cit.*, s. 1199.

[10] Uchwała SN z dnia 9 czerwca 1976 r., III CZP 46/75, OSNCP 1976, Nr 9, poz. 184, teza XIII.

1/ władza rodzicielska jest wykonywana m.in. w celu zapewnienia dziecku **bezpieczeństwa**,
2/ wykonywanie władzy rodzicielskiej jest przede wszystkim **obowiązkiem** rodziców, a dziecko jest winne rodzicom **posłuszeństwo**,
3/ najważniejszym wyznacznikiem sposobu wykonywania władzy rodzicielskiej jest **dobro dziecka**.

Rodzice, którym przysługuje władza rodzicielska, są zatem odpowiedzialni za bezpieczeństwo dziecka w cyberprzestrzeni – tak jak w innych przestrzeniach życia. Korzystanie z technologii informatycznych generuje jednak specyficzne problemy, które wiążą się z określeniem zakresu autonomii dziecka w tej przestrzeni i dozwolonej (czy nakazanej) ingerencji rodziców[11].

W 2008 r. przeprowadzona została nowelizacja przepisów Kodeksu rodzinnego i opiekuńczego[12], która – w świetle uzasadnienia rządowego projektu nowelizacji – realizować miała model „racjonalnego partnerstwa"[13], a więc wzmacniać autonomię i podmiotowość dziecka w relacjach z rodzicami. Niezależnie od oceny samej idei nowelizacji, przeprowadzone zmiany należy ocenić krytycznie z uwagi na ich nieprecyzyjny, niejasny charakter. I tak w art. 95 § 1 k.r.o. dodano nową dyrektywę określającą sposób wykonywania władzy rodzicielskiej: wymóg poszanowania praw i godności dziecka.

Obowiązek przestrzegania praw dziecka jest oczywisty i nie wymaga proklamowania na poziomie kodeksowym, zaś kategoria godności dziecka mieści się w pojęciu jego praw, a przede wszystkim w istniejącej już w Kodeksie rodzinnym i opiekuńczym klauzuli dobra dziecka. Z punktu widzenia przedmiotu niniejszego opracowania istotniejsza jest zmiana art. 95 § 2 k.r.o. polegająca na uzupełnieniu przepisu nakładającego na dziecko obowiązek posłuszeństwa, obowiązkiem wysłuchania opinii i zaleceń rodziców w sprawach, w których może ono **samodzielnie podejmować decyzje** i **składać oświadczenia woli**.

---

[11] Egzemplifikacji zagrożeń, jakie mogą dotyczyć dziecka korzystającego z Internetu, dokonała J. Uliasz. Por. J. Uliasz, *Prawna ochrona prywatności oraz wolności dzieci w Internecie*, „Zeszyty Naukowe Uniwersytetu Rzeszowskiego" 2020, z. 110, s. 285 i n.

[12] Ustawa z dnia 6 listopada 2008 r. o zmianie ustawy – Kodeks rodzinny i opiekuńczy oraz niektórych innych ustaw (Dz.U. Nr 220, poz. 1431).

[13] Projekt ustawy o zmianie ustawy – Kodeks rodzinny i opiekuńczy oraz niektórych innych ustaw, Druk sejmowy VI kadencji nr 888.

Pojawia się wątpliwość, czy w przypadku tym na dziecku nie ciąży obowiązek posłuszeństwa, a jedynie wysłuchania opinii i zaleceń rodziców. Niejasne jest sformułowanie odwołujące się do możliwości samodzielnego podejmowania decyzji przez dziecko – trudno określić jakie jest odniesienie normatywne tej przesłanki. Wątpliwości mogą z całą mocą ujawnić się w przypadkach korzystania przez dziecko ze środków komunikacji elektronicznej, zwłaszcza co do dzieci mających ukończone 13 lat, które posiadają ograniczoną zdolność do czynności prawnych i mogą dokonywać czynności prawnych. W przypadku młodszych dzieci, niezdolnych do czynności prawnych, ustawodawca dopuszcza zawarcie umowy powszechnie zawieranej w drobnych bieżących sprawach życia codziennego (art. 14 § 2 Kodeksu cywilnego[14]), a więc – jak się wydaje – złożenie oświadczenia woli[15].

Korzystanie ze środków komunikacji elektronicznej przez dziecko sprawia, że możliwość wystąpienia opisanych wyżej sytuacji staje się jeszcze bardziej prawdopodobna ze względu na anonimowość w sieci. O ile dziecko, które próbuje zawrzeć umowę np. w sklepie, może napotkać przeszkody z uwagi na swój wiek, o tyle w Internecie takie ograniczenia praktycznie nie istnieją. Niezależnie od zagadnienia cywilnoprawnej skuteczności czynności prawnej dokonanej przez dziecko, na gruncie przepisów o władzy rodzicielskiej rozważenia wymaga problem zakresu autonomii dziecka, a co za tym idzie zakresu obowiązków i uprawnień rodziców. Uwzględniając całokształt regulacji Kodeksu rodzinnego i opiekuńczego, a zwłaszcza prymat dobra dziecka oraz wychowywania jako podstawowego obowiązku rodziców, należy odrzucić możliwość gramatycznej wykładni art. 95 § 2 k.r.o. prowadzącej do ograniczenia obowiązku posłuszeństwa dziecka. Oznaczałoby to w pewnym zakresie zdjęcie z rodziców odpowiedzialności za wychowywanie dziecka, który to obowiązek realizuje się w codziennym życiu, a więc przede wszystkim w sprawach drobnych, w których

[14] Ustawa z dnia 23 kwietnia 1964 r., Dz.U z 1964 r., Nr 16, poz. 93 z późn. zm., dalej: k.c.

[15] Zagadnienie wymaga głębszej analizy i przekracza ramy niniejszego opracowania. Na temat pojęć „czynności prawnej" i „oświadczenia woli" por. np. Z. Radwański, K. Mularski, [w:] *System Prawa Prywatnego, Prawo cywilne – część ogólna, t. 2*, red. Z. Radwański, A. Olejniczak, Warszawa 2019, s. 56 i n.; W. Rozwadowski, *Spory wokół definicji czynności prawnej w polskim prawie cywilnym*, „Państwo i Prawo" 2014, nr 9, s. 53 i n.

dziecko działa samodzielnie. Niezależnie zatem od cywilnoprawnej skuteczności dokonanych przez dziecko czynności prawnych, jest ono zawsze winne rodzicom posłuszeństwo, a rodzice mają obowiązek kierować dzieckiem w tym zakresie. W szczególności dotyczy to aktywności dziecka w Internecie, czy też nabywania lub dysponowania środkami komunikacji elektronicznej, również wtedy gdy wchodzą one w skład majątku dziecka lub dziecko uzyskuje pełną zdolność prawną co do tych przedmiotów[16].

Problematyka autonomii dziecka w relacjach z rodzicami pozostaje w związku z prawami chronionymi na poziomie konstytucyjnym, w szczególności prawem rodziców do wychowania dziecka w zgodzie z własnymi przekonaniami (art. 48 Konstytucji RP z dnia 2 kwietnia 1997 r., Dz.U. z 1997 r. Nr 78, poz. 483), prawa do ochrony prawnej życia prywatnego (art. 47 Konstytucji RP), czy wreszcie wolności i ochrony tajemnicy komunikowania się (art. 49 Konstytucji RP).

W doktrynie prawa konstytucyjnego a także orzecznictwie Trybunału Konstytucyjnego prawo rodziców do wychowania dziecka jest określane jako najważniejsze prawo rodzicielskie i element praw, które mają charakter przyrodzony i naturalny i nie pochodzą z nadania państwowego, choć są wykonywane pod kontrolą państwową i społeczną[17]. Co istotne, przepis art. 48 Konstytucji RP rozszerza ochronę prawa rodziców do wychowania, gwarantując im możliwość wychowywania dziecka w zgodzie ze swoimi przekonaniami. Swoboda rodziców w tym aspekcie jest zazwyczaj podnoszona w odniesieniu do ewentualnej ingerencji osób postronnych, instytucji, kościołów czy organów państwa[18]. Z uwagi na przedmiot niniejszego opracowania istotne jest skonfrontowanie prawa rodziców z chronioną prawnie autonomią dziecka. W tym zakresie art. 48 Konstytucji RP stanowi, że wychowanie dziecka przez rodziców powinno uwzględniać stopień jego dojrzałości, wolność jego sumienia i wyznania oraz przekonania dziecka. Tak sformułowany przepis jedynie sygnalizuje

[16] Szerzej zagadnienie to zostanie omówione w drugiej części niniejszego opracowania.

[17] Por. wyroki TK z dnia: 11 października 2011 r., K 16/10, OTK-A 2011, Nr 8, poz. 80; 21 stycznia 2014 r., SK 5/12, OTK-A 2014, Nr 1, poz. 2. Por. też W. Borysiak, [w:] *Konstytucja RP. Tom I. Komentarz do art. 1–86*, red. M. Safjan, L. Bosek, Warszawa 2016, art. 48, Nb 37.

[18] Por. np. P. Sarnecki, [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz. Tom II*, red. L. Garlicki, M. Zubik, M. Derlatka, Warszawa 2016, art. 48, pkt 5.

podmiotowość i autonomię dziecka, nie daje jednak wskazań na czym owo „uwzględnianie" miałoby polegać, jaki „stopień dojrzałości" uzasadnia „uwzględnianie", jak realizują się wolności sumienia i wyznania dziecka, czy wreszcie jakie „przekonania" dziecka rodzice mają obowiązek „uwzględniać". Ponownie należy podkreślić, że korzystanie z różnych form komunikacji elektronicznej przez dziecko jest źródłem problemów w zasygnalizowanym wyżej zakresie. Przed rodzicami pojawia się perspektywa weryfikacji treści, które docierają do dziecka oraz wydania odpowiednich zakazów. Praktycznym problemem będzie przykładowo możliwość egzekwowania przez rodziców wobec starszych dzieci stosowania filtrów rodzicielskich czy oprogramowania dającego wgląd w aktywność dziecka w Internecie, w szczególności korespondencji z innymi osobami[19].

W piśmiennictwie proponuje się niekiedy poszukiwanie punktu odniesienia wyznaczającego poziom autonomii dziecka w istniejących szczegółowych regulacjach prawnych, które posługują się zazwyczaj granicą ukończenia 13. roku życia[20]. To cenne spostrzeżenie nie prowadzi jednak do w pełni satysfakcjonujących rezultatów, skoro osiągnięcie tego wieku zazwyczaj nie eliminuje uprawnień rodziców (np. zgoda na czynność prawną dokonaną przez osobę z ograniczoną zdolnością do czynności prawnych, tzw. równoległa zgoda pacjenta małoletniego i jego przedstawiciela ustawowego), a granica 13 lat nie jest jedyną granicą przyjmowaną w polskim ustawodawstwie (np. wiek 15 lat jako granica warunkowej odpowiedzialności karnej, wiek 16 lat uprawniający do wcześniejszego zawarcia związku małżeńskiego przez kobietę za zezwoleniem sądu opiekuńczego)[21].

Jak się wydaje, tendencja do podkreślania autonomii dziecka, znajdująca wyraz zwłaszcza w unormowaniach art. 48 ust. 1 zd. 2 Konstytucji RP oraz art. 95 § 2 *in fine* k.r.o. jest w pewnej mierze konsekwencją nietrafnego pojmowania

[19] Wyodrębnienie sfery aktywności dziecka w Internecie jest uzasadnione również w kontekście coraz częstszego postrzegania korzystania z Internetu jako prawa człowieka. Por. K. Stępniak, *Prawo do Internetu jako środka zapewniającego partycypację w państwie demokratycznym*, „Studia Prawnicze i Administracyjne" 2017, nr 21(3), s. 66 i n.

[20] M. Ożóg, *Prawo rodziców do wychowania dziecka zgodnie z przekonaniami w świetle Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 2997 r.*, „Studia z Prawa Wyznaniowego" 2015, t. 18, s. 271–275.

[21] Autor przywołanej w poprzednim przypisie publikacji dochodzi ostatecznie do wniosku, że ostateczną granicą osiągnięcia autonomii w sferze wolności sumienia i religii jest osiągnięcie pełnoletności. *Ibidem*, s. 275.

praw rodziców i dzieci jako sprzecznych[22]. Jak już wcześniej wskazano, właściwe rozumienie tych relacji zakłada postrzeganie uprawnień rodziców jako konsekwencji ich obowiązku wychowania dziecka, wynikającego z przysługującej im władzy rodzicielskiej i ocenianego zgodnie z priorytetem zasady dobra dziecka[23]. Granica uprawnień rodziców powinna być wyznaczana nie tyle abstrakcyjnie pojmowaną autonomią dziecka, ale wychowawczym celem ich obowiązków. Podobnie autonomia dziecka nie powinna być traktowana jako wartość sama w sobie, ale instrument pożądany w procesie wychowawczym, prowadzącym do usamodzielnienia dziecka. Wychowanie zaś jest procesem wieloaspektowym, który musi być oceniany *in casu*, w odniesieniu do konkretnej sytuacji dziecka i jako taki nie poddaje się próbom kodyfikacyjnym.

Problem określenia granic autonomii dziecka jest związany z zagadnieniem ochrony życia prywatnego i tajemnicy komunikowania się, chronionych w art. 47 i 49 Konstytucji RP[24]. W piśmiennictwie wskazuje się, że przedmiotem ochrony art. 49 Konstytucji RP są wszelkie okoliczności związane z podejmowaniem czynności komunikowania się, a podmiotem jest każdy[25]. Określony konstytucyjnie zakres ochrony ma więc charakter szeroki tak pod względem przedmiotowym, jak i podmiotowym, a jej ograniczenie musi wynikać z ustawy

[22] Jak słusznie wskazano w piśmiennictwie, „tłumaczenie i stosowanie przepisów normujących treść i wykonywanie władzy rodzicielskiej z jednej strony oraz przepisów gwarantujących dziecku jego prawa z drugiej strony, nie powinno ani zakładać, ani powodować przeciwstawności praw i obowiązków rodziców oraz praw dziecka". M. Nazar, *Niektóre zagadnienia małżeństwa i rodziny w świetle unormowań Konstytucji RP z dnia 2 kwietnia 1997 r.*, „Rejent" 1997, nr 5(73), s. 121; Warto jednocześnie zauważyć, że przywołany pogląd został sformułowany przed implementacją w Kodeksie rodzinnym i opiekuńczym rozwiązań normatywnych nawiązujących do konstrukcji charakterystycznych dla ochrony praw i wolności człowieka.

[23] Na jej podstawowe znaczenie dla interpretacji art. 48 Konstytucji RP zwraca uwagę P. Sarnecki, *op. cit.*, art. 48, pkt 5.

[24] W piśmiennictwie podkreśla się, że konstytucyjne pojęcie „komunikowania się" ma bardziej nowoczesny charakter niż tradycyjne określenie „korespondencja" i z pewnością odnosi się do komunikacji z wykorzystaniem narzędzi elektronicznych, w tym w Internecie, por. np. S. Jarosz-Żukowska, *Konstytucyjnoprawne aspekty ochrony tajemnicy komunikowania się w Internecie*, „Przegląd Prawa i Administracji" 2008, t. LXXVIII, s. 13; M. Rogalski, P. Szustakiewicz, *Pojęcie i zakres tajemnicy komunikacji elektronicznej*, „Ius Novum" 2022, nr 1, s. 60.

[25] Por. np. M. Wild, [w:] *Konstytucja RP. Tom I. Komentarz do art. 1–86*, red. M. Safjan, L. Bosek, Warszawa 2016, art. 49, Nb 7 i 14.

i może następować w sposób w niej określony[26]. Ustrojodawca wymaga zatem pewnego stopnia konkretyzacji odstępstw od ochrony omawianego prawa. W orzecznictwie Trybunału Konstytucyjnego podkreśla się, że „[u]stawodawca nie może poprzez niejasne formułowanie tekstu przepisów pozostawiać organom mającym je stosować nadmiernej swobody przy ustalaniu w praktyce zakresu podmiotowego i przedmiotowego ograniczeń konstytucyjnych wolności i praw jednostki."[27].

Przepisy prawa rodzinnego nie przewidują wprost uprawnienia rodziców do naruszania tajemnicy komunikowania się ich dziecka. Nie może jednak budzić wątpliwości, że ochrona praw i wolności dziecka nie może mieć charakteru absolutnego[28] i musi uwzględniać inne wartości chronione konstytucyjnie i na poziomie ustawowym. Wyrazem takiego podejścia może być deklaracja zgłoszona przez Polskę przy ratyfikacji Konwencji o prawach dziecka, o treści następującej: „wykonania przez dziecko jego praw określonych w konwencji, dokonuje się z poszanowaniem władzy rodzicielskiej, zgodnie z polskimi zwyczajami i tradycjami dotyczącymi miejsca dziecka w rodzinie i poza rodziną"[29]. Tak więc ochrona tajemnicy komunikowania się dziecka musi uwzględniać konstytucyjnie gwarantowane prawo rodziców do wychowania swojego dziecka oraz obowiązki wynikające z przysługującej im władzy rodzicielskiej, kształtowane przez prawo rodzinne. Autonomia dziecka w zakresie prawa do prywatności i ochrony tajemnicy komunikowania się jest limitowana w stosunkach z rodzicami przez ciążący na nich obowiązek zapewnienia dziecku bezpieczeństwa, będący składową obowiązku wychowywania dziecka. Należy przyjąć w związku z tym, że co do zasady rodzice mają obowiązek kontroli

[26] Ten wymóg podyktowany jest treścią art. 49 Konstytucji RP, jak również art. 31 ust. 3 Konstytucji RP.

[27] Por. wyrok TK z dnia 20 kwietnia 2004 r., K 45/02, OTK-A 2004, Nr 4, poz. 30.

[28] W odniesieniu do praw dziecka określonych w Konwencji o prawach dziecka z dnia 20 listopada 1989 r. stanowisko takie prezentuje P. Zamelski. Por. P. Zamelski, *Prawo do ochrony życia prywatnego*, [w:] *Konwencja o prawach dziecka. Wybór zagadnień* (*artykuły i komentarze*), red. S.L. Stadniczeńko, Warszawa 2015, s. 122.

[29] Konwencja o prawach dziecka z dnia 20 listopada 1989 r. (Dz.U. z 1991 Nr 120, poz. 526).

działań podejmowanych przez dziecko w ramach korzystania ze środków komunikacji elektronicznej.

W świetle obowiązujących unormowań prawnych nie sposób też określić granicy wiekowej, która przed osiągnięciem przez dziecko pełnoletności różnicowałaby poziom ochrony jego autonomii w zakresie tajemnicy korespondencji w stosunkach z rodzicami. Należy w związku z tym przyjąć, że omawiany obowiązek rodziców ciąży na nich przez cały czas wykonywania przez nich władzy rodzicielskiej, a więc do osiągnięcia przez dziecko pełnoletności. Nadużycie tego prawa może spotkać się z ingerencją sądu opiekuńczego jedynie w wyjątkowych przypadkach, w których postępowanie rodziców staje się sprzeczne z dobrem dziecka.

3. Korzystanie przez dziecko z przedmiotów komunikacji elektronicznej – perspektywa cywilistyczna

3.1. Uwagi ogólne

Powyżej zarysowana została ocena prawna korzystania przez dziecko z narzędzi komunikacji elektronicznej z perspektywy rodzinnoprawnej – obowiązków i praw rodziców w zakresie pieczy nad osobą dziecka, jego wychowania (art. 95 § 1 k.r.o.) oraz obowiązku troski o fizyczny i duchowy rozwój dziecka (art. 96 § 1 k.r.o.). Dopełnieniem tych rozważań musi być analiza dokonana z perspektywy cywilnoprawnej. Należy odpowiedzieć na pytanie, czy rodzic ma odpowiednie instrumenty prawne dla działań ingerujących w możliwość korzystania z takich przedmiotów przez dziecko oraz czy regulacje cywilnoprawne są właściwie zharmonizowane z rozwiązaniami prawa rodzinnego. Już wstępnie można stwierdzić, że problem własności urządzeń służących do komunikacji elektronicznej, sprawowania zarządu nad tymi przedmiotami, charakteru uprawnień dziecka czy charakteru faktycznego władztwa nad tymi urządzeniami może mieć niezwykle istotne znaczenie z perspektywy zakresu autonomii dziecka w używaniu tych urządzeń, jak również możliwości ingerencji rodziców w tę autonomię. Zagadnienie sytuacji prawnej dziecka pozostającego pod władzą rodzicielską i korzystającego z przedmiotów umożliwiających

komunikację elektroniczną musi być poddane analizie wariantowo. Pierwszy przypadek zakłada, że dziecko nie jest właścicielem tych urządzeń, ale rodzic.

3.2. Sytuacja prawna dziecka niebędącego właścicielem przedmiotów

Nie budzi wątpliwości, że rodzice mogą a nawet muszą z uwagi na obowiązek pieczy nad osobą dziecka, udostępnić czy przekazać dziecku pewne przedmioty do użytku[30]. Odnosząc się już ściśle do urządzeń umożliwiających komunikację elektroniczną (komputer, smartfon, tablet itp.), nie należy uznać za kwestyjne stwierdzenia, że rodzic jako właściciel może po pierwsze, przykładowo instalować oprogramowanie ograniczające sposób i czas jego używania. Po drugie, rodzic oddając dziecku urządzenie do używania, może określić zakres, czas i sposób tego używania.

Możliwość używania przez dziecko pozostające pod władzą rodzicielską analizowanych urządzeń, których właścicielem pozostaje rodzic, stawia pytanie o charakter prawny tego władztwa i ewentualnie jego podstawę. Zagadnienie nie było przedmiotem rozważań w doktrynie prawa rodzinnego, a kwestia ma istotne znaczenie przykładowo z perspektywy ochrony władztwa faktycznego dziecka nad wskazanymi przedmiotami majątkowymi czy też np. jego dziedziczności.

Wstępnie, co oczywiste, należy stwierdzić, że w analizowanej konfiguracji tzn., gdy właścicielem środków komunikacji elektronicznej pozostaje rodzic, dziecko używające tych przedmiotów nie jest ich posiadaczem samoistnym. Zdecydowanie bardziej problematyczna jest kwalifikacja analizowanego władztwa z perspektywy definiowania posiadania zależnego. Zgodnie z art. 336 k.c., posiadaczem jest również ten (poza posiadaczem samoistnym), kto rzeczą faktycznie włada jak użytkownik, zastawnik, najemca, dzierżawca lub mający inne prawo, z którym łączy się określone władztwo nad cudzą rzeczą.

[30] Zob. T. Sokołowski, *Władza rodzicielska nad dorastającym dzieckiem*, Poznań 1987, s. 116 i n.; *idem*, [w:] *Kodeks cywilny. Komentarz. Tom I. Część ogólna*, red. A. Kidyba, LEX 2012, art. 2, Nb 5.

Fundamentalne pytanie dotyczy kwestii czy istnieje (może istnieć) prawo dziecka do używania rzeczy oddanej mu przez rodzica, z którym wiąże się określone władztwo nad tą rzeczą. Już na wstępie należy zaznaczyć, że konstruowanie takiego prawa jest wątpliwe. Najistotniejszym argumentem na rzecz takiej tezy jest stwierdzenie, że w sytuacji, w której rodzic oddaje dziecku do używania np. smartfon czy tablet jego intencją nie jest wykreowanie żadnego nowego, niezależnego od władzy rodzicielskiej stosunku prawnego. Nieporozumieniem byłaby przykładowo próba konstruowania stosunku prawnego użyczenia czy też podobnego. Nie następuje określenie żadnych elementów treści umowy, a oddanie rzeczy ma charakter czysto faktyczny. Konstruowanie stosunku prawnego, którego źródłem musiałaby być umowa, stawiałoby kwestię zidentyfikowania osób składających oświadczenia woli. W przypadku dziecka, które nie ukończyło lat 13 i nie ma zdolności do czynności prawnych, należałoby rozważyć możliwość dokonania czynności przez rodzica – przedstawiciela ustawowego z samym sobą. Prowadząc analizę *ad absurdum*, należałoby rozważyć czy w każdym przypadku rodzic może być przedstawicielem ustawowym dziecka. Co prawda zgodnie z art. 98 § 1 pkt 2 k.r.o. wyłączenie reprezentacji nie dotyczy czynności polegających na bezpłatnym przysporzeniu na rzecz dziecka jednak można zadać pytanie co w sytuacji, gdy rodzic „złożył ofertę", zgodnie z którą dziecko otrzyma komputer do użytku na określony czas, jeżeli w zamian posprząta swój pokój i czy takie zastrzeżenie należałoby uznać za zobowiązanie, a więc również przysporzenie oraz rozważyć ustanowienie kuratora, który mógłby w imieniu dziecka czynności takiej dokonać. Wątpliwości budziłaby również możliwość zakończenia takiego stosunku prawnego, wszak przykładowo art. 715 i 716 k.c. przewidują szczegółowe regulacje dotyczące zakończenia użyczenia. Podawałoby to w wątpliwość możliwość jednostronnego i natychmiastowego zakończenia stosunku prawnego przez rodzica.

Oddanie przedmiotów do używania dziecku następuje w wykonywaniu władzy rodzicielskiej, ale ma charakter czysto faktyczny. Ponadto taki sam charakter ma ta czynność w przypadku dziecka niemającego zdolności do czynności prawych, jak również nastolatka, który ma ograniczoną zdolność do czynności prawnych. Konstatacja powyższa nie oznacza, że nie jest możliwe skonstruowanie stosunku prawnego i prawa dającego dziecku uprawnienie

do władania rzeczą oddaną przez rodzica. Możliwe byłoby zarówno wykreowanie takiego prawa o charakterze względnym (np. użyczenia), jak również rzeczowym (np. użytkowania). Sytuacje takie należy uznać jednak za nietypowe i wywołanie wskazanych skutków musi wynikać z treści składanych oświadczeń.

Zasadnicze odrzucenie tworzenia prawa, „z którym łączy się określone władztwo nad cudzą rzeczą", stawia pytanie, czy mimo to dziecko można uznać za posiadacza zależnego. W doktrynie prawa cywilnego nie budzi wątpliwości, że posiadaczowi nie musi przysługiwać prawo, w zakresie którego włada rzeczą[31]. Problematyczne jest jednak to czy można uznać za posiadanie zależne władanie rzeczą w sytuacji, gdy konstrukcyjnie w ogóle brak jest prawa, któremu odpowiadać miałoby takie władztwo nad rzeczą. Kwestię należy uznać za wysoce kontrowersyjną i dotykającą fundamentów systemu prawa cywilnego: charakteru posiadania[32]. W pewnym zakresie zagadnienie dotyczy problemu, na ile polski system prawny został oparty na romańskiej koncepcji posiadania wyróżniającej elementy *corpus* i *animus* czy też konstrukcję posiadania praw, a na ile na koncepcji germańskiej opartej na elemencie faktycznym *corpus* oraz odrzucającej posiadanie praw[33]. Ujęcie nawiązujące do koncepcji romańskiej, upatrujące podstaw rozróżnienia rodzajów posiadania w elemencie *animus* zdaje się ściślej wiązać koncepcję tego władztwa z prawem podmiotowym, którego posiadanie ma być cieniem[34] czy też

[31] Zamiast wielu: J. Gołaczyński, [w:] *System Prawa Prywatnego. Tom 4. Prawo rzeczowe*, red. E. Gniewek, Warszawa 2021, s. 626 i n.

[32] Jak podkreślił A. Stelmachowski, na wstępie swojej fundamentalnej monografii: „[p]osiadanie należy od dawna do tych instytucji prawa cywilnego, które zawsze budziły zainteresowanie prawników, i jest przy tym rzeczą znamienną, że jakkolwiek napisano na jej temat już wiele tomów oraz stworzono wiele teorii, to jednak w rzeczywistości wyjaśniono niewiele, a w związku z tym pozostało nadal wiele punktów spornych oraz zagadnień do dnia dzisiejszego właściwie nie rozwiązanych" (A. Stelmachowski, *Istota i funkcje posiadania*, Warszawa 1953, s. 3). Należy zauważyć, że nadal kwestie konstrukcyjne posiadania budzą wątpliwości i spory dotyczące zagadnień podstawowych.

[33] Zob. A. Kunicki, *Elementy romańskie i germańskie w konstrukcji posiadania według kodeksu cywilnego*, „Studia Prawnicze" 1970, z. 26–27, s. 70 i n.; K. Zaradkiewicz, *Romańska teoria posiadania a kodeks cywilny*, „Studia Iurudica", t. LXIV, s. 104 i n.

[34] J. Carbonnier, za: A. Kunicki, *op. cit.*, s. 86.

sobowtórem[35]. Jak zaznaczał jeszcze w czasie obowiązywania dekretu prawo rzeczowe[36] W. Czachórski:

> [w]ładztwo posiadacza powinno zawsze co do swego zakresu odpowiadać treści pewnego prawa podmiotowego […] przez co rozumiemy, że prawo takie (gdyby istniało) w razie jego wykonywania przejawiało by się tak właśnie jak władztwo faktyczne posiadacza[37].

Ścisłe powiązanie posiadania z prawem podmiotowym wynika również z koncepcji „posiadania praw". Fryderyk Zoll przyjmował, że:

> [p]osiadanie jest mocą faktyczną wykonywania pewnego prawa podmiotowego, majątkowego, jako to własności, służebności, prawa zabudowy, najmu, dzierżawy itd. „Tzw. posiadanie rzeczy" nie jest posiadaniem rzeczy, ale także posiadaniem prawa, mianowicie prawa własności. Posiadanie oznacza bowiem zawsze faktyczną moc wykonywania prawa […][38].

Pomimo zgłaszanych wątpliwości co do aktualności pewnych elementów teorii romańskiej na gruncie Kodeksu cywilnego, w szczególności w zakresie koncepcji posiadania praw[39], nie można, jak się wydaje, na gruncie obowiązującego art. 336 k.c. zakwestionować wymagania istnienia elementu *animus* i postrzegać posiadanie jako „czysty" stan faktyczny – fizyczne władztwo nad rzeczą[40]. Skłania to do uznania, że posiadanie nie jest „przedprawnym" stanem

---

35 S. Kołodziejski, *Istota, treść i rodzaje posiadania*, „Palestra" 1966, nr 6, s. 18.

36 Dekret z dnia 11 października 1946 r. prawo rzeczowe, Dz.U. z 1946 r., Nr 57, poz. 319. Jak podkreślano w doktrynie, dekret został jednoznacznie oparty na tradycyjnej romańskiej teorii posiadania. E. Skowrońska-Bocian, M. Warciński, [w:] *Kodeks cywilny. Tom I. Komentarz. Art. 1–449*[*10*], red. K. Pietrzykowski, Legalis 2020, art. 336, Nb 1.

37 W. Czachórski, *Pojęcie i treść posiadania według obowiązującego prawa rzeczowego,* „Nowe Prawo" 1957, nr 5, *passim*.

38 F. Zoll, *Posiadanie w przyszłym kodeksie cywilnym polskim,* RPEiS 1930, z. 1, s. 173.

39 A. Kunicki, *op. cit.,* s. 91 i n.

40 Zob. K. Zaradkiewicz, *op. cit.,* s. 107; E. Skowrońska-Bocian, M. Warciński, *op. cit.*, *passim*.

faktycznym niezależnym od regulacji normatywnej[41]. Stanowisko takie uniemożliwia przyjęcie, że dziecko władające przedmiotem oddanym mu przez rodzica, nie wykonując własnego prawa, z którym łączy się władztwo nad rzeczą, jest posiadaczem zależnym.

Za takim stanowiskiem przemawiają również argumenty systemowe. Uznanie dziecka za posiadacza otwierałoby problem podstawy pozbawienia go tego statusu przez rodzica. Posiadanie jest stanem (faktycznym[42] czy prawnym[43]) chronionym przez normy prawne. Zgodnie art. 342 k.c., nie wolno naruszać samowolnie posiadania. Choć w dalszej części opracowania zaprezentowana zostanie interpretacja, zgodnie z którą naruszenie władztwa dziecka przez rodzica wykonującego władzę rodzicielską nie można uznać za samowolne naruszenie posiadania, jednak przyjęcie w analizowanej sytuacji, że dziecko jest posiadaczem komplikuje zagadnienie wcześniejszego odebrania przedmiotu oddanego do używania. Trudno również, choć problem jest głównie teoretyczny, nawet rozważać dziedziczenie takiego stanu przez spadkobierców dziecka.

Kolejnym zagadnieniem wymagającym rozważenia jest pytanie, czy władztwo faktyczne dziecka możne w opisanych okolicznościach zostać uznane za dzierżenie. Zgodnie z art. 338 k.c., kto rzeczą faktycznie włada za kogo innego, jest dzierżycielem. Konstrukcyjnym elementem dzierżenia jest wola sprawowania faktycznego władztwa za kogo innego (*animus possidendi pro alieno*)[44]. *Prima facie* można by uznać dziecko za dzierżyciela władającego rzeczą za rodzica – właściciela i posiadacza samoistnego. Problematyczne jest jednak to, że dziecko władając pewnym przedmiotem (np. używając telefonu czy tabletu) nie włada tym przedmiotem za rodzica[45], ale działa we własnym interesie. Konstatacja taka przemawia przeciwko uznaniu dziecka w opisanych okolicznościach za dzierżyciela.

---

[41] J. Ignatowicz, *Ochrona posiadania*, Warszawa 1963, s. 91 i n. Odmienne stanowisko zajmuje: B. Lackoroński, [w:] *Kodeks cywilny. Komentarz*, red. K. Osajda, Legalis 2021, art. 336, Nb 16.

[42] Zob. M. Gocłowski, *Posiadanie w ujęciu kodeksu cywilnego* (*Prawo podmiotowe czy stan faktyczny?*), „Państwo i Prawo" 2001, nr 2, s. 44 i n. oraz cytowaną tam literaturę.

[43] K. Zaradkiewicz, *op. cit.*, s. 112.

[44] J. Gołaczyński, *op. cit.*, s. 633; B. Lackoroński, [w:] *Kodeks…*, art. 338, Nb 1.

[45] Oczywiście można wyobrazić sobie taką sytuację, gdy rodzic oddaje dziecku swój telefon z poleceniem wysłania wiadomości o określonej treści np. do kogoś z rodziny.

Pomimo braku regulacji ustawowej, zarówno w literaturze[46], jak i orzecznictwie Sądu Najwyższego[47] przyjmuje się, że posiadanie i dzierżenie nie są jedynymi formami faktycznego władztwa nad rzeczą. Wyróżnia się również władztwo prekaryjne, a czasem nawet dalsze rodzaje władztwa takie jak *quasi*-prekarium[48]. Istotą prekarium jest brak stosunku prawnego pomiędzy podmiotem mającym tytuł prawny do rzeczy oraz sprawującym faktyczne władztwo nad rzeczą[49]. Oparte jest ono na zaufaniu lub grzeczności posiadacza[50]. Prekarium jest stosunkiem społecznym niemającym charakteru prawnego[51]. Podkreśla się również każdoczesną jego odwołalność oraz brak ochrony posesoryjnej[52]. Stanowisko o braku ochrony posesoryjnej nie jest jednak powszechnie przyjęte. Zaprezentowany został pogląd, zgodnie z którym prekarzysta jest dzierżycielem[53]. Umożliwiałoby to odpowiednie stosowanie przepisów o obronie koniecznej i dozwolonej samopomocy do prekarzysty na mocy odesłania z art. 343 § 3 k.c. Pogląd ten został jednak odrzucony przez większość przedstawicieli doktryny[54]. Należy także zauważyć, że – jak zdaje się wynikać z kontekstu rozważań autora koncepcji – ochrona własna posiadacza miałaby raczej dotyczyć osób trzecich, a ponadto wyróżniał on również władztwo *quasi*-prekaryjne[55] (które przez innych autorów jest kwalifikowane po prostu jako prekarium[56]).

---

[46] J. Ignatowicz, *Ochrona…*, s. 91 i n.; P. Księżak, *Precarium w prawie polskim*, „Rejent" 2007, nr 2, s. 58; E. Skowrońska-Bocian, M. Warciński, *op. cit.*, art. 338, Nb 3; J. Gołaczyński, *op. cit.*, s. 634; B. Lackoroński, [w:] *Kodeks…*, art. 338, Nb 6 i n.

[47] Przykładowo w orzeczeniach z dnia: 1 września 1958, 1 CR 745/58; 24 listopada 1976 r., IV CR 70/76; 10 marca 1977 r., IV CR 52/77; 13 września 2001 r., IV CKN 425/00; 15 stycznia 2010 r., I CSK 355/09.

[48] J. Ignatowicz, *Ochrona…*, s. 94 i n.

[49] B. Lackoroński, [w:] *Kodeks…*, art. 338, Nb 7.

[50] E. Skowrońska-Bocian, M. Warciński, *op. cit.*, art. 338, Nb 3.

[51] P. Księżak, *Precarium…*, s. 66 i n.

[52] *Ibidem*, s. 70; B. Lackoroński, [w:] *Kodeks…*, art. 338, Nb 8, 11; J. Gołaczyński, *op. cit.*, s. 634.

[53] J. Ignatowicz, *Ochrona…*, s. 94; I. Kunicki, [w:] *System prawa cywilnego. Tom 2. Prawo własności i inne prawa rzeczowe*, red. J. Ignatowicz, Wrocław 1977, s. 838; tak również SN w postanowieniu z dnia 15 stycznia 2010 r., I CSK 355/09, OSNC 2010, nr 10, poz. 139.

[54] P. Księżak, *Precarium…*, s. 62; S. Rudnicki, [w:] *Komentarz do kodeksu cywilnego. Księga druga. Własność i inne prawa rzeczowe*, G. Rudnicki, S. Rudnicki, LEX 2011, art. 338, Nb 2; E. Skowrońska-Bocian, M. Warciński, *op. cit.*, art. 338, Nb 3; J. Gołaczyński, *op. cit.*, s. 634; B. Lackoroński, [w:] *Kodeks…*, art. 338, Nb 11.

[55] J. Ignatowicz, *Ochrona…*, s. 95.

[56] P. Księżak, *Precarium…*, s. 71.

W takim przypadku władztwo nie podlegałoby kwalifikacji jako dzierżenie[57] i nie byłoby chronione.

Uznanie władztwa faktycznego dziecka nad przedmiotami oddanymi do używania przez rodzica będącego właścicielem *stricte* za prekarium może budzić pewne wątpliwości chociażby z perspektywy „nozologicznej", biorąc pod uwagę jego genezę[58]. Pomiędzy opisywaną sytuacją a prekarium występuje jedna niezwykle doniosła zbieżność: brak stosunku prawnego oraz wykreowania jakiegokolwiek prawa do władania rzeczą przez dziecko. Opisywana relacja ma charakter pozaprawny – czysto faktyczny. Jak podkreślił P. Księżak, „[p]rekarium […] nie jest relacją prawną, lecz opartą na przyjaźni lub więzach rodzinnych [podkr. – M.D.]"[59]. Na tej właśnie płaszczyźnie – czysto faktycznej – należy kwalifikować władztwo dziecka w przypadku braku skonstruowania stosunku prawnego np. umowy darowizny. Nie ma również znaczenia czy dziecko ma ograniczoną zdolność do czynności prawnych czy też zdolności tej nie ma. Konsekwencją powyższej kwalifikacji jest przyjęcie każdoczesnej odwołalności oddania dziecku rzeczy, jak również nieprzysługiwanie dziecku ochrony posesoryjnej. W każdym więc momencie rodzic może ograniczyć czy zakończyć korzystanie przez dziecko ze środków komunikacji elektronicznej. W przypadku, gdyby korzystanie to było sprzeczne z dobrem dziecka, miałby nawet taki obowiązek wynikający z władzy rodzicielskiej.

3.3. Sytuacja prawna dziecka będącego właścicielem przedmiotów

Drugim wariantem wymagającym rozważenia jest sytuacja, gdy właścicielem przedmiotów komunikacji elektronicznej jest samo dziecko. Może ono nabyć własność tych przedmiotów na podstawie różnych zdarzeń prawnych: umów – w szczególności darowizny (darczyńcą może być również rodzic wykonujący

[57] J. Ignatowicz, *Ochrona*…, s. 95.

[58] *Ibidem*, s. 90.

[59] P. Księżak, *Glosa do postanowienia Sądu Najwyższego z dnia 15 stycznia 2010 r., I CSK 355/09*, „Rejent" 2010, nr 12, s. 82.

władzę rodzicielską), sprzedaży itd., jak również dziedziczenia. Z perspektywy cywilnoprawnej – w szczególności sposobów nabycia przedmiotów do majątku dziecka istotne jest to, czy dziecko ma ograniczoną zdolność do czynności prawnych (jest niepełnoletnie, ale ukończyło lat trzynaście – art. 15 k.c.) czy też w ogóle nie ma zdolności do czynności prawnych (nie ukończyło lat trzynastu albo zostało całkowicie ubezwłasnowolnione – art. 12 k.c.).

W przypadku dzieci niemających zdolności do czynności prawnych rodzic ma duży zakres prawnej kontroli co do przedmiotów majątkowych nabywanych przez dziecko. W przypadku czynności prawnych możliwość ich dokonywania ma rodzic, działając jako przedstawiciel ustawowy dziecka (art. 98 § 1 k.r.o.), a wyjątkowo kurator (art. 99 k.r.o.). W przypadku dziedziczenia również to rodzic jako przedstawiciel ustawowy składa w imieniu dziecka oświadczenie o przyjęciu spadku (art. 1012 i n. k.c.) czy też zapisu windykacyjnego (art. 1012 i n. k.c. stosowane odpowiednio w drodze odesłania z art. 981^5 k.c.). Dziecko samodzielnie ma możliwość wyłącznie zawierania umów w drobnych bieżących sprawach życia codziennego a umowy takie stają się ważne dopiero z chwilą ich wykonania (art. 14 § 2 k.c.)[60]. Umowy, na podstawie których następuje nabycie przedmiotów służących do komunikacji elektronicznej, nie mogą być uznane, przynajmniej obecnie, za drobne bieżące sprawy życia codziennego.

Zakres kontroli rodziców jest bardziej ograniczony w przypadku dzieci, które mają ograniczoną zdolność do czynności prawnych. O ile w przypadku czynności prawnych, przez które osoba taka zaciąga zobowiązanie np. umowy sprzedaży telefonu czy komputera, potrzebna jest zgoda przedstawiciela ustawowego, o tyle w przypadku czynności, które nie stanowią zobowiązania ani

[60] W różny sposób określa się mechanizm ważności umów zawieranych zgodnie z art. 14 § 2 k.c. Tradycyjnie cywilistyka upatruje we wskazanym przepisie mechanizm ustawowej konwalidacji nieważnej umowy (zamiast wielu zob. A. Wolter, J. Ignatowicz, K. Stefaniuk, *Prawo cywilne. Zarys części ogólnej*, Warszawa 2020, s. 425). Autorzy ujmujący czynność prawną jako czynność konwencjonalną upatrują we wskazanym przepisie wyjątku od braku zdolności do czynności prawnych osób, które nie ukończyły lat trzynastu bądź zostały całkowicie ubezwłasnowolnione i przyznania im w zakresie przedmiotowych czynności takiej zdolności (tak w szczególności Z. Radwański, A. Olejniczak, *Prawo cywilne – część ogólna*, Warszawa 2015, s. 352).

rozporządzenia, zgoda taka nie jest wymagana[61]. Przykładowo dziecko może samodzielnie zawrzeć jako obdarowany umowę darowizny nieobciążoną poleceniem[62]. Ponadto zgodnie z art. 21 k.c., dziecko mające ograniczoną zdolność do czynności prawnych może bez zgody przedstawiciela ustawowego rozporządzać swoim zarobkiem (chyba że sąd opiekuńczy postanowił inaczej).

Obowiązujące w prawie cywilnym rozwiązania, przyznając starszemu małoletniemu dziecku ograniczoną zdolność do czynności prawnych, powodują, że kontrola rodziców w zakresie nabywania przedmiotów majątkowych zostaje w pewnym zakresie ograniczona.

Zagadnienie nabywania przedmiotów takich jak środki komunikacji elektronicznej do majątku dziecka należy zdecydowanie odróżnić od kwestii sprawowania zarządu tymi przedmiotami. Zasadniczo rodzice, którym przysługuje władza rodzicielska, są obowiązani sprawować zarząd majątkiem dziecka (art. 101 § 1 k.r.o.). Typową sytuacją jest więc sprawowanie zarządu również przedmiotami majątkowymi istotnymi z perspektywy niniejszego opracowania. Od zasady sprawowania zarządu majątkiem dziecka przez rodziców przewidziano kilka wyjątków. Zgodnie z art. 102 k.r.o., w umowie darowizny albo w testamencie można zastrzec, że przedmioty przypadające dziecku z tytułu darowizny lub testamentu nie będą objęte zarządem sprawowanym przez rodziców. Jeżeli darczyńca lub spadkodawca nie wyznaczył zarządcy, zarząd sprawuje kurator ustanowiony przez sąd opiekuńczy. Należy przyłączyć się do poglądu, zgodnie z którym w sytuacji opisanej w art. 102 k.r.o., należy stosować zasadę surogacji w stosunku do przedmiotów nabytych przez dziecko tytułem darowizny lub w następstwie otwarcia spadku[63]. Wniosek taki wywodzi się z zasady, zgodnie z którą przy braku wskazań ustawowych należy przyjąć surogację

[61] Zamiast wielu S. Grzybowski, [w:] *System prawa cywilnego, t. I, Część ogólna*, red. S. Grzybowski, Wrocław 1985, s. 345.

[62] Zob. uchwałę SN z dnia 30 kwietnia 1977 r., III CZP 73/76, OSNC 1978, nr 2, poz. 19.

[63] B. Lackoroński, *Wyłączenie zarządu rodziców przedmiotami przypadającymi dziecku z tytułu darowizny lub testamentu*, [w:] *Ius et Ratio. Księga Jubileuszowa Profesor Elżbiety Skowrońskiej-Bocian,* red. J. Wierciński, A. Gołaszewska, M. Olechowski, W. Borysiak, Warszawa 2022, s. 518.

rzeczową jako jedyny sposób ochrony majątku odrębnego[64]. Pogląd prowadzi do przyjęcia, że z zarządu rodziców wyłączone są nie tylko przedmioty stanowiące przedmiot darowizny bądź przypadające dziecku w wyniku otwarcia spadku, ale również to, co jest nabywane ze środków pochodzących z tego majątku (pożytki i surogaty)[65]. Odnosząc taki wniosek do przedmiotowych rozważań, należy uznać, że przykładowo, jeżeli przedmiotem darowizny, do której odnosi się art. 102 k.r.o., była kwota pieniężna i w zamian za te pieniądze nabyte zostaną przedmioty służące do komunikacji elektronicznej (komputer, telefon itp.), to przedmioty te również będą wyłączone z zarządu rodziców. W tych przypadkach zarząd będzie sprawował zarządca wyznaczony przez darczyńcę albo spadkodawcę bądź kurator ustanowiony przez sąd.

Opisana sytuacja nie jest jedyną, gdy pewne elementy majątku dziecka w tym przedmioty służące komunikacji elektronicznej są wyłączone spod zarządu rodziców. Zgodnie z art. 101 § 2 k.r.o., zarząd rodziców nie obejmuje zarobku dziecka ani przedmiotów oddanych mu do swobodnego użytku. Związane jest to z regulacją art. 21 i 22 k.c.[66] i dotyczy wyłącznie dzieci mających ograniczoną zdolność do czynności prawnych[67]. Osoby takie mogą bez zgody przedstawiciela ustawowego rozporządzać swoim zarobkiem[68] (art. 21 k.c.), jak również uzyskują pełną zdolność do czynności prawnych w zakresie czynności dotyczących przedmiotów oddanych do swobodnego użytku przez przedstawiciela ustawowego (art. 22 k.c.). Wskazanymi przedmiotami zarządza więc samodzielnie dziecko mające ograniczoną zdolność do czynności prawnych. Kwestyjnym zagadnieniem jest to, czy wyłączenie zarządu rodziców dotyczy również surogatów zarobku oraz przedmiotów oddanych do swobodnego

[64] Zob. A. Ohanowicz, *Glosa do orzeczenia SN z dnia 18.X.1961 r., 4 Cr57/60*, „Państwo i Prawo" 1962, nr 8–9, s. 465; E. Kitłowski, *Surogacja rzeczowa w prawie cywilnym,* Warszawa 1969, s. 125 i n.; B. Lackoroński, *Wyłączenie…*, s. 518.

[65] B. Lackoroński, *Wyłączenie…*, s. 518.

[66] J. Słyk, *op. cit.*, art. 101, Nb 12.

[67] J. Ignatowicz, [w:] *System…*, s. 831.

[68] Chyba że sąd opiekuńczy z ważnych powodów postanowi inaczej.

użytku. W doktrynie wyrażono stanowisko twierdzące[69], jak i kontestujące zastosowanie w tym przypadku zasady surogacji rzeczowej[70].

We wszystkich przypadkach, gdy dziecko jest właścicielem rzeczy w tym oczywiście środków komunikacji elektronicznej, należy uznać, że jest ono posiadaczem samoistnym. Pozostawiając na boku szczegółowe rozważania, należy tylko zasygnalizować, że w doktrynie[71] i orzecznictwie SN[72] dominuje ujęcie zakładające dziedziczność posiadania. Ponadto należy przyjąć możliwość nabycia posiadania przez przedstawiciela ustawowego[73]. W przypadku dzieci starszych, które mogą działać z dostatecznym rozeznaniem, możliwe jest samodzielne nabycie posiadania[74]. Przedstawiciela ustawowego dziecka dokonującego czynności zarządu jego majątkiem należy natomiast uznać za dzierżyciela[75].

Z perspektywy niniejszych rozważań przynajmniej *prima facie* istotne znaczenie ma wyróżnienie dwóch sytuacji: gdy to rodzice są obowiązani i uprawnieni do zarządu przedmiotami majątkowymi służącymi do komunikacji elektronicznej oraz gdy zarząd sprawuje inna osoba: samo dziecko ewentualnie zarządca albo kurator. Powstaje pytanie, czy sytuacja taka ma wpływ na dopuszczalność kontroli zachowań dziecka przykładowo przez instalowanie oprogramowania ochrony rodzicielskiej czy też bezpośrednie ograniczanie sposobu i czasu używania takich urządzeń.

Wypowiedzi doktryny we wskazanym zakresie są niezwykle skromne. Stanowisko o braku bezpośredniej kompetencji rodziców w tym zakresie zajął J. Strzebińczyk, stwierdzając, że:

---

[69] J. Ignatowicz, [w:] *System…*, s. 831; J. Słyk, *op. cit.*, Nb 15; J. Gajda, [w:] *Kodeks rodzinny i opiekuńczy. Komentarz*, red. K. Pietrzykowski, art. 101, Nb 19; T. Sokołowski, [w:] *Kodeks rodzinny i opiekuńczy. Komentarz*, red. H. Dolecki, T. Sokołowski, Warszawa 2013, s. 697.

[70] A. Wolter, *Prawo cywilne. Zarys części ogólnej,* Warszawa 1967, s. 148; R. Strugała, [w:] *Kodeks cywilny. Komentarz*, red. E. Gniewek, P. Machnikowski, Legalis 2021, art. 22, Nb 3; P. Księżak, [w:] *Kodeks cywilny. Komentarz*, red. K. Osajda, Legalis 2021, art. 21, Nb 4.

[71] W. Borysiak, [w:] *Kodeks cywilny. Komentarz,* red. K. Osajda, Legalis 2021, art. 922, Nb 331 i n.

[72] Zob. w szczególności postanowienia SN z dnia: 4 października 2002 r., III CKN 521/01; 2 lutego 2017 r., I CSK 260/16; 16 listopada 2017 r., V CSK 15/17.

[73] Zob. J. Ignatowicz, *Ochrona…*, s. 56; M. Krajewski, *Charakter prawny przeniesienia posiadania*, SPP 2013, nr 3, s. 101.

[74] J. Ignatowicz, [w:] *Kodeks cywilny. Komentarz. Tom 1*, red. Z. Resich, s. 811; M. Krajewski, *op. cit.*, s. 97.

[75] B. Lackoroński, [w:] *Kodeks…*, art. 338, Nb 5; J. Ignatowicz, [w:] *Kodeks…*, s. 776.

> względem zarobków podopiecznego oraz przedmiotów oddanych mu do swobodnej dyspozycji piecza opiekuna[76] ogranicza się w zasadzie do kontrolowania sposobu ich wykorzystania i do ewentualnego zawiadamiania sądu opiekuńczego o konieczności podjęcia stosownej interwencji, w wypadku zauważonych w tym zakresie nieprawidłowości[77].

Częściowo odmienne stanowisko zajął na gruncie opieki nad małoletnim L. Kociucki, który poza obowiązkiem poinformowania sądu o potrzebie ograniczenia możliwości rozporządzania przez małoletniego jego zarobkiem, stwierdził, że „może on odebrać małoletniemu przedmiot oddany mu do swobodnego użytku lub wyznaczyć określony sposób jego użytkowania"[78]. Możliwość odebrania przedmiotów oddanych dziecku do swobodnego użytku dopuścił również T. Sokołowski, stwierdzając, że postępowanie dziecka podlega nadal nadzorowi rodziców. O ile przedstawiciel nie może

> pozbawić go uzyskanych „definitywnie" uprawnień i kompetencji z art. 22 k.c., czyli prawa własności oraz możności rozporządzania tym przedmiotem, ale może i powinien odebrać dziecku posiadanie tego przedmiotu. Oddanie takich przedmiotów nie jest zatem „nieodwracalne", ale tylko w sensie posesoryjnym a nie petytoryjnym[79].

Jeszcze dalej idący pogląd zaprezentował J. Słyk, który – odwołując się do analogicznego stosowania art. 101 k.c. regulującego odwołanie pełnomocnictwa – przyjął dopuszczalność odebrania dziecku swobodnego użytku przedmiotów[80].

Podstawowe znaczenie dla rozwiązania wskazanego problemu ma zwrócenie uwagi na pojęcie „zarządu majątkiem dziecka". Szczegółowe rozważania dotyczące jego definiowania wykraczają poza zakres niniejszego opracowania,

---

[76] Jak się wydaje Autor odnosił się do władzy rodzicielskiej. Cytowany fragment został zamieszczony w rozdziale dotyczącym właśnie władzy rodzicielskiej.

[77] J. Strzebińczyk, *op. cit.*, s. 285.

[78] L. Kociucki, *Opieka nad małoletnim*, Warszawa 1993, s. 163.

[79] T. Sokołowski, [w:] *Kodeks…*, red. A. Kidyba, art. 22, Nb 15.

[80] J. Słyk, *op. cit.*, art. 101, Nb 19.

jak również nie są konieczne dla toku rozważań. Zarząd majątkiem dziecka jako pojęcie niezdefiniowane w ustawie stało się przedmiotem rozbieżnych interpretacji[81]. Nie podlega jednak kwestii, że w przypadku zarządu chodzi o sferę prawną dziecka dotyczącą jego interesów ekonomicznych[82]. Analiza czynności rodziców polegających na odebraniu przedmiotu służącego do komunikacji elektronicznej z uwagi na jego wykorzystywanie sprzeczne z dobrem dziecka czy też ograniczające możliwość korzystania z takich przedmiotów dotyczy interesów ekonomicznych dziecka jedynie pośrednio – „refleksowo". Bezpośrednio czynności te dotyczą pieczy nad osobą dziecka, a nie zarządu jego majątkiem[83]. Jak już wcześniej wskazano, rodzice wychowują dziecko pozostające pod władzą rodzicielską i kierują nim, a ponadto obowiązani są troszczyć się o jego fizyczny i duchowy rozwój (art. 96 k.r.o.). Ograniczenie sprawowania zarządu przez rodziców dotyczące pewnych przedmiotów nie ma wpływu na ten obowiązek. Oddziaływanie na dziecko mające zapobiegać uszczerbkom fizycznym czy psychicznym dotyczy innej płaszczyzny niż zarząd majątkiem. Należy uznać, że rodzice mają obowiązek i uprawnienie ingerencji w korzystanie przez dziecko z przedmiotów, którymi zarządza ono samo, kurator czy też zarządca, jeżeli jest to uzasadnione jego dobrem i stanowi wykonywanie pieczy nad osobą dziecka. Takie zachowanie nie stanowi ingerencji w sferę zarządu. Przykładowo w odniesieniu do przedmiotów oddanych dziecku do swobodnego użytku – dziecko ma nadal pełną zdolność do czynności prawnych dotyczącą tych przedmiotów. Jeżeli przedmiotem tym jest komputer, tablet czy telefon – dziecko nadal może je zbyć czy obciążyć[84].

W skrajnych przypadkach, gdy zastosowanie innych środków wychowawczych (np. perswazji) nie dało efektów, ograniczenie możliwości korzystania

---

[81] Zob. przegląd stanowisk doktryny: K. Gołębiowski, *op. cit.*, s. 56 i n.; S. Romanow, *Zarząd majątkiem dziecka sprawowany przez rodziców*, „Transformacje Prawa Prywatnego" 2021, nr 1, s. 137 i n.

[82] T. Sokołowski, [w:] *Kodeks rodzinny…*, red. H. Dolecki, T. Sokołowski, s. 697; J. Słyk, *op. cit.*, art. 101, Nb 3; S. Romanow, *op. cit.*, s. 143 i n.

[83] W tym kierunku wypowiedział się L. Kociucki, stwierdzając, że czynności takie wiążą się bezpośrednio z osobą małoletniego, ale należą również do pieczy nad jego majątkiem: L. Kociucki, *op. cit.*, s. 163.

[84] Tak T. Sokołowski, [w:] *Kodeks…*, red. A. Kidyba, art. 22, Nb 12.

z przedmiotów komunikacji elektronicznej (w tym przez zainstalowanie oprogramowania ochrony rodzicielskiej) albo uniemożliwienie ich używania będzie stanowiło naruszenie własności przedmiotów, których dziecko jest właścicielem, jak również naruszenie jego posiadania samoistnego.

Zgodnie z art. 342 k.c., nie wolno naruszać samowolnie posiadania. Ustawa chroni każde posiadanie (w dobrej i złej wierze, zgodne z prawem i bezprawne itd.[85]). W analizowanym przypadku należy jednak uznać, że naruszenie posiadania w wykonywaniu władzy rodzicielskiej nie ma charakteru samowolnego. Samowolne naruszenie posiadania to naruszenie niedozwolone (zabronione)[86]. Taki charakter naruszenia wyłącza uprawnienie wynikające z przepisów prawa[87]. Należy uznać, że z władzy rodzicielskiej wynika uprawnienie rodziców do ingerencji również we władztwo faktyczne dziecka, w tym posiadanie. Za takim wnioskiem przemawiają: charakter władzy rodzicielskiej zawierający istotne elementy władcze, a nawet publicznoprawne[88], obowiązek, a nie wyłącznie uprawnienie jej wykonywania, jak również ogólne założenie o supremacji w prawie rodzinnym praw i obowiązków niemajątkowych nad majątkowymi[89]. Z tego samego powodu – istnienia uprawnienia rodziców do ograniczenia władania dziecka tymi przedmiotami – opisane zachowania rodziców nie mogą być kwalifikowane jako bezprawne naruszenie własności i podlegać ochronie petytoryjnej.

---

[85] E. Skowrońska-Bocian, M. Warciński, *op. cit.*, art. 342, Nb 1.

[86] *Ibidem*, art. 342, Nb 5.

[87] J. Ignatowicz, *Ochrona…*, *passim*; B. Lackoroński, [w:] *Kodeks…*, art. 342, Nb 3.

[88] T. Sokołowski, *Władza rodzicielska…*, s. 93, *idem*, [w:] *Kodeks cywilny…*, red. H. Dolecki, T. Sokołowski, s. 646; A. Łapiński określał władzę rodzicielską jako funkcję społeczną: A. Łapiński, *Ograniczenia władzy rodzicielskiej,* Warszawa 1975, s. 23.

[89] J. Ignatowicz, M. Nazar, *Prawo rodzinne,* Warszawa 2016, *passim*, wskazując na zasadę uniezależnienia osobistych stosunków rodzinnych od wpływu czynników majątkowych i określając ją jako „oczywistą dla współczesnego człowieka".

4. Wnioski

Podsumowując powyższe rozważania, należy stwierdzić, że rozwiązania cywilnoprawne zostały w sposób ogólnie poprawny „zsynchronizowane" z regulacjami prawa rodzinnego i zapewniają możliwość wykonywania władzy rodzicielskiej również zakresie ochrony dziecka przed negatywnymi konsekwencjami używania, a właściwie „nadużywania" przedmiotów komunikacji elektronicznej. Stwierdzenie powyższe jest prawdziwe jednak przy przyjęciu zaproponowanej interpretacji przepisów czyniącej punktem wyjścia obowiązki i prawa rodziców, z których wynika obowiązek zapewnienia dziecku bezpieczeństwa, jak również przyjmującej, że rozwiązania cywilnoprawne mają charakter w pewnym zakresie podporządkowany i służą urzeczywistnieniu celów, jakim służy władza rodzicielska. Z uwagi na mogące rodzić się wątpliwości należałoby postulować wprowadzenie do Kodeksu rodzinnego i opiekuńczego niebudzącej wątpliwości podstawy do naruszania władztwa faktycznego dziecka nad różnymi przedmiotami, o ile następuje to w wykonywaniu władzy rodzicielskiej i jest uzasadnione dobrem dziecka.

Bibliografia

Czachórski W., *Pojęcie i treść posiadania według obowiązującego prawa rzeczowego,* „Nowe Prawo" 1957, nr 5.

Garlicki L., Zubik M., Derlatka M. (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz. Tom II*, Warszawa 2016.

Gniewek E. (red.), *System Prawa Prywatnego. Tom 4. Prawo rzeczowe*, Warszawa 2021.

Gniewek E., Machnikowski P. (red.), *Kodeks cywilny. Komentarz*, Legalis 2021.

Gocłowski M., *Posiadanie w ujęciu kodeksu cywilnego* (*Prawo podmiotowe czy stan faktyczny?*), „Państwo i Prawo" 2001, nr 2.

Gołębiowski K., *Uwagi dotyczące zarządu majątkiem dziecka pozostającego pod władzą rodzicielską*, [w:] *Wybrane zagadnienia polskiego prawa prywatnego. Księga pamiątkowa ku czci Doktora Józefa Kremisa i Doktora Jerzego Strzebińczyka*, red. J. Jezioro, K. Zagrobelny, Wrocław 2019.

Ignatowicz J., *Ochrona posiadania*, Warszawa 1963.

Ignatowicz J. (red.), *System prawa cywilnego. Tom 2. Prawo własności i inne prawa rzeczowe*, Wrocław 1977.

Ignatowicz J., Nazar M., *Prawo rodzinne,* Warszawa 2016.
Jagielski K., *Istota i treść władzy rodzicielskiej*, „Studia Cywilistyczne" 1963, t. III.
Jarosz-Żukowska S., *Konstytucyjnoprawne aspekty ochrony tajemnicy komunikowania się w Internecie*, „Przegląd Prawa i Administracji" 2008, t. LXXVIII.
Kidyba A. (red.), *Kodeks cywilny. Komentarz. Tom I. Część ogólna*, LEX 2012.
Kitłowski E., *Surogacja rzeczowa w prawie cywilnym,* Warszawa 1969.
Kołodziejski S., *Istota, treść i rodzaje posiadania*, „Palestra" 1966, nr 6, s. 18.
Księżak P., *Glosa do postanowienia Sądu Najwyższego z dnia 15 stycznia 2010 r. I CSK 355/09*, „Rejent" 2010, nr 12, s. 82.
Księżak P., *Precarium w prawie polskim*, „Rejent" 2007, nr 2.
Kunicki A., *Elementy romańskie i germańskie w konstrukcji posiadania według kodeksu cywilnego*, „Studia Prawnicze" 1970, z. 26–27.
Lackoroński B., *Wyłączenie zarządu rodziców przedmiotami przypadającymi dziecku z tytułu darowizny lub testamentu*, [w:] *Ius et Ratio. Księga Jubileuszowa Profesor Elżbiety Skowrońskiej-Bocian,* red. J. Wierciński, A. Gołaszewska, M. Olechowski, W. Borysiak, Warszawa 2022.
Nazar M., *Niektóre zagadnienia małżeństwa i rodziny w świetle unormowań Konstytucji RP z dnia 2 kwietnia 1997 r.*, „Rejent" 1997, nr 5(73).
Ohanowicz A., *Glosa do orzeczenia SN z dnia 18.X.1961 r., 4 Cr57/60*, „Państwo i Prawo" 1962, nr 8–9.
Osajda K. (red.), *Kodeks rodzinny i opiekuńczy. Komentarz Przepisy wprowadzające KRO*, Warszawa 2017.
Osajda K. (red.), *Kodeks cywilny. Komentarz*, Legalis 2021.
Ożóg M., *Prawo rodziców do wychowania dziecka zgodnie z przekonaniami w świetle Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 2997 r.*, „Studia z Prawa Wyznaniowego" 2015, t. 18.
Piątowski J.S. (red.), *System prawa rodzinnego i opiekuńczego*, Wrocław 1985.
Pietrzykowski K. (red.), *Kodeks cywilny. Tom I. Komentarz. Art. 1–449*[*10*], Legalis 2020.
Radwański Z., Olejniczak A. (red.), *System Prawa Prywatnego, Prawo cywilne – część ogólna, t. 2*, Warszawa 2019.
Rogalski M., Szustakiewicz P., *Pojęcie i zakres tajemnicy komunikacji elektronicznej*, „Ius Novum" 2022, nr 1.
Romanow S., *Zarząd majątkiem dziecka sprawowany przez rodziców*, „Transformacje Prawa Prywatnego" 2021, nr 1.
Rozwadowski W., *Spory wokół definicji czynności prawnej w polskim prawie cywilnym*, „Państwo i Prawo" 2014, nr 9.
Safjan M., Bosek L. (red.), *Konstytucja RP. Tom I. Komentarz do art. 1–86*, Warszawa 2016.
Smyczyński T. (red.), *System Prawa Prywatnego. Tom 12. Prawo rodzinne i opiekuńcze*, Warszawa 2011.
Smyczyński T., Andrzejewski M., *Prawo rodzinne i opiekuńcze*, Warszawa 2020.
Sokołowski T., *Władza rodzicielska nad dorastającym dzieckiem*, Poznań 1987.

Stelmachowski A., *Istota i funkcje posiadania*, Warszawa 1953.
Stępniak K., *Prawo do Internetu jako środka zapewniającego partycypację w państwie demokratycznym*, „Studia Prawnicze i Administracyjne" 2017, nr 21(3).
Uliasz J., *Prawna ochrona prywatności oraz wolności dzieci w Internecie*, „Zeszyty Naukowe Uniwersytetu Rzeszowskiego" 2020, z. 110.
Wolter A., Ignatowicz J., Stefaniuk K., *Prawo cywilne. Zarys części ogólnej*, Warszawa 2020.
Wolter A., *Prawo cywilne. Zarys części ogólnej,* Warszawa 1967.
Zamelski P., *Prawo do ochrony życia prywatnego*, [w:] *Konwencja o prawach dziecka. Wybór zagadnień* (*artykuły i komentarze*), red. S.L. Stadniczeńko, Warszawa 2015.
Zaradkiewicz K., *Romańska teoria posiadania a kodeks cywilny*, „Studia Iurudica", t. LXIV.
Zoll F., *Posiadanie w przyszłym kodeksie cywilnym polskim*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 1930, z. 1.

Akty prawne

Dekret z dnia 11 października 1946 r. prawo rzeczowe (Dz.U. z 1946 r., Nr 57, poz. 319).
Konwencja o prawach dziecka z dnia 20 listopada 1989 r. (Dz.U. z 1991 Nr 120, poz. 526).
Projekt ustawy o zmianie ustawy – Kodeks rodzinny i opiekuńczy oraz niektórych innych ustaw, Druk sejmowy VI kadencji nr 888.
Uchwała SN z dnia 9 czerwca 1976 r., III CZP 46/75, OSNCP 1976, Nr 9, poz. 184, teza XIII.
Ustawa z dnia 23 kwietnia 1964 r. (Dz.U z 1964 r., Nr 16, poz. 93 z późn. zm.).
Ustawa z dnia 6 listopada 2008 r. o zmianie ustawy – Kodeks rodzinny i opiekuńczy oraz niektórych innych ustaw (Dz.U. Nr 220, poz. 1431).

Katarzyna Grzelak-Bach

Centralne Biuro Zwalczania Cyberprzestępczości – główne cele na przyszłość

1. Wprowadzenie

Powszechne wykorzystywanie technologii informatycznych jest znakiem naszych czasów, swego rodzaju rewolucją cyfrową. Komputer i Internet to narzędzia, bez których nie potrafi dziś funkcjonować ani administracja, ani gospodarka, ani pojedynczy obywatel[1]. Zjawisko przestępczości lokowanej w przestrzeni wirtualnej jest związane z rosnącą liczbą użytkowników Internetu, a także z ich również finansową aktywnością w sieci[2]. Nasza aktywność w cyberprzestrzeni to nie tylko rozrywka, aktywność w social mediach, ale też jest to pozyskiwanie danych, nauka, bankowość elektroniczna czy też szeroko pojęte inwestycje. Rewolucja cyfrowa, a także związane z nią przemiany społeczne i gospodarcze obok ogromnych korzyści przyniosły także nieznane wcześniej zjawiska o przestępczym charakterze, a nieustanny postęp techniczny dodatkowo nie przystaje do formułowanych w piśmiennictwie definicji „przestępczości komputerowej"[3]. Pewne próby definiowania zjawiska podejmowane są w gremiach organizacji międzynarodowych i tak w przedmiocie cyberprzestępczości Rada Europy przyjęła konwencję z 23 listopada 2001 r.

---

[1] Por. I. Oleksiewicz, *Cyberterroryzm jako realne zagrożenie dla Polski*, „Rocznik Bezpieczeństwa Międzynarodowego" 2018, t. 12, nr 1, s. 54.

[2] M. Górka, *Wybrane aspekty polityki cyberbezpieczeństwa Unii Europejskiej na przykładzie Europolu*, „Przegląd Geopolityczny" 2018, nr 25, s. 86–103.

[3] Szerzej A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 30 i n.; M. Siwicki, *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012, nr 7–8, s. 246–256; K. Witek, *Przestępczość komputerowa – aspekty prawne*, „Edukacja – Technika – Informatyka" 2018, nr 2(24), s. 39–47.

o cyberprzestępczości[4], jednak tam treści przyjęte szybko uległy dezaktualizacji, nie nadążając za postępem i kreatywnością środowisk cyberprzestępczych[5].

Jak wynika z przeprowadzonych badań, ofiarami wszelkich form nielegalnej działalności w Internecie (w tym także związanej z rozsiewaniem wirusów komputerowych oraz innych typów złośliwego oprogramowania) padają w skali światowej setki tysięcy ofiar tego typu bezprawnej aktywności na sekundę. Krajobraz cyberbezpieczeństwa ciągle się zmienia, ale oczywiste jest, że cyberzagrożenia stają się coraz poważniejsze i występują coraz częściej. Warto jednak wskazać, że niestety aż 85% naruszeń cyberbezpieczeństwa spowodowanych jest błędem ludzkim[6], zaś 94% wszystkich złośliwych programów jest dostarczanych przez e-mail[7].

Specjaliści od cyberbezpieczeństwa wskazują, że cyberprzestępcy będą zawsze przed nami, ale wiedzą też, że dzięki czujności internautów, pracy ekspertów, współpracy wielu osób można temu zapobiec[8]. Przykładem tzw. dobrych praktyk jest działalność zespołu Dyżurnet.pl[9], kiedy to w 2020 r., trafiło do nich ponad 8 tys. zgłoszeń, z czego 2,5 tys. zostało zakwalifikowanych jako treści CSAM, czyli pokazujące seksualne wykorzystywanie dzieci. Również dzięki zgłoszeniom internautów do CERT Polska zablokowano ponad 21,5 tys. stron, które służyły do dokonywania oszustw, przestępstw. Wymaga podkreślenia,

---

[4] Konwencja jest wiążącym instrumentem międzynarodowym dotyczącym cyberprzestępczości, który zyskał szerokie międzynarodowe poparcie. Przepisy konwencji dały podstawy do stworzenia platformy międzynarodowych konsultacji w zakresie dotyczącym skutecznego stosowania i wdrażania zawartych w niej przepisów, identyfikacji związanych z tym problemów oraz wspólnych mechanizmów współpracy. Konwencja Rady Europy o cyberprzestępczości („Konwencja o cyberprzestępczości") podpisana 23 listopada 2001 r. (Dz.U. z 2015 r. poz. 728).

[5] Szerzej P. Olber, *Prawno-kryminalistyczne aspekty zabezpieczania i pozyskiwania dowodów elektronicznych z chmur obliczeniowych*, Szczytno 2021, s. 141–142.

[6] Więcej na ten temat w raporcie – https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/ (dostęp: 27.12.2022 r.).

[7] Rok 2021 był sztandarowym rokiem dla cyberprzestępców, którzy wykorzystali pandemię COVID-19 i wzrost pracy zdalnej, atakując luki zarówno techniczne, jak i społeczne. Dane na ten temat dostępne – https://www.csoonline.com/article/3634869/top-cybersecurity-statistics-trends-and-facts.html (dostęp: 1.12.2022 r.).

[8] Por. M. Wróbel, *Cyberprzestępczość w polskim systemie prawnym*, „Wiedza Obronna" 2014, nr 4, s. 72–90.

[9] W zakładce aktualności, można śledzić bieżące kampanie: https://dyzurnet.pl/aktualnosci/wpis/aplikacje-mobilne-czy-nasze-dzieci-sa-bezpieczne (dostęp: 18.12.2022 r.).

że znacząca liczba przestępstw komputerowych, pozostaje niewykryta w szarej strefie i wymyka się wszelkim statystykom[10]. Specyfika przestępstw popełnianych w cyberprzestrzeni powoduje bowiem, że wiele tego typu czynów pozostaje nieujawnionych lub nie jest poprawnie identyfikowanych jako przestępstwo. Powodem takiego stanu rzeczy jest z jednej strony fakt, że sam użytkownik komputera lub innego urządzenia, który nie ma świadomości i wiedzy, że padł ofiarą przestępstwa, z drugiej zaś zdarzenia, które są wykrywane i poprawnie kwalifikowane jako przestępne, nie zawsze zostają zgłoszone organom ścigania. W przypadku dużych firm zachowanie w tajemnicy informacji o tym, że uległy one skutecznemu atakowi hackerskiemu, w którym przełamano zbyt słabe zabezpieczenia infrastruktury teleinformatycznej przedsiębiorstwa, może nie tylko być próbą ochrony swojego wizerunku, lecz także sposobem na uniknięcie ewentualnych konsekwencji odszkodowawczych (np. informacja o cyberataku na bank, w którego wyniku mogło dojść do wycieku poufnych danych jego klientów)[11].

[10] W 2020 r. zarejestrowano 10 420 incydentów cyberbezpieczeństwa, co stanowiło wzrost o 60,7% w porównaniu do roku ubiegłego. Najpopularniejszym typem incydentu był phishing – stanowił aż 73% wszystkich obsłużonych incydentów. Liczba takich zgłoszeń wzrosła o 116% rok do roku. Znaczący wpływ na zwiększenie liczby zarejestrowanych incydentów phishingowych miała wprowadzona w marcu 2020 r. Lista Ostrzeżeń przed stronami niebezpiecznymi. Najpopularniejsze scenariusze phishingowe miały na celu zdobycie danych logowania do konta Facebook, numeru karty płatniczej lub danych logowania do bankowości internetowej. Wykorzystywano do tego m.in. wpisy na Facebooku z sensacyjnie wyglądającymi nagłówkami, fałszywe wiadomości SMS oraz wiadomości na komunikatorze WhatsApp. Raport podsumowuje zagrożenia, z jakimi mieli do czynienia polscy użytkownicy Internetu, jak również omawia działalność samego Zespołu. Raport „Krajobraz bezpieczeństwa polskiego Internetu 2020", s. 13, dostępny https://cert.pl/uploads/docs/Raport_CP_2020.pdf#page=12 (dostęp: 22.12.2021 r.).

[11] Podstawą działającego w NASK CSIRT (ang. *Computer Security Incident Response Team*) jest ustawa o krajowym systemie cyberbezpieczeństwa transponująca do polskiego prawa dyrektywę w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (tzw. dyrektywę NIS). Na mocy ustawy role CSIRT poziomu krajowego przyjęły na siebie Agencja Bezpieczeństwa Wewnętrznego (CSIRT GOV), NASK – Państwowy Instytut Badawczy (CSIRT NASK) oraz resort obrony narodowej (CSIRT MON). Współpracują one ze sobą oraz z organami właściwymi do spraw cyberbezpieczeństwa, https://www.nask.pl/pl/aktualnosci/4260,Nie-badz-obojetny-Zglaszaj-przestepstwa-dokonywane-w-sieci.html (dostęp: 11.12.2022 r.).

Z badania NASK opublikowanego we wrześniu 2021 r., dotyczącego zachowania polskich nastolatków w Internecie i ich opinii na temat sieci, w którym uwzględniono również opinie rodziców wynikało, że:

> dorośli bardziej niż ich dzieci i podopieczni ufają bezpieczeństwu swoich danych w związku z korzystaniem z internetowych serwisów hazardowych i używaniem inteligentnych urządzeń mających możliwość łączenia się z Internetem.

Ponadto, rodzice obawiają się, że wraz z cyfrową transformacją rosnąć będzie liczba incydentów zagrażających cyberbezpieczeństwu (65,8%). Według uczniów najbardziej niebezpieczne pod względem zachowania prywatności w sieci jest otwieranie podejrzanych załączników (64,5%). Kolejne wskazania respondentów dotyczyły korzystania z serwisów hazardowych (47,2%), publikowania prywatnych zdjęć (45%), filmów (43,9%) oraz aktywności w mediach społecznościowych (40,3%). Dużą liczbę wskazań uzyskały także odpowiedzi odnoszące się do sfery transakcji online: udostępniania (38,7%) oraz wysyłania (41,4%) bliskim loginu bądź hasła do kont w sklepach i serwisach aukcyjnych. Najrzadziej wskazywane odpowiedzi, a więc aktywności sieciowe, które są według respondentów najmniej ryzykowne, to korzystanie z przeglądarek (4,3%), ze stron i portali informacyjnych (4,8%), poczty internetowej (5,5%), technologii chmury (5,9%) czy wypełnianie quizów i testów w serwisach społecznościowych (6,7%). W porównaniu z poprzednią edycją badania (z 2018 r.) znacząco spadł odsetek odpowiedzi wskazujących na niebezpieczeństwo związane z korzystaniem z serwisów społecznościowych (z 58,7% do 40,3%), co wskazuje na rosnący poziom świadomości użytkowania tych platform przez uczniów[12].

W sierpniu 2021 r. EURO PAP informował (na podstawie danych Europolu), że „pandemia Covid-19 doprowadziła do znacznego wzrostu już wcześniej wysokiej liczby przypadków wykorzystywania seksualnego dzieci w Internecie"

[12] Raport „Nastolatki 3.0", https://www.nask.pl/pl/aktualnosci/4294,Raport-Nastolatki-30-mlodziez-spedza-coraz-wiecej-godzin-w-internecie.html (dostęp: 12.12.2022 r.).

oraz, że Parlament Europejski zatwierdził w lipcu nowe przepisy umożliwiające dostawcom usług internetowych dalsze dobrowolne wykrywanie, usuwanie i zgłaszanie przypadków wykorzystywania seksualnego dzieci online[13]. Z kolei coroczne międzynarodowe Badania Bezpieczeństwa Informacji EY (przeprowadzone od marca do maja 2021 r.), wśród osób zawodowo odpowiedzialnych za cyberbezpieczeństwo pokazały, że: 40% tych osób, jak nigdy dotąd niepokoiło się o zdolność organizacji do odpierania cyberzagrożeń, a 81% firm nie konsultowało planów nowych inicjatyw biznesowych z działami cyberbezpieczeństwa[14].

Ze wspólnego badania Krajowego Rejestru Długów i serwisu ChronPESEL.pl przeprowadzonego pod patronatem Urzędu Ochrony Danych Osobowych w marcu 2021 r. przez IMAS International, wynikało, że co czwarty Polak (25%) boi się ze w trakcie pandemii padnie ofiarą hakerów, a co drugi (53,8%) nie wie lub nie jest pewien jakie działania należy podjąć w przypadku wycieku danych z serwisu internetowego na którym ma się konto[15]. Trzech na dziesięciu badanych twierdziło, że w trakcie pandemii otrzymało podejrzane wiadomości skłaniające do udostępnienia danych[16]. Raport Grant Thornton opublikowany w lutym 2020 r., bazując na dwóch badaniach z 2019 r., ukazał, że polskie firmy czują się bezpiecznie. Aż 70% firm z nich na pytanie, czy są przygotowane na cyberataki, odpowiadała twierdząco. Kolejne pytania pokazały jednak, że wysoki poziom samozadowolenia wynikał raczej z niskiej świadomości

[13] Europol: znaczny wzrost przypadków wykorzystywania seksualnego dzieci w Internecie, https://europapnews.pap.pl/europol-znaczny-wzrost-przypadkow-wykorzystywania-seksualnego-dzieci-w internecie (dostęp: 12.12.2022 r.).

[14] Badanie EY dostępne: https://www.ey.com/pl_pl/news/2021/08/global-information-security-survey, (dostęp: 12.12.2022 r.). *EY: zdolność firm do odbierania cyberzagrożeń budzi wątpliwości*, https://www.wirtualnemedia.pl/artykul/cyberzagrozenia-dla-firm-co-robic (dostęp: 12.12.2022 r.).

[15] *Zagrożenia dla bezpieczeństwa i ochrony danych*, https://krd.pl/centrum-prasowe/raporty/2021/zagrozenia-dla-bezpieczenstwa-i-ochrony-danych-zdaniem-polakow (dostęp: 12.12.2022 r.).

[16] *Młodzi Polacy świadomi zagrożeń i przygotowani do ochrony danych osobowych w czasie pandemii*, https://krd.pl/centrum-prasowe/raporty/2021/mlodzi-polacy-swiadomi-zagrozen-i-przygotowani-do-ochrony-danych-osobowych-w-czasie-pandemii (dostęp: 12.12.2022 r.).

tego, czym są procedury zarządzania cyberbezpieczeństwem niż z faktycznego dobrego przygotowania na zagrożenia[17].

Wcześniej w kilku informacjach pokontrolnych NIK informowała, że Ministerstwo Edukacji Narodowej, Ministerstwo Cyfryzacji, szkoły oraz Policja nie rozpoznały właściwie i nie określiły skali zagrożenia jaką niesie cyberprzemoc wśród dzieci i młodzieży[18].

Problemy dotyczące, cyberbezpieczeństwa i współczesnych zagrożeń wymagają podjęcia działań prewencyjnych. W statystykach polskiej Policji nadal nie ma publikowanych w jednym miejscu całościowych danych dotyczących cyberprzestępczości i jej różnych aspektów[19]. Dodatkowo problemem jest brak jednolitych standardów współpracy Policji, organów prokuratury oraz sądów w zakresie działań mających na celu ustalanie tożsamości sprawcy niedozwolonych czynów. Niepokojący jest także brak świadomości osób, których mienie lub dobra osobiste zostały naruszone, co do tego, iż przysługują im jakiekolwiek środki prawne pozwalające na egzekwowanie praw. Rzecznik Praw Obywatelskich zwracał wielokrotnie się o poinformowanie o przyjętej praktyce, a także wytycznych, jakie posiadają prokuratorzy prowadzący sprawy dotyczące przestępstw popełnianych za pośrednictwem Internetu, a związanych m.in. z naruszeniem dóbr osobistych użytkowników sieci. Rzecznik prosił też o sugestie odnośnie do systemowych działań, które mogłyby wpłynąć pozytywnie na ochronę praw obywateli[20].

---

[17] *Zamek z papieru, czyli zarządzanie ryzykiem cyfrowym w polskich firmach z badań*, https://grantthornton.pl/wp-content/uploads/2020/02/Zamek-z-papieru-czyli-zarz%C4%85dzanie-ryzykiem-cyfrowym-RAPORT-Grant-Thornton-26-02-2020-1.pdf (dostęp: 3.12.2022 r.).

[18] *NIK o cyberprzemocy wśród dzieci i młodzieży*, https://www.nik.gov.pl/aktualnosci/nik-o-cyberprzemocy wsrod-dzieci-i-mlodziezy.html (dostęp: 3.12.2022 r.).

[19] Na stronie polskiej Policji znajdziemy szereg artykułów dotyczących przedmiotowego zjawiska, https://policja.pl/pol/tagi/301,cyberprzestepczosc.html (dostęp: 3.12.2022 r.), jednakże statystyk skupiających w jednym miejscu przestępstwa popełnione z wykorzystaniem sieci, niestety brak https://statystyka.policja.pl/st/wybrane-statystyki (dostęp: 28.12.2022 r.).

[20] Treść wystąpienia RPO z dnia 6 września 2012 r. do Prokuratora Generalnego, https://sprawy-generalne.brpo.gov.pl/pdf//2012/08/710680/1668392.pdf (dostęp: 10.12.2022 r.).

2. Centralne Biuro Zwalczania Cyberprzestępczości

Odpowiedzią na stale rozwijającą się przestępczość w sieci ma być powołane 12 stycznia 2022 r. Centralne Biuro Zwalczania Cyberprzestępczości (dalej: CBZC)[21]. Specgrupa wysoko wykwalifikowanych funkcjonariuszy Policji ma być odpowiedzialna za rozpoznawanie, zapobieganie i zwalczanie przestępstw popełnionych przy użyciu nowoczesnych technologii teleinformatycznych na terenie całego państwa oraz wspieranie w niezbędnym zakresie pozostałych jednostek organizacyjnych Policji, głównie poprzez zwiększenie zdolności operacyjnych[22].

Pomysł stworzenia kompleksowych rozwiązań[23], wynikał z analiz skali cyberprzestępczości oraz w związku z pilną potrzebą podnoszenia jakości działania służb bezpieczeństwa i porządku publicznego i ich możliwości operacyjnych w zakresie realizowanych zadań ustawowych. Upowszechnienie dostępu do Internetu, w kontekście globalnego charakteru cyberprzestrzeni, przy jednocześnie stosunkowo dużej możliwości zachowania anonimowości sprzyjało bowiem występowaniu różnego rodzaju zagrożeń nie tylko dotyczących bezpieczeństwa systemów informatycznych, ale także o charakterze stricte przestępczym (dotyczącym m.in. przestępczości o charakterze ekonomicznym, kryminalnym, w tym przestępstw pedofilskich czy narkotykowych). Planowane zmiany strukturalne w Policji poprzez stworzenie jednostki właściwej w zakresie zwalczania przestępczości w cyberprzestrzeni (CBZC), będą stanowiły odpowiedź w zakresie zwiększenia bezpieczeństwa wewnętrznego, zarówno w skali krajowej, jak i międzynarodowej. Działania nakierowane

[21] Szczegóły na temat nowej formacji w polskiej Policji, https://policja.pl/pol/cbzc (dostęp: 1.12.2022 r.).

[22] Projekt został złożony jako przedłożenie rządowe, Ministrem odpowiedzialnym za przedstawienie wniosku do wykazu praw Rady Ministrów był Minister Maciej Wąsik, Sekretarz Stanu w MSWiA, https://legislacja.rcl.gov.pl/projekt/12351202l (dostęp: 13.12.2022 r.).

[23] Na konferencji prasowej w Kancelarii Prezesa Rady Ministrów 27 lipca 2021 r., ogłoszono, że warto aby polska Policja miała odpowiednie instrumenty, najlepsze rozwiązania i kompetencje do walki z cyberprzestępczością, żeby mogli jak najlepiej odpowiadać na te zagrożenia, toteż zapowiedziano powstanie nowej jednostki Policji – Centralnego Biura Zwalczania Cyberprzestępczości – https://www.gov.pl/web/mswia/powstanie-centralne-biuro-zwalczania-cyberprzestepczosci (dostęp: 22.12.2021 r.).

na wzmocnienie skuteczności Policji przełożą się bezpośrednio na zwiększenie ogólnokrajowego poziomu bezpieczeństwa i stabilizacji porządku publicznego. Pozwolą one w szczególności na unowocześnienie wyposażenia i zapewnienie jego adekwatności względem środków wykorzystywanych przez przestępców.

Szczegółowe analizy wykazały, że na przestrzeni ostatnich lat wzrosła znacząco skala cyberprzestępczości, co przejawiało się m. in. poprzez wzrost liczby incydentów związanych z mową nienawiści oraz tzw. hejtu w sieci (ang. *cyberbullying*); oszustw popełnianych w cyberprzestrzeni oraz zdarzeń z wykorzystaniem złośliwego oprogramowania; oszustw i wymuszeń przy wykorzystaniu narzędzi anonimizujących, a także przestępstw finansowych, w tym prania pieniędzy pochodzących z przestępstw, przede wszystkim z wykorzystaniem kryptowalut[24]. Rosnącą skalę cyberprzestępczości w Polsce pokazały również statystyki, wskazujące, że największa liczba cyberprzestępstw była popełniana w określonych kategoriach przestępstw takich jak przeciwko: mieniu; prawom autorskim i prawom pokrewnym; wolności seksualnej i obyczajności; ochronie informacji; wiarygodności dokumentów; własności przemysłowej; wolności; czci i nietykalności cielesnej[25]. Pomysłodawcy projektu, w załączonym dokumencie oceny skutków regulacji (dalej: OSR) dowodzili słuszności podjęcia działań legislacyjnych, które miały doprowadzić do stworzenia kompleksowych rozwiązań systemowych. Podnoszono, że polska Policja, jak i organy ścigania innych państw, nie są w pełni przygotowane na walkę z nowoczesnymi formami przestępczości, w tym szczególnie z cyberprzestępczością[26].

[24] Dokument oceny skutków regulacji z 13 października 2021 r., załączony do projektu Ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości, s. 1, https://legislacja.rcl.gov.pl/projekt/12351202/katalog/12814938#12814938 (dostęp: 22.12.2022 r.).

[25] *Ibidem*.

[26] Por. tezę M. Stefanowicz: „Jest przewidywany dalszy wzrost przestępczości w zakresie wykorzystania zaawansowanych technologii informatycznych, które mogą dotyczyć nowych aspektów, jak np. upowszechniający się podpis elektroniczny. Internet będzie używany także do szantażu i wyłudzeń, np. poprzez groźbę wykorzystania luk w zabezpieczeniach systemów komputerowych lub «eksploatację» skradzionych informacji. Będzie ujawniana coraz większa liczba przestępstw komputerowych o wysokiej jednostkowo wartości strat, a także nastąpi dalszy wzrost liczby oszustw na aukcyjnych portalach internetowych. Największym zagrożeniem najprawdopodobniej będzie – ze względu na mało skomplikowany charakter przestępstwa – oszustwo dokonywane z wykorzystaniem platform handlowych i portali aukcyjnych".

Wynika to m.in. z charakteru czynności wykonywanych przez służbę kryminalną, w ramach której funkcjonują komórki organizacyjne zwalczające cyberprzestępczość, w których schemat działań oparty jest na ściganiu sprawców cyberprzestępstw, a nie na działaniach związanych z rozpoznawaniem i zapobieganiem tego rodzaju przestępczości. W większości przypadków działania policjantów zwalczających cyberprzestępczość rozpoczynają się w momencie uzyskania informacji o zaistniałym incydencie, tym samym sprawcy czynów zabronionych są o krok przed organami ścigania. Zgodnie z treścią informacji zawartych w OSR, niezbędne stało się ustanowienie jednolitej w skali kraju jednostki organizacyjnej Policji i powołanie w tym celu nowej służby w ramach Policji[27]. Efektywność działania Policji w zakresie zapobiegania i zwalczania cyberprzestępczości wymagała także zapewnienia skutecznego i profesjonalnego wyszkolenia funkcjonariuszy. W OSR wyjaśniono, iż mimo że od 2016 r. w ramach struktury Komendy Głównej Policji funkcjonowało Biuro do Walki z Cyberprzestępczością, które realizowało czynności związane z wykrywaniem sprawców przestępstw popełnionych przy użyciu nowoczesnych technologii teleinformatycznych, a także na poziomie komend wojewódzkich Policji (oraz Komendzie Stołecznej Policji) istnieją natomiast komórki organizacyjne, podległe właściwemu miejscowo komendantowi wojewódzkiemu Policji (Komendantowi Stołecznemu Policji), to powołanie CBZC było niezbędne[28].

W OSR znajduje się też szczegółowy opis struktury nowo utworzonej jednostki. Projektodawca, nawiązując do struktur Centralnego Biura Śledczego Policji, zaproponował powierzenie kierowania nowotworzoną jednostką Policji Komendantowi CBZC jako organowi podległemu Komendantowi Głównemu Policji, który jednocześnie stawał się bezpośrednim przełożonym policjantów CBZC. Komendanta CBZC będzie powoływał spośród oficerów Policji i odwoływał minister właściwy ds. wewnętrznych na wniosek Komendanta Głównego Policji, natomiast Zastępców Komendanta CBZC będzie powoływał spośród oficerów i odwoływał Komendant Główny Policji na wniosek

M. Stefanowicz, *Cyberprzestępczość – próba diagnozy zjawiska,* „Kwartalnik Policyjny" 2017, nr 4, s. 19–24.

[27] Dokument oceny skutków regulacji z 13 października 2021 r., s. 2.

[28] *Ibidem*, s. 3.

Komendanta CBZC. Komendant CBZC będzie posiadał również pełne kompetencje kadrowo-szkoleniowe w stosunku do policjantów CBZC. Uznano, że utworzenie CBZC usprawni koordynację działań Policji w zakresie zapobiegania i zwalczania przestępstw popełnianych przy użyciu nowoczesnych technologii teleinformatycznych. Planowane zmiany strukturalne umożliwią również dokonywanie wyspecjalizowanego doboru funkcjonariuszy do służby zwalczania cyberprzestępczości[29]. Jednocześnie funkcjonariusze nowej służby nadal będą mogli korzystać ze wszystkich uprawnień przysługujących dotychczas funkcjonariuszom Policji, co przy jednoczesnym przypisaniu określonych uprawnień Komendantowi CBZC przyspieszy dotychczas realizowane procedury[30].

Projekt na rządowym etapie prac legislacyjnych spotkał się z pośrednim odbiorem[31], zarówno przez opinię publiczną jak też członków rządu. Główne wątpliwości budziło m.in. zrezygnowanie z testów sprawnościowych kandydatów do służby w CBZC[32], a także obawy związane z tzw. „drenażem kadr",

[29] W pracach nad ustawą rząd zapewniał, głównie w doniesieniach medialnych, że żadna z 350 obecnie zajmujących się w Policji zwalczaniem cyberprzestępczości osób, nie straci pracy po powołaniu nowej formacji. Mogą najwyżej zostać skierowani do innych zadań, ale ich doświadczenia przydadzą się w Policji. Policjanci w CBZC będą dodatkowo wynagradzani – będzie im przysługiwał stały dodatek nie niższy niż 70 proc. i nie wyższy niż 130 proc. miesięcznego przeciętnego uposażenia policjantów. – https://niebezpiecznik.pl/post/centralne-biuro-zwalczania-cyberprzestepczosci/; a także https://www.telepolis.pl/wiadomosci/prawo-finanse-statystyki/policja-internet-cyberprzestepcy-cbcz (dostęp: 17.12.2022 r.).

[30] Dokument oceny skutków regulacji z dnia 13 października 2021 r., s. 3–4.

[31] CBZC będzie uprawnione do tworzenia, nabywania i użytkowania specjalnych programów komputerowych i urządzeń „hakerskich", dzięki którym, jak wskazuje Wnioskodawca, Policjanci służby zwalczania cyberprzestępczości, będą mogli uzyskać dostęp do informacji dla nich nieprzeznaczonych, przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne ich zabezpieczenia, jak też dostęp do całości lub części systemu teleinformatycznego. Stosowane wspomnianych rozwiązań technologiczny ma służyć na zasadach określonych w ustawie do zapobiegania i zwalczania przestępstw, przy których możliwe jest stosowanie czynności operacyjno-rozpoznawczych (co do zasady wymagane postanowienie sądu okręgowego po zgodzie prokuratury) – Nadmierne rozszerzenie kontroli operacyjnej to jedno z podstawowych zastrzeżeń wobec projektu powołującego w policji jednostkę do zwalczania cyberprzestępczości – szerzej: https://praca.gazetaprawna.pl/artykuly/8287125,-cyberpolicja-ustawa-rozszerzona-kontrola-operacyjna-nowelizacja.html (dostęp: 7.12.2022 r.).

[32] „[…] dla sprawnej realizacji zadań związanych ze zwalczaniem cyberprzestępczości niezbędne jest zapewnienie zasobu kadrowego, to jednak jako wątpliwa jawi się zasadność wyeliminowania z etapów postępowania kwalifikacyjnego dla kandydatów do służby zwalczania cyberprzestępczości testu wiedzy i testu sprawności fizycznej", https://legislacja.rcl.gov.pl/docs//2/12351202/12814938/12814941/dokument527805.pdf (dostęp: 4.12.2022 r.).

głównie z grona pracowników administracji publicznej rządowej czy też samorządowej[33]. Docelowo, służba zwalczania cyberprzestępczości ma liczyć łącznie zatrudnianych sukcesywnie[34] do 2025 r. 1 800 funkcjonariuszy, zaś infrastruktura niezbędna do pełnej działalności na zostać przygotowana finalnie do 2031 r.[35] Ustawa wprowadza zmiany w procedurze naboru do służby w Policji, które mają na celu umożliwienie prowadzenia postępowania kwalifikacyjnego w stosunku do kandydatów ubiegających się o przyjęcie bezpośrednio do służby w jednostce zwalczania cyberprzestępczości – dodany zostaje etap postępowania kwalifikacyjnego w postaci sprawdzenia wiedzy i umiejętności z zakresu informatyki, funkcjonowania systemów informatycznych, systemów teleinformatycznych, sieci teleinformatycznych oraz znajomości języka obcego z tego zakresu.

---

[33] Dr Łukasz Olejnik, badacz i konsultant cyberbezpieczeństwa, pytany przez CyberDefence24.pl o pomysł powołania Centralnego Biura Zwalczania Cyberprzestępczości twierdził, że: „Nie jesteśmy dziś w stanie ocenić czy może dojść do ryzyka kanibalizacji innych jednostek przez CBZC, ale jeśli taki problem by zaistniał, to byłoby to wysoce niefortunne. One zajmują się trochę innymi obszarami, ale oczywiście finanse są ważne. Trzeba by pomyśleć o zapewnieniu dobrych warunków finansowych szerzej, wszystkim; […] Wydaje mi się, że to może być ciekawa oferta dla niektórych osób zainteresowanych tym obszarem cyberbezpieczeństwa. Bardzo dużo będzie też zależało od kierownictwa i dowództwa tej struktury […] Jeśli chodzi wyłącznie o kwestie finansowe, to oczywiście nie można konkurować bezpośrednio na tym polu z rynkiem komercyjnym. Ale to niekoniecznie musi być problem. Trzeba by jednak pomyśleć nad zagwarantowaniem, że nie dojdzie do finansowej konkurencji z innymi strukturami państwowymi, bo mogłoby dojść wtedy do czasowego ryzyka destabilizacji", https://www.cyberdefence24.pl/pomysl-stworzenia-cbzc-przynosi-wiele-pytan-wazny-nadzor-etyczno-prawny (dostęp: 23.11.2021 r.).

[34] Harmonogram zatrudniania oraz kalkulacja wydatków osobowych: w 2022 r. – 300 etatów, w 2023 r. – 500 etatów, w 2024 r. – 500 etatów, w 2025 r. – 500 etatów – więcej w dokumencie oceny skutków regulacji z 13 października 2021 r., s. 9.

[35] Oszacowane koszty utworzenia CBZC wynoszą 4,43 mld zł w ciągu 10 lat, w tym 450 mln zł na budowę siedziby CBZC oraz 250 mln zł na zakupy sprzętu – nie zaprezentowano jednak szczegółowych założeń oszacowania tych kosztów, na podstawie szacunkowej skali zadań, które będzie realizować CBZC. Wskazane zostały jedynie przesłanki pozyskania nowej siedziby na potrzeby CBZC o zwiększonej etatyzacji oraz ogólna charakterystyka narzędzi i wyposażenia, którymi powinna dysponować nowa służba. Jednakże nie przedstawiono podstaw oszacowania potrzeb zwiększenia etatyzacji Policji o 1 800 etatów w CBZC (koszty w ciągu 10 lat dla budżetu państwa – 3 472 mln zł, wpływy sektora finansów publicznych z tytułu podatku dochodowego i składek – 615 mln zł). Całość finansowania będzie pochodzić z rezerw celowych budżetu państwa, które będą musiały ulec zwiększeniu. – więcej dokument oceny skutków regulacji z 13 października 2021 r., s. 7.

Ustawa rozszerza katalog przestępstw, w przypadku których możliwe jest zastosowanie kontroli operacyjnej, o przestępstwa określone w następujących przepisach Kodeksu karnego[36]:

- art. 200a k.k. – elektroniczna korupcja seksualna małoletniego,
- art. 200b k.k. – propagowanie pedofilii,
- art. 224a k.k. – fałszywy alarm,
- art. 267 § 1–4 k.k. – hacking komputerowy, czyli bezprawne uzyskanie informacji,
- art. 268a § 1 i 2 k.k. – niszczenie danych informatycznych,
- art. 269 k.k. – sabotaż komputerowy – zakłócenie systemu,
- art. 269a k.k. – zakłócenie pracy w sieci,
- art. 269b § 1 k.k. – bezprawne wykorzystanie programów i danych,
- art. 279 § 1 k.k. – kradzież z włamaniem,
- art. 287 § 1 k.k. – oszustwo komputerowe.

W ustawie uregulowano także kwestie związane z kierowaniem policjantów na przeszkolenie, do szkoły, na studia wyższe lub podyplomowe w kraju lub za granicą, a także na aplikacje w zawodach prawniczych, realizowane poza jednostkami szkoleniowymi Policji. Przewidziano zawarcie umowy, gdy koszt nauki przekraczać będzie kwotę sześciokrotności wysokości wynagrodzenia minimalnego. Ustawa określa także przypadki, w których powstanie konieczność zwrotu kosztów poniesionych na naukę oraz możliwość zwolnienia z obowiązku zwrotu – w szczególnych przypadkach uzasadnionych sytuacją życiową, rodzinną lub materialną[37].

Projekt, dynamicznie przeprocedowany na etapie rządowym, trafił do laski marszałkowskiej już 12 listopada 2021 r.[38], gdzie poddano projekt badaniu w Biurze Analiz Sejmowych[39]. Projekt ustawy stanowił przedłożenie rządowe

[36] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. Dz.U. z 2020 r. poz. 1444 z późn. zm.).

[37] Rządowy projekt ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości, https://www.sejm.gov.pl/sejm9.nsf/agent.xsp?symbol=RPL&Id=RM-0610-139-21 (dostęp: 2.12.2022 r.).

[38] Druk sejmowy nr 1742, https://www.sejm.gov.pl/Sejm9.nsf/PrzebiegProc.xsp?nr=1742 (dostęp: 5.12.2022 r.).

[39] M. Bajor-Stachańczyk, *Ocena skutków prawnych regulacji zawartej w rządowym projekcie ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw w związku z powołaniem*

(druk sejmowy nr 1742). Pierwsze czytanie projektu odbyło się 17 listopada 2021 r. na 42 posiedzeniu Sejmu. Zgłoszony wniosek o odrzucenie projektu w pierwszym czytaniu nie uzyskał poparcia. Projekt został skierowany do Komisji Administracji i Spraw Wewnętrznych. Komisja przyjęła sprawozdanie (druk sejmowy nr 1796), w którym zarekomendowała Sejmowi przyjęcie załączonego projektu ustawy.

Podczas prac nad rządowym projektem posłowie skrócili tytuł samej ustawy, na bardziej oddający istotę przepisów „o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości". W głosowaniach posłowie odrzucili część poprawek zgłoszonych w II czytaniu, m.in. ograniczającą prawo nowej formacji do kontroli operacyjnej. Przyjęli jedną poprawkę dotyczącą uszczegółowienia zasad prowadzenia naboru kandydatów do nowej formacji w części badania psychologicznego – by jego częścią był test psychologiczny, co wzbudzało pewne wątpliwości już na etapie prac rządowych[40]. Na etapie prac senackich ustawa również podlegała ocenie, tym razem Biura Legislacyjnego Senatu[41]. Senat jednogłośnie przyjął – wraz z poprawkami – przepisy dotyczące powołania Centralnego Biura Zwalczania Cyberprzestępczości. Za ustawą niemal jednogłośnie zagłosowało 98 senatorów[42]. W dniu 20 grudnia 2021 r. ustawę przekazano do podpisu Prezydentowi RP[43], zaś 28 grudnia 2021 r.,

---

Centralnego Biura Zwalczania Cyberprzestępczości (*druk sejmowy nr 1742*), 24 listopada 2021 r., https://www.sejm.gov.pl/Sejm9.nsf/opinieBAS.xsp?nr=1742 (dostęp: 3.12.2022 r.).

[40] Druk nr 1796-A, Dodatkowe sprawozdanie Komisji Administracji i Spraw Wewnętrznych o rządowym projekcie ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości, https://www.sejm.gov.pl/Sejm9.nsf/druk.xsp?nr=1796-A (dostęp: 3.12.2022 r.).

[41] B. Mandylis, *Opinia do ustawy o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości* (*druk senacki nr 588*), 13 grudnia 2021 r., https://www.senat.gov.pl/gfx/senat/pl/senateksper tyzy/6180/plik/5880.pdf (dostęp: 3.12.2022 r.).

[42] Druk 588-Z, Sprawozdanie Komisji Samorządu Terytorialnego i Administracji Państwowej oraz Komisji Praw Człowieka, Praworządności i Petycji (wraz z zestawieniem wniosków) o ustawie o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości, https://www.senat.gov.pl/prace/druki/page,3.html?nr=588&kadencja=10 (dostęp: 3.12.2022 r.).

[43] Ustawa z dnia 17 grudnia 2021 r. o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości – podpisana 28 grudnia 2021 r., https://www.prezydent.pl/prawo/ustawy-podpisane/ustawy-podpisane-w-grudniu-2021-r,45902 (dostęp: 9.12.2022 r.).

dokonano publikacji ustawy[44]. 12 stycznia 2022 r. ustawa weszła w życie – powołano Centralne Biuro Zwalczania Cyberprzestępczości. 1 maja 2022 r. Minister Spraw Wewnętrznych i Administracji Mariusz Kamiński z dniem 1 maja 2022 r. powołał insp. Adama Cieślaka na stanowisko Komendanta Centralnego Biura Zwalczania Cyberprzestępczości, zaś 16 maja 2022 r. Komendant Główny Policji gen. insp. Jarosław Szymczyk powołał mł. insp. Michała Pudło oraz kom. Marcina Bednarza na zastępców Komendanta Centralnego Biura Zwalczania Cyberprzestępczości[45].

Wejście w życie ustawy otworzyło zatem nowy rozdział w polskiej Policji, dając wachlarz nowych możliwości, ale też stawiając wysoko oczekiwania, które systematycznie wzrastają poprzez pomysłowość przestępców i postęp technologiczny. Oprogramowanie i sprzęt systemów informatycznych i telekomunikacyjnych aktualnie posiadanych w ramach struktur Policji wymagają znacznego udoskonalenia, a w szczególności unowocześnienia systemów operacyjnych, które będą musiały charakteryzować się zwiększoną niezawodnością i bezpieczeństwem, rozwoju sprzętu do ochrony danych, urządzeń komunikacyjnych, protokołów transmisji danych. Warto bowiem mieć na uwadze, że liczba cyberataków na organizacje i osoby fizyczne jest znacząca i według prognoz będzie rosła[46]. Przeznaczenie z budżetu państwa środków na utworzenie służby zwalczania cyberprzestępczości wzmocniło motywacyjny system uposażeń funkcjonariuszy zapobiegających i zwalczających cyberprzestępczość, co pozwoliło na pozyskanie osób posiadających fachową wiedzę w tym zakresie, w warunkach konkurencyjnych wynagrodzeń oferowanych dla specjalistów w tej dziedzinie przez inne służby czy rynek komercyjny. Warto w tym miejscu również wspomnieć o świadczeniu teleinformatycznym, bowiem 1 stycznia 2022 r.

[44] Ustawa z dnia 17 grudnia 2021 r. o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości, data ogłoszenia 28 grudnia 20221 r., (Dz.U. z 2021 r., poz. 2447), https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20210002447 (dostęp: 9.12.2022 r.).

[45] Kalendarium dostępne – https://cbzc.policja.gov.pl/bzc/o-cbzc/historia-powstania/12,Historia-powstania-Centralnego-Biura-Zwalczania-Cyberprzestepczosci.html (dostęp: 27.12.2022 r.).

[46] J. Runowicz-Piotrowska, *Sprawozdanie z międzynarodowej konferencji naukowej „Krajobraz cyberprzestępczości w dobie COVID-19", Szczytno* (*formuła online*)*, 17 marca 2021 r.*, „Policja" 2021, nr 1, s. 41–47.

weszły w życie przepisy ustawy określającej zasady przyznawania świadczenia teleinformatycznego osobom realizującym zadania z zakresu cyberbezpieczeństwa, ustawą objęto również funkcjonariuszy Policji[47]. Przepisy rozporządzenia wskazują zaś na możliwe stawki przyznanego świadczenia wypłacanego obok wynagrodzenia zasadniczego, co ma zatrzymać odpływ wysoko wykwalifikowanej kadry z instytucji publicznych[48].

Nowoczesne służby do walki z cyberprzestępczością muszą mieć możliwość korzystania z najnowszych narzędzi do wyszukiwania, akwizycji, zabezpieczania oraz analizy danych cyfrowych tak, aby cyfrowy materiał dowodowy, zdobyty z wykorzystaniem tych narzędzi był pełnoprawny i respektowany przez sądy. Fakt, że świat przestępczy wykorzystuje coraz bardziej wyrafinowane metody ukrywania swojej działalności, wymusza na organach ścigania posiadanie coraz bardziej zaawansowanych (a zatem droższych) narzędzi. Nowo utworzona jednostka organizacyjna Policji posiada na swoim wyposażeniu urządzenia, za pomocą których będzie możliwe wysoko zaawansowane wyodrębnianie cyfrowych danych kryminalistycznych m.in. z komputerów stacjonarnych, urządzeń mobilnych, chmur cyfrowych, dronów czy też innych urządzeń podłączonych do Internetu (IoT). Dodatkowo niezbędnym wyposażeniem CBZC będzie mobilne laboratorium informatyki śledczej, komputery stacjonarne i przenośne o zwiększonej mocy obliczeniowej, serwery. CBZC to także inwestycja w bardzo zaawansowany sprzęt, odpowiednie serwery oraz wysoko wyspecjalizowane oprogramowanie, po to aby „nadążyć" za przestępcami działającymi w cyberprzestrzeni. Zakupiono również wymagane aplikacje

[47] Świadczenie teleinformatyczne można też przyznać osobom realizującym zadania w zakresie zapewnienia cyberbezpieczeństwa w służbach, czyli w ABW, AW, CBA, jednostkach organizacyjnych podległych premierowi lub ministrom, Kancelarii premiera oraz w urzędach obsługujących ministrów, Kancelarii Prezydenta RP, Kancelarii: Sejmu i Senatu, Policji, prokuraturze, SKW, SWW, Straży Granicznej oraz Służbie Ochrony Państwa – Ustawa z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz.U. 2021 poz. 2333).

[48] Rozporządzenie określa wysokości świadczenia teleinformatycznego dla osób realizujących zadania z zakresu cyber (ustawa określa max, tj. dwudziestojednokrotność kwoty bazowej dla członków korpusu służby cywilnej). Wysokość uzależniona od rodzaju zadań i doświadczenia eksperta (min. 2000 zł, max. 30 000 zł) – Rozporządzenie Rady Ministrów z dnia 19 stycznia 2022 r. w sprawie wysokości świadczenia teleinformatycznego dla osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz.U. z 2022 r., poz. 131).

służące do kompleksowego przetwarzania i analizy danych pochodzących z różnych źródeł: komputerów, dysków, urządzeń mobilnych, chmury, zasobów sieciowych i innych. Ważnym czynnikiem będzie także posiadanie dostępu do komercyjnych serwisów pozwalających na szybką weryfikację tożsamości oraz zintegrowanie ich z posiadanymi systemami. Na budowę siedziby CBZC zaplanowano bowiem kwotę 450 mln zł[49].

Oczekiwania społeczne są bardzo duże, ale też funkcjonariusze, liczą że specjalna grupa zyska nie tylko prestiż ale i godne warunki płacowe. W chwili obecnej wynagrodzenia funkcjonariuszy zajmujących się ściganiem cyberprzestępczości nie są atrakcyjne pod względem finansowym dla osób posiadających specjalistyczne wykształcenie i wiedzę w obszarze niezbędnym lub pożądanym w celu zwalczania cyberprzestępczości[50]. Od kilku lat obserwowana jest stała fluktuacja wykwalifikowanej kadry z instytucji rządowych. Rynek pracy jest zdecydowanie bardziej konkurencyjny niż kilka lat temu, np. w branży IT średnie zarobki mogą osiągać poziom 20–40 tys. zł, a zapotrzebowanie na fachowców w tej dziedzinie rośnie i będzie wzrastało coraz szybciej[51]. Utworzenie CBZC, ale także przyznanie świadczenia teleinformatycznego[52], to działania zmierzające do zatrzymania w formacji wysoko wykwalifikowanych funkcjonariuszy Policji, a także pozyskanie nowych kandydatów do pracy, co potwierdza dostrzeżenie

[49] Więcej informacji na temat przyszłej infrastruktury i kosztów CBZC – dokument oceny skutków regulacji z 13 października 2021 r., s. 8.

[50] W dniu 18 stycznia 2022 r. zostało opublikowane rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 12 stycznia 2022 r. w sprawie postępowania kwalifikacyjnego w stosunku do kandydatów ubiegających się o przyjęcie do służby w Policji (Dz.U. poz. 109), gdzie zawarte są szczegółowe informacje dotyczące wymagań, jakie muszą spełnić kandydaci ubiegający się do służby w CBZC.

[51] Rządowe podmioty zajmujące się cyberbezpieczeństwem mają poważny problem kadrowy. Chodzi o to, że warunki finansowe w polskiej branży IT w sektorze prywatnym są obecnie znacznie lepsze niż to, co może zaoferować państwo. Więcej: https://www.wirtualnemedia.pl/artykul/cyberbezpieczenstwo-pensje (dostęp: 2.12.2022 r.).

[52] Oferuje się specjalne świadczenie dla funkcjonariuszy pełniących służbę na stanowisku związanym z bezpośrednim rozpoznawaniem i zwalczaniem przestępstw popełnionych przy użyciu systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej oraz zapobieganiem tym przestępstwom, a także wykrywaniem i ściganiem sprawców tych przestępstw. Świadczenie to wynosi od 70 do 130% przeciętnego uposażenia policjantów. Na dzień 7 listopada 2022 r. dodatek ten kształtuje się na poziomie 4800–8800 zł brutto. Więcej informacji – https://cbzc.policja.gov.pl/bzc/aktualnosci/92,Ruszyl-proces-doboru-do-Centralnego-Biura-Zwalczania-Cyberprzestepczosci.html (dostęp: 27.12.2022 r.).

i refleksję nad problemem „podkupowania" przez rynek komercyjny. Zadaniem nowopowstałej jednostki jest rozpoznawanie i zwalczanie przestępstw popełnionych przy użyciu systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej oraz zapobiegania tym przestępstwom, a także wykrywania i ścigania sprawców tych przestępstw. Funkcjonariusze pełniący służbę w CBZC będą również wspierali w niezbędnym zakresie jednostki organizacyjne Policji w rozpoznawaniu, zapobieganiu i zwalczaniu tego typu przestępstw. Zatem obecnie poszukiwani są kandydaci z wiedzą z zakresu nowoczesnych technologii, informatyki, programowania, którzy chcieliby zrobić coś dobrego zwalczając przestępczość internetową, chcieliby ochronić innych przed zagrożeniami i stanąć po dobrej stronie sieci, mogą zostać policjantem CBZC[53].

3. Rozwiązania krajowe w zakresie walki z cyberatakami w wybranych państwach – omówienie

W Holandii funkcjonuje Narodowe Centrum Cyberbezpieczeństwa (NCSC), które stanowi część Ministerstwa Sprawiedliwości i Bezpieczeństwa[54]. Zadania tego podmiotu od 9 listopada 2018 r. reguluje ustawa o bezpieczeństwie systemów sieciowych i informatycznych (niderl. *Wet beveiliging netwerk- en informatiesystemen*, WBNI)[55]. WBNI określa ustawowe zadania NCSC w zakresie cyberbezpieczeństwa. Organizacje z kluczowych sektorów oraz rząd centralny są zobowiązane do zgłaszania do NCSC poważnych incydentów związanych z bezpieczeństwem cyfrowym. Dostawcy podstawowych usług (niderl. *aanbieders van essentiële diensten*, AED) oraz dostawcy usług cyfrowych (DSP) muszą przestrzegać przepisów niniejszego prawa. WBNI ma na celu zwiększenie odporności cyfrowej Holandii, złagodzenie skutków incydentów cybernetycznych, a tym

[53] Nabór do formacji - https://cbzc.policja.gov.pl/bzc/rekrutacja/dobor-do-sluzby-w-cbzc/74,Praca-i-sluzba-w-CBZC.html (dostęp: 27.12.2022 r.).

[54] Dodatkowe informacje: https://english.ncsc.nl/about-the-ncsc (dostęp: 15.12.2022 r.).

[55] Test aktu normatywnego dostępny: https://wetten-overheid-nl.translate.goog/BWBR0041515/2021-08-01?_x_tr_sl=nl&_x_tr_tl=pl&_x_tr_hl=pl&_x_tr_pto=sc (dostęp: 3.12.2022 r.).

samym zapobieganie zakłóceniom społecznym. W przypadku zagrożenia lub incydentu w sieci i systemach informatycznych ważnych dostawców, organów rządowych lub DSP, funkcjonują komputerowe zespoły kryzysowe, które zapewniają niezbędną pomoc. WBNI określa te zespoły mianem CSIRT (ang. *Computer Security Incident Response Teams*)[56]. Zgodnie z WBNI, CSIRT dla AED jest Narodowe Centrum Cyberbezpieczeństwa (NCSC). Do zadań NCSC należy m.in.: reagowanie na incydenty zgłaszane dobrowolnie lub w ramach obowiązku zgłoszenia; monitorowanie incydentów na poziomie krajowym, zapewnianie wczesnego ostrzegania usługodawców oraz rozpowszechnianie informacji o zagrożeniach i incydentach; uczestnictwo w międzynarodowej sieci CSIRT, a także utrzymywanie kontaktów ukierunkowanych na współpracę z sektorem prywatnym[57].

Kolejnym podmiotem wartym uwagi, jest szwajcarskie Narodowe Centrum Bezpieczeństwa Cybernetycznego (NCSC) jest centrum kompetencyjnym Konfederacji w zakresie bezpieczeństwa cybernetycznego, a tym samym pierwszym punktem kontaktowym dla przedsiębiorstw, administracji publicznej, instytucji edukacyjnych i ogółu społeczeństwa w kwestiach cybernetycznych[58]. Jest odpowiedzialne za skoordynowane wdrażanie krajowej strategii ochrony Szwajcarii przed cyberzagrożeniami na lata 2018–2022 (NCS). Cyberbezpieczeństwo odgrywa kluczową rolę w krajowej i międzynarodowej polityce zagranicznej i polityce bezpieczeństwa, a także staje się coraz ważniejszym czynnikiem zarówno dla ogółu społeczeństwa, jak i dla Szwajcarii jako miejsca prowadzenia działalności gospodarczej. Poprzez utworzenie NCSC, pod kierownictwem Federalnego Delegata ds. Bezpieczeństwa Cybernetycznego, Rada Federalna ma na celu wspieranie ludności, gospodarki, instytucji edukacyjnych i administracji publicznej w ochronie przed zagrożeniami cybernetycznymi i poprawie bezpieczeństwa własnych systemów. Przyjęte przez Radę Federalną rozporządzenie

[56] Więcej o działalności instytucji: https://www.sidn.nl/en/cybersecurity/sidn-csirt (dostęp: 3.12.2022 r.).

[57] Więcej na temat działań: https://english.ncsc.nl/about-the-ncsc/statutory-task (dostęp: 3.12.2022 r.).

[58] Więcej informacji: https://www.ncsc.admin.ch/ncsc/en/home/ueber-ncsc/das-ncsc.html (dostęp: 3.12.2022 r.).

w sprawie ochrony przed cyberzagrożeniami w administracji federalnej (CyRO) weszło w życie w dniu 1 lipca 2020 r.[59] Stanowi ono podstawę prawną dla utworzenia i rozbudowy NCSC, a także reguluje strukturę, zadania i obowiązki zaangażowanych organów. Centrum Raportowania i Analiz Bezpieczeństwa Informacji (MELANI), wraz z krajowym zespołem reagowania na incydenty komputerowe (GovCERT), zostało włączone do NCSC jako ośrodek wiedzy technicznej i dalej rozbudowywane. Nowo utworzony krajowy punkt kontaktowy otrzymuje zgłoszenia o cyberincydentach od społeczeństwa i środowiska biznesowego, analizuje je i przedstawia zgłaszającym ocenę incydentu, a także zalecenia dotyczące dalszych działań[60].

Litewskie Narodowe Centrum Cyberbezpieczeństwa podlegające Ministerstwu Obrony Narodowej (NCSC) jest główną litewską instytucją zajmującą się cyberbezpieczeństwem, odpowiedzialną za jednolite zarządzanie incydentami cybernetycznymi, monitorowanie i kontrolę realizacji wymogów cyberbezpieczeństwa, akredytację zasobów informacyjnych[61]. Misja NCSC to bycie centrum wiedzy o cyberbezpieczeństwie dla skutecznego zarządzania incydentami cybernetycznymi i silnego systemu zapobiegania cyberbezpieczeństwu w kraju. Zatwierdzony regulamin NCSC przewiduje następujące główne cele operacyjne instytucji: realizacja polityki cyberbezpieczeństwa państwa; wykonywanie funkcji Służby Bezpieczeństwa; wykonywanie funkcji krajowej służby ochrony łączności; upowszechnianie informacji, prowadzenie badań i analiz dotyczących zagadnień cyberbezpieczeństwa. Od 2018 r. na zasadzie jednego okienka NCSC zapewnia pomoc instytucjom państwowym i biznesowym oraz obywatelom. W ramach swoich kompetencji NCSC podejmuje decyzje wraz z instytucjami i organizacjami państwowymi oraz innymi podmiotami

[59] Raporty z działalności dostępne – National Cyber Security Centre NCSC, https://www.ncsc.admin.ch/ncsc/en/home/dokumentation/berichte/lageberichte/halbjahresbericht-2021-1.html (dostęp: 4.12.2022 r.).

[60] Szerzej o działalności na rzecz społeczeństwa i poszczególnych programów: https://www.ncsc.admin.ch/ncsc/en/home/dokumentation/sensibilisierung/sensibilisierung_oeffentlichkeit.html (dostęp: 4.12.2022 r.).

[61] Więcej o działalności instytucji: https://www.nksc.lt/en/ (dostęp: 4.12.2022 r.).

gospodarczymi w sprawach zasobów informacyjnych państwa oraz krytycznej infrastruktury teleinformatycznej w zakresie cyberbezpieczeństwa[62].

Irlandzkie Narodowe Centrum Cyberbezpieczeństwa (NCSC) zostało założone w 2011 r. i jest operacyjnym ramieniem Departamentu Środowiska, Klimatu i Komunikacji (DECC). NCSC jest odpowiedzialne za doradzanie i informowanie rządowych dostawców IT i krytycznej infrastruktury narodowej o bieżących zagrożeniach i podatnościach związanych z bezpieczeństwem informacji w sieci. Do głównych zadań NCSC należy kierowanie zarządzaniem poważnymi incydentami związanymi z bezpieczeństwem cybernetycznym w całym rządzie, zapewnianie obywatelom i przedsiębiorstwom wskazówek i porad dotyczących poważnych incydentów związanych z bezpieczeństwem cybernetycznym oraz rozwijanie silnych międzynarodowych relacji w globalnej społeczności bezpieczeństwa cybernetycznego w celu wymiany informacji[63]. Narodowe Centrum Cyberbezpieczeństwa Irlandii (NCSC) angażuje się w kompleksowy zestaw zadań związanych z bezpieczeństwem cybernetycznym, koncentrując się przede wszystkim na zabezpieczeniu sieci rządowych i zabezpieczeniu krytycznej infrastruktury narodowej podejmując działania mające na celu zmniejszenie podatności krytycznych systemów i sieci w państwie na incydenty i ataki cybernetyczne[64].

W Portugalii funkcjonujące Krajowe Centrum Cyberbezpieczeństwa (CNCS) ma za zadanie pomagać obywatelom i firmom w korzystaniu z cyberprzestrzeni w sposób bezpłatny, niezawodny i bezpieczny. Narodowe Centrum Bezpieczeństwa Cybernetycznego (CNCS) rozwija swoją misję, mając na celu przyczynienie się do swobodnego, niezawodnego i bezpiecznego korzystania z cyberprzestrzeni w interesie narodowym w kontekście bezpiecznej interakcji, w jak największym stopniu, ludzi, procesów i technologii. Pełniąc rolę koordynatora operacyjnego i organu krajowego w kwestiach bezpieczeństwa cybernetycznego dla podmiotów państwowych, operatorów krajowej infrastruktury krytycznej, operatorów podstawowych usług i dostawców usług

[62] Prezentacja struktury podmiotu: https://www.nksc.lt/en/structure.html (dostęp: 4.12.2022 r.).

[63] Więcej o działalności instytucji: https://www.ncsc.gov.ie/ (dostęp: 13.12.2022 r.).

[64] Dodatkowe informacje: https://www.ncsc.gov.ie/about/ (dostęp: 14.12.2022 r.).

cyfrowych, CNCS przekazuje również swoje działania ogółowi społeczeństwa. CNCS opracowuje zestaw działań skierowanych do obywateli i organizacji[65].

Narodowy Instytut Bezpieczeństwa Cybernetycznego Hiszpanii (INCIBE) działa na rzecz wzmocnienia zaufania cyfrowego, zwiększenia bezpieczeństwa i odporności cybernetycznej oraz przyczynia się do rozwoju rynku cyfrowego w celu promowania bezpiecznego korzystania z cyberprzestrzeni w Hiszpanii. INCIBE jest spółką podlegającą Ministerstwu Spraw Gospodarczych i Transformacji Cyfrowej za pośrednictwem Sekretarza Stanu ds. Cyfryzacji i Sztucznej Inteligencji i stał się jednostką wzorcową w zakresie rozwoju bezpieczeństwa cybernetycznego i zaufania cyfrowego dla obywateli, sieci akademickich i badawczych, specjalistów, przedsiębiorstw, a zwłaszcza dla sektorów strategicznych. Dzięki działalności opartej na badaniach, świadczeniu usług i koordynacji z podmiotami posiadającymi kompetencje w tej dziedzinie, INCIBE przyczynia się do budowania bezpieczeństwa cybernetycznego na poziomie krajowym i międzynarodowym. Misją INCIBE jest wzmocnienie bezpieczeństwa cybernetycznego, zaufania oraz ochrony informacji i prywatności w usługach społeczeństwa informacyjnego, zapewniając wartość dla obywateli, przedsiębiorstw, administracji, hiszpańskiej sieci akademickiej i badawczej, sektora technologii informacyjnych i komunikacyjnych oraz sektorów strategicznych w ogóle[66].

Bibliografia

Adamski A., *Prawo karne komputerowe*, Warszawa 2000.

Bajor-Stachańczyk M., *Ocena skutków prawnych regulacji zawartej w rządowym projekcie ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości* (*druk sejmowy nr 1742*), 24 listopada 2021 r.

Górka M., *Wybrane aspekty polityki cyberbezpieczeństwa Unii Europejskiej na przykładzie Europolu*, „Przegląd Geopolityczny" 2018, nr 25.

[65] Więcej o działalności instytucji: https://www.cncs.gov.pt/pt/sobre-nos/ (dostęp: 14.12.2022 r.).

[66] Więcej o działalności instytucji: https://www.incibe.es/que-es-incibe (dostęp: 3.12.2022 r.).

Mandylis B., *Opinia do ustawy o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości* (*druk senacki nr 588*), 13 grudnia 2021 r.
Olber P., *Prawno-kryminalistyczne aspekty zabezpieczania i pozyskiwania dowodów elektronicznych z chmur obliczeniowych*, Szczytno 2021.
Oleksiewicz I., *Cyberterroryzm jako realne zagrożenie dla Polski*, „Rocznik Bezpieczeństwa Międzynarodowego" 2018, t. 12, nr 1.
Runowicz-Piotrowska J., *Sprawozdanie z międzynarodowej konferencji naukowej „Krajobraz cyberprzestępczości w dobie COVID-19", Szczytno* (*formuła online*), *17 marca 2021 r.*, „Policja" 2021, nr 1.
Siwicki M., *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012, nr 7–8.
Stefanowicz M., *Cyberprzestępczość – próba diagnozy zjawiska*, „Kwartalnik Policyjny" 2017, nr 4.
Witek K., *Przestępczość komputerowa – aspekty prawne*, „Edukacja – Technika – Informatyka" 2018, nr 2(24).
Wróbel M., *Cyberprzestępczość w polskim systemie prawnym*, „Wiedza Obronna" 2014, nr 4.

Akty prawne

Konwencja Rady Europy o cyberprzestępczości podpisana 23 listopada 2001 r. (Dz.U. z 2015 r., poz. 728).
Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 12 stycznia 2022 r. w sprawie postępowania kwalifikacyjnego w stosunku do kandydatów ubiegających się o przyjęcie do służby w Policji (Dz.U. poz. 109).
Ustawa z dnia 17 grudnia 2021 r. o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości (Dz.U. z 2021 r., poz. 2447).
Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. Dz.U. z 2020 r. poz. 1444 z późn. zm.).

Netografia

https://cert.pl/uploads/docs/Raport_CP_2020.pdf#page=12 (dostęp: 3.12.2022 r.).
https://dyzurnet.pl/aktualnosci/wpis/aplikacje-mobilne-czy-nasze-dzieci-sa-bezpieczne (dostęp: 3.12.2022 r.).
https://english.ncsc.nl/about-the-ncsc (dostęp: 3.12.2022 r.).
https://english.ncsc.nl/about-the-ncsc/statutory-task (dostęp: 3.12.2022 r.).
https://europapnews.pap.pl/europol-znaczny-wzrost-przypadkow-wykorzystywania-seksualnego-dzieci-w internecie (dostęp: 3.12.2022 r.).

https://grantthornton.pl/wp-content/uploads/2020/02/Zamek-z-papieru-czyli-zarz%C4%85dzanie-ryzykiem-cyfrowym-RAPORT-Grant-Thornton-26-02-2020-1.pdf (dostęp: 3.12.2022 r.).
https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20210002447 (dostęp: 3.12.2022 r.).
https://krd.pl/centrum-prasowe/raporty/2021/mlodzi-polacy-swiadomi-zagrozen-i-przygotowani-do-ochrony-danych-osobowych-w-czasie-pandemii (dostęp: 3.12.2022 r.).
https://krd.pl/centrum-prasowe/raporty/2021/zagrozenia-dla-bezpieczenstwa-i-ochrony-danych-zdaniem-polakow (dostęp: 3.12.2022 r.).
https://legislacja.rcl.gov.pl/docs//2/12351202/12814938/12814941/dokument527805.pdf (dostęp: 3.12.2022 r.).
https://legislacja.rcl.gov.pl/projekt/12351202/katalog/12814938#12814938 (dostęp: 3.12.2022 r.).
https://legislacja.rcl.gov.pl/projekt/12351202l (dostęp: 3.12.2022 r.).
https://niebezpiecznik.pl/post/centralne-biuro-zwalczania-cyberprzestepczosci/ (dostęp: 3.12.2022 r.).
https://policja.pl/pol/cbzc (dostęp: 3.12.2022 r.).
https://policja.pl/pol/tagi/301,cyberprzestepczosc.html (dostęp: 3.12.2022 r.).
https://praca.gazetaprawna.pl/artykuly/8287125,cyberpolicja-ustawa-rozszerzona-kontrola-operacyjna-nowelizacja.html (dostęp: 3.12.2022 r.).
https://sprawy-generalne.brpo.gov.pl/pdf//2012/08/710680/1668392.pdf (dostęp: 3.12.2022 r.).
https://statystyka.policja.pl/st/wybrane-statystyki (dostęp: 3.12.2022 r.).
https://wetten-overheid-nl.translate.goog/BWBR0041515/2021-0801?_x_tr_sl=nl&_x_tr_tl=pl&_x_tr_hl=pl&_x_tr_pto=sc (dostęp: 3.12.2022 r.).
https://www.cncs.gov.pt/pt/sobre-nos/ (dostęp: 3.12.2022 r.).
https://www.csoonline.com/article/3634869/top-cybersecurity-statistics-trends-and-facts.html (dostęp: 3.12.2022 r.).
https://www.cyberdefence24.pl/pomysl-stworzenia-cbzc-przynosi-wiele-pytan-wazny-nadzor-etyczno-prawny (dostęp: 3.12.2022 r.).
https://www.ey.com/pl_pl/news/2021/08/global-information-security-survey (dostęp: 3.12.2022 r.).
https://www.gov.pl/web/mswia/powstanie-centralne-biuro-zwalczania-cyberprzestepczosci (dostęp: 3.12.2022 r.).
https://www.incibe.es/que-es-incibe (dostęp: 3.12.2022 r.).
https://www.nask.pl/pl/aktualnosci/4260,Nie-badz-obojetny-Zglaszaj-przestepstwa-dokonywane-w-sieci.html (dostęp: 3.12.2022 r.).
https://www.nask.pl/pl/aktualnosci/4294,Raport-Nastolatki-30-mlodziez-spedza-coraz-wiecej-godzin-w-internecie.html (dostęp: 3.12.2022 r.).
https://www.ncsc.admin.ch/ncsc/en/home/dokumentation/berichte/lageberichte/halbjahresbericht-2021-1.html (dostęp: 3.12.2022 r.).

https://www.ncsc.admin.ch/ncsc/en/home/dokumentation/sensibilisierung/sensibilisierung_oeffentlichkeit.html (dostęp: 3.12.2022 r.).
https://www.ncsc.admin.ch/ncsc/en/home/ueber-ncsc/das-ncsc.html (dostęp: 3.12.2022 r.).
https://www.ncsc.gov.ie/ (dostęp: 3.12.2022 r.).
https://www.ncsc.gov.ie/about/ (dostęp: 3.12.2022 r.).
https://www.nik.gov.pl/aktualnosci/nik-o-cyberprzemocy wsrod-dzieci-i-mlodziezy.html (dostęp: 3.12.2022 r.).
https://www.nksc.lt/en/ (dostęp: 3.12.2022 r.).
https://www.nksc.lt/en/structure.html (dostęp: 3.12.2022 r.).
https://www.prezydent.pl/prawo/ustawy-podpisane/ustawy-podpisane-w-grudniu-2021-r,45902 (dostęp: 3.12.2022 r.).
https://www.sejm.gov.pl/sejm9.nsf/agent.xsp?symbol=RPL&Id=RM-0610-139-21 (dostęp: 3.12.2022 r.).
https://www.sejm.gov.pl/Sejm9.nsf/druk.xsp?nr=1796-A (dostęp: 3.12.2022 r.).
https://www.sejm.gov.pl/Sejm9.nsf/opinieBAS.xsp?nr=1742 (dostęp: 3.12.2022 r.).
https://www.sejm.gov.pl/Sejm9.nsf/PrzebiegProc.xsp?nr=1742 (dostęp: 3.12.2022 r.).
https://www.senat.gov.pl/gfx/senat/pl/senatekspertyzy/6180/plik/5880.pdf (dostęp: 3.12.2022 r.).
https://www.senat.gov.pl/prace/druki/page,3.html?nr=588&kadencja=10 (dostęp: 3.12.2022 r.).
https://www.sidn.nl/en/cybersecurity/sidn-csirt (dostęp: 3.12.2022 r.).
https://www.telepolis.pl/wiadomosci/prawo-finanse-statystyki/policja-internet-cyberprzestepcy-cbcz (dostęp: 3.12.2022 r.).
https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/ (dostęp: 3.12.2022 r.).
https://www.wirtualnemedia.pl/artykul/cyberbezpieczenstwo-pensje (dostęp: 3.12.2022 r.).
https://www.wirtualnemedia.pl/artykul/cyberzagrozenia-dla-firm-co-robic (dostęp: 3.12.2022 r.).

Agnieszka Mikos-Sitek

Cyberbezpieczeństwo w działalności sektora bankowego – regulacje krajowe

1. Wprowadzenie

Postępujący rozwój technologiczny jest stale obecny w różnych obszarach funkcjonowania rynku finansowego, a konieczność transformacji cyfrowej dotyczy wszystkich uczestników tego rynku, w tym banków. Przed sektorem bankowym, spełniającym kryteria w zakresie stosowania najbardziej nowoczesnych rozwiązań cyfrowych, pojawia się wiele wyzwań, również tych związanych z zapewnieniem bezpieczeństwa świadczonych usług. W ostatnich latach można zaobserwować – co zdecydowanie będzie także udziałem przyszłości – stale rosnące oczekiwania klientów banków w zakresie stosowania w praktyce bankowej zaawansowanych technologii, co jest konsekwencją postępującego procesu cyfryzacji poszczególnych aspektów życia codziennego. W procesie postępującej rewolucji cyfrowej, obejmującej swoim zakresem niemal wszystkie dziedziny życia społeczno-gospodarczego, potrzeby i oczekiwania klientów banków także podlegają stałym zmianom. Proces ten jest dodatkowym wyzwaniem dla banków, biorąc pod uwagę fakt, że postępuje on w szybkim tempie i towarzyszą mu dodatkowo oczekiwania równie szybkiego dostosowania rozwiązań wykorzystywanych w praktyce bankowej. Należy jednocześnie zwrócić uwagę, że proces cyfryzacji dotyczy pełnego *spectrum* działania banków. Nie mówimy w tym przypadku wyłącznie o świadczeniu usług i kontakcie z klientem, ale również o wewnętrznych rozwiązaniach składających się na ogólnie rozumianą sferę organizacyjną funkcjonowania banku.

Rozwój technologiczny niesie ze sobą wiele pozytywnych skutków, jednak w zależności od analizowanych aspektów tego rozwoju należy również dostrzec jego negatywne konsekwencje. Dotyczą one m.in. coraz bardziej dotkliwych w skutkach działań przestępczych zagrażających bezpieczeństwu korzystania

z bankowości elektronicznej. Nasilenie zjawisk związanych z cyberprzestępczością ma swoją odpowiedz w stosownych działaniach banków, innych uczestników rynku finansowego oraz instytucji publicznych odpowiedzialnych za poszczególne aspekty funkcjonowania tego rynku. Z korzystaniem z bankowości elektronicznej wiąże się szczególna odpowiedzialność, która po stronie banków związana jest z koniecznością stworzenia i korzystania z infrastruktury zapewniającej bezpieczeństwo świadczonych usług, a co za tym idzie bezpieczeństwo zgromadzonych w banku środków. Odpowiedzialność ta dotyczy również klienta banku, który przy dokonywaniu wszelkich transakcji powinien wykazać się znajomością zasad bezpieczeństwa, a także stosować się do wytycznych banku w zakresie koniecznych reguł bezpiecznego korzystania z bankowości elektronicznej. W obydwu przypadkach zasadniczą miarą w ocenie prawidłowości działań jest zachowanie staranności.

Z punktu widzenia banków problematyka cyberbezpieczeństwa ma jednak szczególne znaczenie, ponieważ stanowi ono czynnik determinujący zaufanie klientów. Na banki – jako instytucje zaufania publicznego – nakłada się w tym zakresie szczególne obowiązki, czemu towarzyszą również wysokie oczekiwania klientów. Doświadczenia ostatnich lat pokazują dodatkowo, że pomimo wielości regulacji i działań służących zachowaniu bezpieczeństwa problem cyberprzestępczości narasta i wymaga stałej uwagi regulacyjnej oraz kształtowania norm i standardów technologicznych o charakterze ochronnym.

2. Podstawowe regulacje prawne

Istotnym elementem kształtującym warunki bezpiecznego korzystania z rozwiązań cyfrowych są obowiązujące regulacje prawne. Kwestie dotyczące cyberbezpieczeństwa oraz leżące u jego podstaw wymagania techniczne, działania prewencyjne, edukacyjne oraz wzorce bezpiecznych zachowań coraz częściej stają się przedmiotem zarówno krajowych, jak również unijnych regulacji prawnych. Ze względu na rosnącą skalę działań przestępczych, coraz bardziej dotkliwe konsekwencje tych działań oraz zmieniające się formy cyberataków – problematyka cyberbezpieczeństwa jest dla ustawodawcy materią stanowiącą

szczególne wyzwanie. Wymaga bowiem stworzenia kompleksowych rozwiązań prawnych dających podstawę funkcjonowania systemu cyberbezpieczeństwa gwarantującego skuteczne zapobieganie zagrożeniom, ale również środków zaradczych w przypadku ich wystąpienia.

W krajowym porządku prawnym problematyka cyberbezpieczeństwa została uregulowana ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[1]. Określa ona organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w jego skład. Powołana ustawa reguluje również sposób sprawowania nadzoru i kontroli w zakresie stosowania jej przepisów, a także zakres Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej (art. 1 k.s.c.u.). Ustawa stanowi implementację do polskiego porządku prawnego dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[2].

Zgodnie z art. 3 k.s.c.u. krajowy system cyberbezpieczeństwa ma na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych (czyli takich, które mają kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej i są wymienione w wykazie usług kluczowych, art. 2 pkt 16 k.s.c.u.) i usług cyfrowych (co oznacza usługi świadczone drogą elektroniczną w rozumieniu przepisów ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[3], wymienionych w załączniku Nr 2 do ustawy o krajowym systemie bezpieczeństwa, tj. usługi internetowej platformy handlowej, przetwarzania w chmurze oraz wyszukiwarki internetowej, zob. art. 2 pkt 15 k.s.c.u.). Artykuł 3 k.s.c.u. wyjaśnia jednocześnie, że cel, jakiemu ma służyć wdrożenie krajowego systemu bezpieczeństwa, zostanie osiągnięty przy zapewnieniu odpowiedniego

[1] T.j. Dz.U. z 2022 r. poz. 1863 z późn. zm.; dalej: k.s.c.u.
[2] Dz.Urz. UE L nr 194, s. 1 (tzw. dyrektywa NIS).
[3] T.j. Dz.U. z 2020 r. poz. 344.

poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów[4].

Zgodnie z art. 4 k.s.c.u. krajowy system cyberbezpieczeństwa obejmuje:

1/ operatorów usług kluczowych,
2/ dostawców usług cyfrowych,
3/ CSIRT MON (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej, art. 2 pkt 2 k.s.c.u.),
4/ CSIRT NASK (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy, art. 2 pkt 3 k.s.c.u.),
5/ CSIRT GOV (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego, art. 2 pkt 1 k.s.c.u.),
6/ sektorowe zespoły cyberbezpieczeństwa,
7/ jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1–6, 8, 9, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych[5],
8/ instytuty badawcze,
9/ Narodowy Bank Polski,
10/ Bank Gospodarstwa Krajowego,
11/ Urząd Dozoru Technicznego,
12/ Polską Agencję Żeglugi Powietrznej,
13/ Polskie Centrum Akredytacji,
14/ Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej,

[4] Zob. F. Radoniewicz, [w:] *Ustawa o krajowym systemie bezpieczeństwa. Komentarz*, red. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019, art. 3; J. Dysarz, [w:] *Ustawa o krajowym systemie bezpieczeństwa. Komentarz*, red. A. Besiekierska, Warszawa 2019, art. 3.

[5] T.j. Dz.U. z 2022 r. poz. 1634 z późn. zm.

15/ spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej[6],
16/ podmioty świadczące usługi z zakresu cyberbezpieczeństwa,
17/ organy właściwe do spraw cyberbezpieczeństwa,
18/ Pojedynczy Punkt Kontaktowy do spraw cyberbezpieczeństwa,
19/ Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa,
20/ Kolegium do Spraw Cyberbezpieczeństwa.

Zakresem podmiotowym ustawy o krajowym systemie bezpieczeństwa zostali objęci zatem w pierwszej kolejności operatorzy usług kluczowych, które analizowana regulacja określa jako usługi o kluczowym znaczeniu dla utrzymania krytycznej działalności społecznej lub gospodarczej wymienione w wykazie usług kluczowych objętych załącznikiem Nr 1 do tej ustawy (art. 2 pkt 16, art. 5 ust. 1 k.s.c.u.)[7]. Doprecyzowano jednocześnie, że operatorem usług kluczowych może być podmiot, który prowadzi działalność wymienioną w wykazie objętym załącznikiem Nr 1 i posiada jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej[8]. Wymaga się ponadto, aby organ właściwy do spraw cyberbezpieczeństwa wydał decyzję o uznaniu danego podmiotu za operatora usługi kluczowej (art. 5 ust. 1 k.s.c.u.). Wydanie przedmiotowej decyzji jest możliwe przy spełnieniu następujących warunków:

1/ podmiot świadczy usługę kluczową,
2/ świadczenie tej usługi jest zależne od systemów informacyjnych,
3/ incydent miałby istotny skutek zakłócający dla świadczenia usługi kluczowej przez ten podmiot (art. 5 ust. 1 k.s.c.u.)[9].

---

[6] T.j. Dz.U. z 2021 r. poz. 679.

[7] Zob. również rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (Dz.U. poz. 1806).

[8] Zob. również rozporządzenie Ministra Cyfryzacji z dnia 14 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo (Dz.U. poz. 2479).

[9] Zob. więcej P. Wajda, *Cyberbezpieczeństwo – sektorowe aspekty regulacyjne*, „IKAR" 2020, nr 2, s. 14 i n.; A. Czarnecka, *Wybrane obowiązki operatorów usług kluczowych na gruncie ustawy o krajowym systemie cyberbezpieczeństwa*, „Informacja w Administracji Publicznej"

Przepisy ustawy precyzują jednocześnie, że istotność skutku zakłócającego incydentu dla świadczenia usługi kluczowej określana jest na podstawie progów istotności skutku zakłócającego (art. 5 ust. 3 k.s.c.u.).

Katalog objęty art. 4 k.s.c.u. wymienia również dostawców usług cyfrowych (zdefiniowanych powyżej), ale również grupę podmiotów publicznych[10], w tym m.in. Narodowy Bank Polski oraz Bank Gospodarstwa Krajowego (art. 4 pkt 9, 10 k.s.c.u.), a w zakres ich obowiązków wpisano przede wszystkim wyznaczenie osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, zarządzanie i obsługę incydentów, zapewnienie osobom, na rzecz których zadanie publiczne jest realizowane, dostępu do wiedzy i użytecznych informacji o cyberbezpieczeństwie oraz określone ustawą obowiązki informacyjne (art. 21–25 k.s.c.u.)[11].

Rozwiązania przyjęte w Polsce dotyczące wskazania organów właściwych w sprawach cyberbezpieczeństwa[12] charakteryzują się podziałem kompetencji pomiędzy różne podmioty – a regulujący tę kwestię art. 41 k.s.c.u. wskazuje w tej grupie przede wszystkim ministrów właściwych dla określonego sektora gospodarki. Biorąc pod uwagę materię niniejszego opracowania, należy jednak przede wszystkim zwrócić uwagę, że jako organ właściwy do spraw cyberbezpieczeństwa dla sektora bankowego i infrastruktury rynków finansowych wskazano Komisję Nadzoru Finansowego (art. 41 pkt 4 k.s.c.u.). Poszczególne zadania i obowiązki organów właściwych w sprawach cyberbezpieczeństwa uregulowano wspólnie (art. 42 i n. k.s.c.u.), różnią się one oczywiście zakresem przedmiotowym związanym z charakterem działalności każdego z nich.

2019, nr 2, s. 64–65; B. Biderman, K. Mroczka, *Uwarunkowania prawne nadzoru nad cyberbezpieczeństwem rynku finansowego w Polsce*, „Bezpieczny Bank" 2022, nr 2(87), s. 51 i n.; S. Dygnatowski, W. Dygnatowski, *Prawne podstawy cyberbezpieczeństwa na tle polskiego i europejskiego ustawodawstwa*, „Journal of KONBiN" 2020, vol. 50, Issue 4, s. 326–328.

[10] Więcej zob. A. Besiekerska, *Ustawa o krajowym systemie cyberbezpieczeństwa. Wybrane obowiązki jednostek sektora finansów publicznych i spółek prawa handlowego wykonujących zadania o charakterze użyteczności publicznej*, „Informacja w Administracji Publicznej" 2019, nr 1, s. 61 i n.

[11] P. Pelc, *Wybrane regulacje dotyczące cyberbezpieczeństwa instytucji finansowych*, „Cybersecurity and Law" 2021, vol. 6, s. 132.

[12] Zob. art. 8 ust. 2 dyrektywy NIS. Zob. również K. Gawkowski, *Bezpieczeństwo cyberprzestrzeni w regulacjach UE*, „Teka of Political Science and International Relations" 2018, t. 13, no 2, s. 65 i n.

Komisja Nadzoru Finansowego – podobnie jak pozostałe organy właściwe w sprawach cyberbezpieczeństwa – realizuje zatem zadania sformułowane w ustawie w obrębie 11 punktów obejmujących:

1/ prowadzenie bieżącej analizy podmiotów w danym sektorze lub podsektorze pod kątem uznania ich za operatora usługi kluczowej lub niespełniania warunków kwalifikujących podmiot jako operatora usługi kluczowej;
2/ wydawanie decyzji o uznaniu podmiotu za operatora usługi kluczowej albo decyzji stwierdzających wygaśnięcie decyzji o uznaniu podmiotu za operatora usługi kluczowej;
3/ przekazywanie do ministra właściwego do spraw informatyzacji wniosków o wpisanie do wykazu operatorów usług kluczowych albo wykreślenie z tego wykazu – niezwłocznie po wydaniu decyzji o uznaniu za operatora usługi kluczowej albo decyzji stwierdzającej wygaśnięcie decyzji o uznaniu za operatora usługi kluczowej;
4/ składanie wniosków o zmianę danych w wykazie operatorów usług kluczowych, nie później niż w terminie 6 miesięcy od zmiany tych danych;
5/ przygotowywanie we współpracy z CSIRT NASK, CSIRT GOV, CSIRT MON i sektorowymi zespołami cyberbezpieczeństwa rekomendacji dotyczących działań mających na celu wzmocnienie cyberbezpieczeństwa, w tym wytycznych sektorowych dotyczących zgłaszania incydentów;
6/ monitorowanie stosowania przepisów ustawy przez operatorów usług kluczowych i dostawców usług cyfrowych;
7/ wzywanie na wniosek CSIRT NASK, CSIRT GOV lub CSIRT MON operatorów usług kluczowych lub dostawców usług cyfrowych do usunięcia w wyznaczonym terminie podatności, które doprowadziły lub mogły doprowadzić do incydentu poważnego, istotnego lub krytycznego;
8/ prowadzenie kontroli operatorów usług kluczowych i dostawców usług cyfrowych;
9/ możliwość prowadzenia współpracy z właściwymi organami państw członkowskich Unii Europejskiej za pośrednictwem Pojedynczego Punktu Kontaktowego;

10/ przetwarzanie informacji, w tym danych osobowych, dotyczących świadczonych usług kluczowych i usług cyfrowych oraz operatorów usług kluczowych lub dostawców usług cyfrowych w zakresie niezbędnym do realizacji zadań wynikających z ustawy;
11/ uczestnictwo w ćwiczeniach w zakresie cyberbezpieczeństwa organizowanych w Rzeczypospolitej Polskiej lub w Unii Europejskiej (art. 42 ust. 1 k.s.c.u.).

Przepisy ustawy o krajowym systemie bezpieczeństwa przewidują przy tym możliwość delegowania zadań przez organ właściwy w sprawach cyberbezpieczeństwa jednostkom podległym lub nadzorowanym. Odbywa się to na podstawie zawartego porozumienia, a okoliczność taka jest związana dodatkowo z obowiązkami informacyjnymi (zob. art. 42 ust. 3–6 k.s.c.u.)[13].

Regulacją istotną z punktu widzenia bezpieczeństwa funkcjonowania sektora bankowego jest również ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych[14]. Ustawa ta nakłada na dostawców usług płatniczych, do których należą także podmioty sektora bankowego (art. 4 u.p.u.), obowiązek podejmowania środków ograniczających ryzyko oraz wprowadzania mechanizmów kontroli służących zarządzaniu ryzykiem operacyjnym oraz ryzykiem naruszenia bezpieczeństwa w zakresie świadczenia usług płatniczych. Działania te dostawca powinien podejmować w ramach systemu zarządzania ryzykiem (zob. w odniesieniu do wymogu posiadania systemu zarządzania ryzykiem, art. 64 ust. 1 pkt 3 u.p.u.) i realizować je w szczególności przez działania związane z:

1/ utrzymywaniem skutecznej procedury zarządzania incydentami, w tym na potrzeby wykrywania i klasyfikacji poważnych incydentów operacyjnych i incydentów związanych z bezpieczeństwem, w tym o charakterze teleinformatycznym,

[13] W niektórych przypadkach przepisy analizowanej ustawy precyzują dodatkowo katalog zadań i obowiązków w odniesieniu do poszczególnych podmiotów (zob. przede wszystkim art. 45, 51 k.s.c.u.). Zob. również B. Biderman, K. Mroczka, *op. cit.*, s. 56–58; K. Walczuk, [w:] *stawa o krajowym systemie bezpieczeństwa. Komentarz*, red. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019, art. 41, 42; J. Dysarz, *op. cit.*, art. 41, 42; A. Czarnecka, *op. cit.*, s. 64–65.

[14] T.j. Dz.U. z 2022 r. poz. 2360 z późn. zm.; dalej: u.p.u.

2/ bieżącą oceną i aktualizacją procedur w zakresie zarządzania ryzykiem operacyjnym i ryzykiem naruszenia bezpieczeństwa, w tym bezpieczeństwa teleinformatycznego, a także bieżącą oceną środków ograniczających ryzyko oraz mechanizmów kontroli (art. 32f ust. 1 u.p.u.).

Wymagania dotyczące systemu zarządzania ryzykiem zostały określone w pkt 2 Wytycznych EBA z dnia 12 stycznia 2018 r. w sprawie środków bezpieczeństwa dotyczących ryzyk operacyjnych i ryzyk dla bezpieczeństwa usług płatniczych[15]. Wytyczne te zostały wydane zgodnie z dyrektywą Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniającą dyrektywy 2002/65/WE, 2009/10/WE, 2013/36/UE i rozporządzenie (UE) Nr 1093/2010 oraz uchylającą dyrektywę 2007/64 (zob. art. 95 ust. 1)[16].

Zgodnie z Wytycznymi EBA dostawcy usług płatniczych powinni opracować skuteczny system zarządzania ryzykami operacyjnymi i ryzykami dla bezpieczeństwa, który powinien podlegać systematycznemu przeglądowi. Powinien być ujęty w formie kompleksowego dokumentu dotyczącego strategii w zakresie bezpieczeństwa, łącznie ze szczegółową oceną ryzyka w odniesieniu do świadczonych przez wnioskodawcę usług płatniczych, a także opisem środków kontroli bezpieczeństwa i ograniczania ryzyka podjętych w celu odpowiedniej ochrony użytkowników usług płatniczych przed zidentyfikowanymi ryzykami, w tym oszustwami i nielegalnym wykorzystywaniem danych szczególnie chronionych i danych osobowych (art. 5 ust. 1 lit. j dyrektywy PSD2). System zarządzania ryzykiem powinien być:

1/ zgodny z gotowością danego dostawcy usług płatniczych do podejmowania ryzyka;
2/ zawierać definicję oraz przydział kluczowych ról i obowiązków, jak również odpowiednich struktur raportowania niezbędnych do wdrożenia środków bezpieczeństwa oraz do zarządzania ryzykami dla bezpieczeństwa i ryzykami operacyjnymi;

---

15 EBA/GL/2017/17.

16 Dz.Urz. UE L nr 337, s. 35; dalej: dyrektywa PSD2.

3/ ustanawiać niezbędne procedury i systemy rozpoznawania, pomiaru i monitorowania różnych ryzyk wynikających z działalności dostawcy usług płatniczych związanej z płatnościami, na które to ryzyka narażony jest dostawca usług płatniczych, oraz procedury i systemy zarządzania takimi ryzykami, a także zawierać rozwiązania zapewniające ciągłość działania (pkt 2.2 Wytycznych EBA).

Przepisy ustawy o usługach płatniczych nakładają dodatkowo na dostawców usług płatniczych obowiązek corocznego przekazywania KNF lub innemu właściwemu organowi nadzoru rocznej informacji o ocenie i aktualizacji procedur w zakresie zarządzania ryzykiem operacyjnym i ryzykiem naruszenia bezpieczeństwa, a także ocenie środków ograniczających ryzyko oraz mechanizmów kontroli (zob. art. 32f ust. 2 u.p.u.; zob. również pkt 3.1 Wytycznych EBA)[17].

Wymienione powyżej regulacje mają kluczowe znaczenie w zanalizowanym zakresie, jednak uzupełniająco należy wymienić jeszcze kilka innych regulacji, które mają znaczenie w dziedzinie cyberbezpieczeństwa, w tym przede wszystkim: ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe[18], ustawa z dnia 6 czerwca 1997 r. – Kodeks karny[19], ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych[20], rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[21].

Należy jednocześnie zwrócić uwagę, że zagadnienia bezpieczeństwa świadczenia usług dotyczące banków regulują rekomendacje KNF[22].

---

[17] Zob. również M. Grabowski, *Ustawa o usługach płatniczych. Komentarz*, Warszawa 2020, art. 32f.

[18] T.j. Dz.U. z 2022 r. poz. 2324 z późn. zm.

[19] T.j. Dz.U. z 2022 r. poz. 1138 z późn. zm.

[20] T.j. Dz.U. z 2019 r. poz. 1781.

[21] Dz.Urz. UE L nr 127, s. 2.

[22] Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach (stanowiąca załącznik do uchwały nr 7/2013 Komisji Nadzoru Finansowego z dnia 8 stycznia 2013 r., Dz.Urz. KNF z 2013 r. poz. 5) oraz Rekomendacja M dotycząca zarządzania ryzykiem operacyjnym w bankach (stanowiąca załącznik do uchwały nr 8/2013 Komisji Nadzoru Finansowego z dnia 8 stycznia 2013 r.,

3. Definicja legalna cyberbezpieczeństwa

Termin „cyberbezpieczeństwo" funkcjonuje obecnie w wielu aktach prawnych zarówno krajowego porządku prawnego, jak również z regulacjach unijnych. Pojęcie to zostało zdefiniowane w ustawie o krajowym systemie cyberbezpieczeństwa, w której w procesie implementacji dyrektywy NIS wyszczególniono 19 definicji. Zgodnie z art. 2 pkt 4 k.s.c.u. cyberbezpieczeństwo oznacza odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Definicja ta odpowiada sformułowanej w dyrektywie NIS definicji bezpieczeństwa sieci i systemów informatycznych[23], zmieniono jednak jej zakres, ponieważ art. 2 pkt 4 k.s.c.u. nie wprowadza odniesienia do jednego z jej aspektów dotyczących „poziomu zaufania", nie wprowadzono również rozróżnienia usług na „dostępne" i „oferowane"[24].

Należy zwrócić uwagę, że definicja cyberbezpieczeństwa odnosi się do tzw. atrybutów bezpieczeństwa informacji – poufności, integralności, dostępności i autentyczności. Poufność oznacza w tym przypadku odniesienie do zasady, zgodnie z którą dostęp do informacji mają tylko osoby uprawnione. Integralność odnosi się do wymogu kompletności i poprawności informacji. Dostępność oznacza, że informacja jest dostępna na żądanie uprawnionej do tego osoby. Poza tymi trzema atrybutami bezpieczeństwa informacji (tzw. CIA – *confidentiality*, *integrity*, *availability*) zgodnie z zapisami objętymi przepisami dyrektywy

Dz.Urz. KNF z 2013 poz. 6). Zob. również P. Pelc, *op. cit.*, s. 138–139; M. Kasprzak, [w:] *Współczesny system bankowy. Ujęcie instytucjonalne*, red. J. Świderska, Warszawa 2013, s. 158 i n.

[23] Zgodnie z art. 4 pkt 2 dyrektywy NIS, „bezpieczeństwo sieci i systemów informatycznych" oznacza odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych lub przekazywanych, lub przetwarzanych danych lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne.

[24] Zob. G. Szpor, *Nowelizacja siatki pojęciowej cyberbezpieczeństwa*, „Monitor Prawniczy" 2020, nr 22, s. 1189 i n.; J. Dysarz, *op. cit.*, art. 2; F. Radoniewicz, [w:] *Ustawa o krajowym systemie bezpieczeństwa*…, art. 2, Nb 3.

NIS do definicji cyberbezpieczeństwa włączono również atrybut autentyczności, rozumiany jako gwarancje co do tożsamości podmiotu lub zasobu[25].

4. Aktywność instytucji publicznych

Kwestia bezpieczeństwa cyfrowego w bankowości, ale i funkcjonowaniu całego rynku finansowego jest traktowana w sposób szczególny i ze świadomością wysokiej szkodliwości występujących działań przestępczych. Banki ze względu na charakter swojej działalności oraz status instytucji zaufania publicznego obciążone są wieloma obowiązkami, których realizacja zapewnia bezpieczeństwo w analizowanym zakresie. Poddając analizie kwestię cyberbezpieczeństwa w sektorze bankowym, należy także pamiętać, że jego zapewnienie służy nie tylko klientom banków, ale również interesom ich samych. Podstawy regulacyjne są bardzo istotnym warunkiem zachowania bezpiecznego (pod względem cyfrowym) funkcjonowania rynku finansowego, jednak czynników warunkujących to bezpieczeństwo jest znacznie więcej i są zidentyfikowane m.in. w obszarze wymagań związanych z bieżącym monitorowaniem przestrzegania obowiązujących przepisów, warunków organizacyjnych i technicznych w działalności banków, a także działaniach edukacyjnych.

Decydująca jest w tym zakresie aktywność instytucji publicznych, których działalność dotyczy obszaru funkcjonowania banków oraz innych uczestników rynku finansowego. Jest ona widoczna w Polsce na wielu płaszczyznach – chociażby w samej strukturze organizacyjnej poszczególnych instytucji, która uwzględnia komórki organizacyjne specjalizujące się w kwestiach cyberbezpieczeństwa. Wymienić można w tym zakresie np. Departament Cyberbezpieczeństwa w strukturze Urzędu KNF, który podejmuje działania związane z zapewnieniem bezpieczeństwa w zakresie funkcjonowania samej instytucji, ale także realizuje zadania związane m.in. z opracowywaniem regulacji wewnętrznych, przygotowywaniem kryteriów oceny i procedur kontrolnych

[25] F. Radoniewicz, [w:] *Ustawa o krajowym systemie bezpieczeństwa…*, art. 2, Nb 3, 4; G. Szpor, *op. cit.*, s. 1191.

dotyczących podmiotów nadzorowanych oraz ich realizacją, opracowywaniem dobrych praktyk oraz rekomendacji dotyczących bezpieczeństwa informacji i środowiska teleinformatycznego – mających znaczenie z punktu widzenia funkcjonowania rynku finansowego. Departament Cyberbezpieczeństwa współpracuje również z organami państwa oraz instytucjami tworzącymi regulacje prawne, standardy i rekomendacje w zakresie ryzyka związanego z obszarami technologii informacyjnej i cyberbezpieczeństwa. Posiada również kompetencje w zakresie zlecania, nadzorowania oraz przeprowadzania audytów, a także zarządzania incydentami w obszarze cyberbezpieczeństwa. Zarządza też wybranymi systemami bezpieczeństwa teleinformatycznego. Aktywność Departamentu Cyberbezpieczeństwa dotyczy również mającego szczególne znaczenie procesu edukacji i przygotowywania kampanii edukacyjnych promujących wiedzę z zakresu cyberbezpieczeństwa[26].

Należy jednocześnie zwrócić uwagę, że w ostatnim czasie zagadnienie cyberbezpieczeństwa w sektorze finansowym jest jednym z zagadnień mocno akcentowanych w działalności Urzędu KNF. Dotyczy to m.in. działań związanych z podniesieniem poziomu bezpieczeństwa informacji przetwarzanych w chmurze, weryfikacją rekomendacji dotyczących zarządzania ryzykami IT na rynku finansowym oraz wprowadzeniem jednolitego modelu analitycznego ryzyka obszaru cyberbezpieczeństwa. Uwzględniono w tym zakresie także działania edukacyjne zwiększające świadomość zagrożeń związanych z cyberbezpieczeństwem[27]. Istotnym elementem aktywności instytucji nadzoru finansowego są wydawane rekomendacje – w miejscu tym przypomnieć należy chociażby rekomendację D dotyczącą zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach, która określa oczekiwania nadzorcze odnośnie do ostrożnego i stabilnego zarządzania w zakresie wymienionych obszarów funkcjonowania banków, w szczególności ryzykiem związanym z tymi obszarami.

---

[26] https://www.knf.gov.pl/o_nas/urzad_komisji/dane_teleadresowe_struktura?articleId=65223&p_id=18 (dostęp: 5.09.2022 r.).

[27] Komisja Nadzoru Finansowego, *Cyfrowa Agenda Nadzoru – plan działań Urzędu KNF w zakresie m.in. nowoczesnych technologii, innowacji oraz cyberbezpieczeństwa*, Warszawa 2019, *passim*.

Zgodnie z omówionymi powyżej przepisami ustawy o krajowym systemie cyberbezpieczeństwa Komisja Nadzoru Finansowego jest organem właściwym do spraw cyberbezpieczeństwa dla sektora bankowego i infrastruktury rynków finansowych (art. 41 pkt 4 k.s.c.u.), z czym związane są realizowane w tym zakresie zadania (zob. omówienie tej problematyki powyżej)[28].

Departament Cyberbezpieczeństwa funkcjonuje również w strukturze Narodowego Banku Polskiego. Realizuje on zadania związane z bieżącym monitorowaniem cyberzagrożeń oraz koordynowaniem obsługi cyberincydentów w systemach i infrastrukturze teleinformatycznej banku centralnego. Sprawując bieżący nadzór nad bezpieczeństwem systemów teleinformatycznych odpowiada jednocześnie za proces doskonalenia metod bieżącego monitorowania cyberbezpieczeństwa. Narodowy Bank Polski jako centralny bank państwa ma oczywiście swój istotny wpływ na kształt regulacji prawnych obowiązujących w analizowanym zakresie[29]. Szczególnie istotna pozostaje jego rola i instrumenty, jakimi dysponuje w realizowanym nadzorze systemowym[30]. Wskazać należy również szeroko realizowaną działalność edukacyjną.

Przepisy ustawy o krajowym systemie cyberbezpieczeństwa wymieniają NBP w grupie podmiotów publicznych odpowiedzialnych za poszczególne aspekty funkcjonowania tego systemu (zob. omówienie tej problematyki powyżej oraz art. 21–25 k.s.c.u.)[31].

Zwrócenia uwagi wymaga również aktywność Związku Banków Polskich, z inicjatywy którego powołany został Komitet Cyberbezpieczeństwa Banków ZBP oraz Zespół Bezpieczeństwa Banków ZBP (a w tym Bankowe Centrum Cyberbezpieczeństwa ZBP)[32], spełniające istotną rolę budowania współpracy samych banków w dziedzinie bezpieczeństwa cyfrowego. Związek Banków

---

[28] Zob. B. Biderman, K. Mroczka, *op. cit.*, s. 56–58; K. Walczuk, *op. cit.*, art. 41, 42; J. Dysarz, *op. cit.*, art. 41, 42.

[29] https://www.nbp.pl/home.aspx?f=/o_nbp/struktura/departamenty/cyberbezpieczenstwa.html (dostęp: 5.09.2022 r.).

[30] K. Dmowska, *Cyberbezpieczeństwo systemu płatniczego w nadzorze systemowym Narodowego Banku Polskiego*, „Bank i Kredyt" 2022, nr 53(4), *passim*.

[31] Zob. również P. Pelc, *op. cit.*, s. 132.

[32] https://www.zbp.pl/Dla-Bankow/Cyberbezpieczenstwo/Cyberbezpieczenstwo-bankow-i-ich-klientow (dostęp: 5.09.2022 r.).

Polskich podejmuje również działania edukacyjne zwiększające świadomość i wiedzę w zakresie bezpiecznego korzystania z bankowości internetowej.

5. Wnioski

Postępująca rewolucja cyfrowa dotyczy coraz to nowych dziedzin życia społecznego i gospodarczego, a wdrażanie rozwiązań, które niesie za sobą, stanowi warunek zachowania możliwości dalszego rozwoju oraz zachowania konkurencyjności różnych podmiotów. Zachodzące zmiany stały się również udziałem podmiotów rynku finansowego, w tym również banków, a rozwiązania cyfrowe stanowią współcześnie istotny element funkcjonowania całego sektora bankowego. Postępujący rozwój technologiczny w różnych obszarach funkcjonowania rynku finansowego, a także konieczność transformacji cyfrowej są dziś podstawą działań zmierzających do rozwoju tej sfery aktywności wszystkich instytucjonalnych uczestników rynku finansowego oraz wdrażających jednocześnie rozwiązania zapewniające bezpieczeństwo cyfrowe na poziomie rozwiązań organizacyjnych, a także bezpieczeństwo korzystania z oferowanych przez nie usług.

Rozwiązania cyfrowe – poza wymiarem istotnych korzyści płynących z ich wykorzystania w działalności sektora bankowego – niosą za sobą istotne zagrożenia związane z występowaniem nasilających się działań przestępczych. Ostatnie lata pokazują nie tylko narastające zjawisko cyberprzestępczości, obserwujemy również zmieniające się formy ataków, których skutki ocenia się jako coraz bardziej zagrażające bezpieczeństwu funkcjonowania sektora finansowego (w tym bankowego) oraz bezpieczeństwu oferowanych usług.

Zagwarantowanie bezpieczeństwa cyfrowego należy rozpatrywać na wielu płaszczyznach. Jedną z pierwszych jest stworzenie podstaw regulacyjnych wprowadzających procedury ostrożnościowe, zasady postępowania w przypadku wystąpienia działań przestępczych i określające kompetencje instytucji, których działalność jest poddana aktywności cyberprzestępców oraz tych, które realizują w odniesieniu do rynku finansowego określone funkcje nadzorcze. Ostatnie lata pokazują, że wiele w tym zakresie zmienia się również w odniesieniu do

regulacji krajowych. W przypadku sektora bankowego szczególne znaczenie ma omówiona powyżej ustawa o krajowym systemie cyberbezpieczeństwa oraz ustawa o usługach płatniczych. Niniejsze opracowanie skupiono przede wszystkim na rozwiązaniach krajowych, natomiast należy zwrócić uwagę na fakt, iż zmiany w prawie krajowym dotyczące analizowanej problematyki często mają podstawę w implementowanych przepisach unijnych. Działania podejmowane w tym zakresie mają na celu osiągnięcie stanu pewności regulacyjnej, istotnej przede wszystkim z punktu widzenia nieprofesjonalnych uczestników rynku finansowego. Istotny udział w procesie budowania struktur bezpiecznego korzystania z rozwiązań cyfrowych mają również instytucje realizujące określone funkcje w krajowym systemie cyberbezpieczeństwa, chociaż ich aktywność w tym zakresie wykracza zdecydowane poza ramy wyłącznie przepisów u.k.s.c.

Poza zakresem niniejszego opracowania są normy i standardy technologiczne związane ze stosowaniem rozwiązań cyfrowych, jednak konieczne jest zwrócenie uwagi również na ten istotny aspekt bezpieczeństwa cyfrowego. Ważnym elementem cyberbezpieczeństwa jest również edukacja, wzrost świadomości istniejących zagrożeń oraz wskazywanie wzorców bezpiecznego korzystania z usług bankowych. Działania edukacyjne są przedmiotem aktywności zarówno banków, jak również właściwych instytucji publicznych.

Stworzenie kompleksowych podstaw regulacyjnych w połączeniu z wdrażaniem najnowszych rozwiązań technologicznych ma również znaczenie dla bezpieczeństwa sektora finansowego (w tym bankowego), a co za tym idzie ważnej kwestii zaufania klientów do banków i innych instytucji finansowych. Stworzenie silnych podstaw bezpieczeństwa stanowi jednocześnie istotny element zapobiegający i mający wpływ na skalę występujących naruszeń.

Bibliografia

Besiekierska A. (red.), *Ustawa o krajowym systemie bezpieczeństwa. Komentarz*, Warszawa 2019.

Besiekerska A., *Ustawa o krajowym systemie cyberbezpieczeństwa. Wybrane obowiązki jednostek sektora finansów publicznych i spółek prawa handlowego wykonujących zadania o charakterze użyteczności publicznej*, „Informacja w Administracji Publicznej" 2019, nr 1.

Biderman B., Mroczka K., *Uwarunkowania prawne nadzoru nad cyberbezpieczeństwem rynku finansowego w Polsce*, „Bezpieczny Bank" 2022, nr 2(87).

Czarnecka A., *Wybrane obowiązki operatorów usług kluczowych na gruncie ustawy o krajowym systemie cyberbezpieczeństwa*, „Informacja w Administracji Publicznej" 2019, nr 2.

Dmowska K., *Cyberbezpieczeństwo systemu płatniczego w nadzorze systemowym Narodowego Banku Polskiego*, „Bank i Kredyt" 2022, nr 53(4).

Dygnatowski S., Dygnatowski W., *Prawne podstawy cyberbezpieczeństwa na tle polskiego i europejskiego ustawodawstwa*, „Journal of KONBiN" 2020, vol. 50, Issue 4.

Gawkowski K., *Bezpieczeństwo cyberprzestrzeni w regulacjach UE*, „Teka of Political Science and International Relations" 2018, vol. 13, no 2.

Grabowski M., *Ustawa o usługach płatniczych. Komentarz*, Warszawa 2020.

Kitler W., Taczkowska-Olszewska J., Radoniewicz F., *Ustawa o krajowym systemie bezpieczeństwa. Komentarz*, Warszawa 2019.

Komisja Nadzoru Finansowego, *Cyfrowa Agenda Nadzoru – plan działań Urzędu KNF w zakresie m.in. nowoczesnych technologii, innowacji oraz cyberbezpieczeństwa*, Warszawa 2019.

Pelc P., *Wybrane regulacje dotyczące cyberbezpieczeństwa instytucji finansowych*, „Cybersecurity and Law" 2021, vol. 6.

Szpor G., *Nowelizacja siatki pojęciowej cyberbezpieczeństwa*, „Monitor Prawniczy" 2020, nr 22.

Świderska J. (red.), *Współczesny system bankowy. Ujęcie instytucjonalne*, Warszawa 2013.

Wajda P., *Cyberbezpieczeństwo – sektorowe aspekty regulacyjne*, „IKAR" 2020, nr 2.

László Dornfeld

Cybercrime prevention through Cybersecurity in Hungary

1. Introduction

The literature on crime prevention has expanded considerably over the last century and has become one of the most researched areas of criminology. Several different trends have emerged in the traditional crime prevention field, with a focus on intervention using different instruments within and outside the criminal policy[1]. Despite this, the novelty and characteristics of cybercrime also pose a challenge to established crime prevention structures. Among them, we can mention the increasing number and decreasing price of devices capable of online connection, which significantly increase the number of potential perpetrators and victims; the greater tendency of people to act deviant online; the possibility of anonymity and hiding traces on the part of the offender; law enforcement problems arising from transnational crime and the rapid development of perpetration techniques[2].

Hungary has adopted a great number of legal provisions, policies, documents, and programs in order to help the prevention of cybercrimes, ranging across many different legal areas, from criminal law to administrative law. Especially the latter most closely follow the various regulations of the European Union and often build additional provisions upon this foundation. Some of these are

[1] A. Borbíró, *Kriminálpolitika és bűnmegelőzés a késő-modernitásban*, PhD Thesis, Budapest 2011, *passim*.

[2] UNODC, *Comprehensive Study on Cybercrime*, 2013, https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (access: 15.08.2022).

aimed at building resilience and strong cybersecurity, while others are aimed at potential victims to help them identify and avoid victimization.

Given the space constraints of this chapter, none of these will be addressed much in detail, rather than that, this chapter mostly aims to give a general overview of the relevant Hungarian legislation and policy, presenting the system as a whole.

2. Strategies and programs

The strategies are important in every legal system, as they are the foundation of this where the operational and strategic priorities are set, which can then be used as the basis for normative legislation. They can also serve as a basic document for law enforcement and judicial bodies to develop their own internal procedures. Strategies usually address a multitude of issues, such as cybercrime prevention and awareness raising, law enforcement and criminal justice capacity, public-private partnerships, legislation, and international cooperation[3].

In the case of Hungary, many different strategies were adopted in the past decade. The National Security Strategy of Hungary should be highlighted[4], which was adopted in 2020 to replace the previous strategy, in use for the previous 8 years. In this document, the safety of cyberspace is present as a security concern for Hungary. The document ranks cyberattacks causing significant damage against "government IT systems, e-government, utilities, strategic enterprises, other critical infrastructure and other computer networks of organizations important to the functioning of society" at number four on the list of security risks[5]. The strategy proposes two main ways of approaching the problem: intensive research and development on the one hand, and the development of defense capabilities on the other[6].

---

[3] UNODC, *Comprehensive Study on Cybercrime*, p. 228.

[4] Government Decree 1163/2020 (21.IV.) on the National Security Strategy of Hungary.

[5] Government Decree 1163/2020, point 124.d.

[6] T. Csiki Varga, P. Tálas, *Magyarország új nemzeti biztonsági stratégiájáról*, „Nemzet és Biztonság" 2020, vol. 3, *passim*.

Another important strategy was adopted in 2019, titled the Network and Information Systems Security Strategy of Hungary[7] which replaced the previous strategy from 2013. The document aims "to create a free, secure and innovative cyberspace, to increase Hungary's competitiveness, to introduce and adapt innovations and new technological solutions securely in the digitalized areas of public administration, government, and economy, to create a more secure electronic public administration system and to develop innovative public services, as well as to increase cybersecurity, awareness, and preparedness in all areas of society". The document builds on the previous strategy extensively, while identifying new threats, such as large-scale cyberattacks, hacktivism[8] , and the fact that Hungary is lagging behind the EU in preparedness, as only 9% of small and medium-sized enterprises have a dedicated information security policy, while for large Hungarian companies the figure is 53%. According to the National Bank of Hungary (MNB), in 2016 financial institutions incurred HUF 1,3 billion HUF in losses from electronic payment fraud[9].

The document highlights the National Cybersecurity Coordination Council, as the government's proposing and consultation body that coordinates cybersecurity in Hungary. Other than that, there are a number of CERTs and CSIRTs in Hungary (including GovCERT as part of the National Cyber Security Center [NCSC][10]) and other administrative bodies, the most important of which is the aforementioned NCSC[11].

Lastly, the Digital Strategy for Child Protection of Hungary[12] should be explored, which aims to create secure cyberspace for children. The document first sets out the essentials of digital child protection, such as the identification

---

[7] Government Decree 1838/2018 (28.XII.)

[8] Ideologically motivated attacks in the cyberspace to achieve an ideological goal or to convey an ideology. See B. Simon, *Hacktivism and its status in Hungary*, „Magyar Rendészet" 2016, vol. 2, *passim*.

[9] B. Gyömbér, *Megjelent Magyarország hálózati és információbiztonsági stratégiája*, Jogalappal, 2019, https://jogalappal.hu/megjelent-magyarorszag-halozati-es-informaciobiztonsagi-strategiaja/ (access: 15.08.2022).

[10] https://nki.gov.hu/ (access: 15.08.2022).

[11] For more information on these, see Z. Kovács, *Kibervédelem és biztonság*, [in:] Kibervédelem a bűnügyi tudományokban, ed. T. Kiss, Budapest 2020.

[12] Government Decree 2012/2015 (29.XII.)

of harmful content and behavior, the state of education, and the roles, and experiences of those involved. The second chapter reviews protection solutions (such as filtering software) and children's rights. In the third chapter, tools for sanctions and assistance are formulated. The last major part of the strategy sets out the objectives and instruments.

While strategies mainly focus on abstract-level problems and challenges, programs are on an operational level, aimed at specific issues. To give an example: nineteen Member States submitted a plan for the 2015 European Crime Prevention Award. The main theme was children and the internet. One of these was the TABBY (Threat Assessment of Bullying Behavior among Youth) in Internet study, which looked at the prevalence of bullying in schools and online in five countries (Bulgaria, Cyprus, Greece, Hungary, and Italy) from 2011–2012. The national program consisted of four consecutive modules: training of teachers and students in recognizing and dealing with online bullying, a first-panel survey, sensitization sessions, and finally a second-panel survey. The results of the research themselves reveal a lot about the phenomenon under study and can be used in practice for the development of future crime prevention and deviance treatment programs in schools. Although the program itself did not have an impact on offenders, the exposure of victims to abuse was significantly reduced[13].

3. Public administration

The most integral part of cybersecurity is administrative law, as it is the public administration that carries out laws and government policies and creates a more secure cyberspace as a result. The legal framework for the protection of cyberspace in Hungary is primarily determined by the relevant legislation of the European Union, which it fully complies with. It goes however well beyond the areas covered by it. Cybersecurity is closely tied to crime prevention as it ensures that systems have a high standard for protection and after handling

[13] K. Parti, *Az iskolai online bántalmazás felmérése és komplex kezelése a TABBY in Internet nemzetközi program keretében*, „Infokommunikáció és Jog" 2012, vol. 9, *passim*.

security incidents, the information regarding them is forwarded to the relevant law enforcement agency.

In the context of the protection of governmental systems, the most relevant legislation is the Act on the electronic information security of state and local government bodies[14], which was adopted in line with the National Cyber Security Strategy at that time[15]. Article 5 of the Act establishes the integrity and availability of the electronic information system and the confidentiality, integrity, and availability (the so-called CIA triad)[16] of data and information handled in the electronic information system as a fundamental requirement for information security. Under Article 6, to ensure this, an organization must establish logical, physical, and administrative safeguards as required by specific legislation. There are two important obligations in the law: on the one hand, the classification of information systems into different classes based on their security needs, and, on the other hand, the classification of the departments dealing with them into different security levels.

Directive 2016/1148 of the European Union was adapted to several different Hungarian laws, including the Act on certain aspects of electronic commerce services and information society services[17], and also in some respect the aforementioned Act on electronic information security. The former contains the provisions on digital service providers (service providers subject to notification in Hungarian terminology), while the latter addresses the essential service providers, who are subject to much stricter rules regarding cybersecurity. Another important aspect of the essential service providers is the Act on Critical Infrastructure[18], which is partly based on the previous EU legislation regarding critical infrastructure. Under the current regime, an operator of a national critical system can be designated as an essential service provider in an administrative procedure, if:

---

[14] Act L of 2013.

[15] G. Berki, *A kibertér, annak veszélyei és a kibervédelem jelenlegi helyzete Magyarországon*, „Nemzetbiztonsági Szemle" 2018, vol. 3, p. 15.

[16] S. Samonas, D. Coss, *The CIA strikes back: Redefining confidentiality, integrity and availability in security*, „Journal of Information System Security" 2013, vol. 3, *passim*.

[17] Act CVIII of 2001.

[18] Act CLXVI of 2012.

1/ provides a service falling within one of the sectors and subsectors listed in Annex II to the NIS Directive,
2/ its service depends on electronic information systems,
3/ and a security incident affecting its service would cause significant disruption to the service it provides.

There is also a possibility to designated non-critical system operators as an essential service providers, based on their own assessment, which is then reviewed by the competent authority. Given the high-security standards for critical system operators, service providers/institutions that are designated as essential service providers will not incur any additional duties to comply with security requirements[19].

Digital service providers must comply less strict rules, the measure they must use is usually not so directly provided for in the legal texts. They must take the necessary measures to prevent the likelihood of incidents occurring on the network and information systems they use and to manage and mitigate the impact of incidents that do occur. A separate government decree calls out for various measures and the relevant authority has the ability to audit the compliance with these rules and it can impose fines on non-compliance. Hungary has developed a stricter regulation than the NIS Directive when during the implementation it requires by Decree that providers of notifiable services must register with the authority designated by the Decree, which keeps a register of registered digital service providers[20].

Other rules for certain providers can be found, which must importantly incorporate the aspect of technological crime prevention. The use of technology for crime prevention is not a new idea, and its application in the field of cybercrime prevention has also emerged quickly. The theoretical basis for this is closely linked to situational crime prevention, which is the idea that crime can be reduced by making it harder to commit crimes, reducing the expected benefits, or increasing the risk of the offender. Two different models emerged over time:

---

[19] T. Bonnyai *et al.*, *Kritikus információs infrastruktúrák védelme*, Budapest 2019, p. 17–19.
[20] *Ibidem*, p. 21.

1/ decriminalization of systems is based on the idea that the possibility of unlawful use of the system should also be eliminated;
2/ building crime prevention into the system, such as the use of passwords to access certain systems.

One such method in Hungary was part of a larger legislative effort for strengthening anti-terrorism after the Brussels terror attacks in 2016. A part of the proposal was to prohibit encrypted communications devices where the authority cannot exercise its right of access (for example Apple phones have so strong defense that not even the manufacturer can access the information stored, even if complied by authorities). This was however met with severe criticism, as many pointed out that the protection of users is also reduced if the state restricts their access to such tools. It was soon clarified that this is only a restriction for certain applications and not meant for a hardware level[21]. The final legislation was much less severe, as it no longer required encryption service providers to provide information on the content of communication to authorities (which would have been an impossible task if the application uses end-to-end encryption), they are only required to provide the metadata of communication (such as the participants, time and location of the communication)[22].

4. Data retention and content filtering

Both instruments in this section derive from EU law. Content filtering means filtering out and then removing or otherwise making inaccessible various types of unlawful content. Three levels of filtering can be distinguished: the primary level is the user, where the level of filtering is set by the computer user or the institution operating the computer; the second level is the filtering applied by the ISP, and the third level is the blocking of content imposed by the state[23].

[21] Bitport, *A titkosítás tiltása veszélyes*, 2016, https://bitport.hu/a-titkositas-tiltasa-veszelyes (access: 15.08.2022).

[22] Government Decree 185/2016. (13.VII.)

[23] K. Parti, L. Marin, *Foltvarrással az on-line illegális tartalom ellen*, „Infokommunikáció és Jog" 2012, vol. 49, p. 58.

Article 149/A of the Act on electronic communications[24] requires Internet access service providers to make available free of charge the downloading of software in Hungarian that enables the protection of minors and is easy to install and use.

One of the foundations of content filtering at the third level is the European Union's Directive 2011/93/EU, Article 25 of which, entitled "Measures against websites containing or disseminating child pornography", imposes an obligation on the Member States to remove or block access to such websites. The transposition of this into domestic law has been done through the permanent inaccessibility of electronic data under Article 77 of the Criminal Code as a measure and the temporary inaccessibility of electronic data under Article 335 of the Code of Criminal Procedure as a coercive measure. This is however not widely used, as evidenced by the electronic register, which contains all use of this measure, having zero entries years after its introduction to the Hungarian legal system[25].

Instead, this instrument has been used for purposes radically different from its original purpose, by other legislations, and is used in cases such as blocking sites that organize illegal gambling and those selling counterfeit or unauthorized medicines. Although these are also important concerns, the use of the instrument in question exceeds the objective pursued. It is for this reason that, from the very beginning of the legal instrument until today, critical voices questioning its necessity have been predominant, as confirmed by practice (or rather the lack of it)[26].

The other instrument we should mention is data retention which was by Directive 2006/24/EC of the EU and was implemented into Hungarian law subsequently. This required communications service providers to specify which data they must retain. The stated aim was to make it available for the investigation, detection, and prosecution of serious crimes. Under Article 5,

[24] Act C of 2003.

[25] B. Gyömbér, *Így működik az állami internetcenzúra Magyarországon*, 2017, https://jogalappal.hu/igy_mukodik_az_internetcenzura_magyarorszagon/ (acess: 15.08.2022).

[26] See for example: Zs. Detrekői, *Blokkolás Magyarországon – hogyan jutottunk el a gyermekpornográfia elleni küzdelemtől a szerencsejáték-oldalak blokkolásáig*, „Infokommunikáció és Jog" 2014, vol. 60, p. 185–187.

the obligation applied to data relating to communications characteristics and subscriber data, but not to content data. It set the period for which the provider could be required to retain the data at between 6 and 24 months from the date of communication and provided that the data must be transmitted to the competent authorities without delay upon request.

In the Digital Rights Ireland and Seitlinger cases (C 293/12 and C 594/12), the Court of Justice of the European Union ruled on 8 April 2014 that the Directive was invalid because it infringed Articles 7 (right to privacy) and 8 (right to the protection of personal data) of the Charter of Fundamental Rights of the European Union and the requirement of proportionality. Prior to this, in certain Member States, the national Constitutional Court has already ruled these provisions unconstitutional, including Czechia, Germany, and Romania. After the CJEU's decision, an odd legal situation has arisen, as data retention has been retained in the Member States' legal systems, which have subsequently become highly fragmented. In the years that followed, the EU did not create new legislation on the issue.

This was the case in Hungary as well, as the provisions in question remained in force until July of 2022, when the Constitutional Court ruled them unconstitutional, as it infringes the right to respect for private life and the right to protection of personal data set out in the Fundamental Law of Hungary[27]. Now the Constitutional Court has ruled that there is a breach of the Constitution: the purpose for which data can be requested should be much more clearly defined, and only with the permission of a judge or other independent body. While many people welcomed this decision, also based on the relevant CJEU ruling, many also expressed their dissatisfaction as to why it had taken so many years to be announced, especially given how the decision puts heavy emphasis on its effect on millions of citizens. It was also met with confusion that while the Constitutional Court found an unconstitutional omission and called on the Parliament to clarify the matter but it did not annul the provisions of the law that violated the fundamental rights.

[27] Constitutional Court Decision 5/2022 (14.VII.)

Bibliography

Berki G., *A kibertér, annak veszélyei és a kibervédelem jelenlegi helyzete Magyarországon*, „Nemzetbiztonsági Szemle" 2018, vol. 3.

Bonnyai T. *et al.*, *Kritikus információs infrastruktúrák védelme*, Budapest 2019.

Csiki Varga T., Tálas P., Magyarország új nemzeti biztonsági stratégiájáról, „Nemzet és Biztonság" 2020, vol. 3.

Detrekői Zs., *Blokkolás Magyarországon – hogyan jutottunk el a gyermekpornográfia elleni küzdelemtől a szerencsejáték-oldalak blokkolásáig*, „Infokommunikáció és Jog" 2014, vol. 60.

Gyömbér B., *Így működik az állami internetcenzúra Magyarországon*, 2017, https://jogalappal.hu/igy_mukodik_az_internetcenzura_magyarorszagon/ (access: 15.08.2022).

Gyömbér B., *Megjelent Magyarország hálózati és információbiztonsági stratégiája*, Jogalappal, 2019, https://jogalappal.hu/megjelent-magyarorszag-halozati-es-informaciobiztonsagi-strategiaja/ (access: 15.08.2022).

Kovács Z., *Kibervédelem és biztonság*, [in:] *Kibervédelem a bűnügyi tudományokban*, ed. T. Kiss, Budapest 2020.

Parti K., *Az iskolai online bántalmazás felmérése és komplex kezelése a TABBY in Internet nemzetközi program keretében*, „Infokommunikáció és Jog" 2012, vol. 9.

Parti K., Marin L., *Foltvarrással az on-line illegális tartalom ellen*, „Infokommunikáció és Jog" 2012, vol. 49.

Samonas S., Coss D., *The CIA strikes back: Redefining confidentiality, integrity and availability in security*, „Journal of Information System Security" 2013, vol. 3.

Simon B., *Hacktivism and its status in Hungary*, „Magyar Rendészet" 2016, vol. 2.

UNODC, *Comprehensive Study on Cybercrime*, 2013.

Tomasz Bojanowski

Rola i zadania wybranych służb specjalnych w zwalczaniu i przeciwdziałaniu cyberprzestępczości

1. Wprowadzenie

Przedmiotem niniejszego artykułu będzie analiza pozycji i zadań wybranych służb specjalnych w zakresie zwalczania i przeciwdziałania cyberprzestępczości. Celem rozważań jest wykazanie istoty i doniosłości działalności służb specjalnych w omawianym zakresie oraz wskazanie na konieczność zmian w systemie funkcjonowania służb specjalnych, które będą miały pozytywny wpływ na zwalczanie i przeciwdziałanie cyberprzestępczości. Asumptem do przedmiotowych analiz będzie omówienie pojęcia „cyberprzestrzeni"[1] i „cyberprzestępczości"[2],

[1] Por. J. Worona, *Regulacje bezpośrednio odnoszące się do cyberprzestrzeni*, [w:] *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*, Warszawa 2020, *passim*; Ł. Goździaszek, *Cyberprzestrzeń spółek handlowych w kontekście prawnych problemów komunikacji elektronicznej*, „Przegląd Prawa Handlowego" 2009, nr 11, s. 29–36; M. Rojszczak, *Cyberprzestrzeń jako nowa płaszczyzna budowania relacji społecznych*, [w:] *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*, Warszawa 2019, *passim*; R. Lipniewicz, *Pojęcie i natura cyberprzestrzeni*, [w:] *Jurysdykcja podatkowa w cyberprzestrzeni*, Warszawa 2018, *passim*; M. Berdel-Dudzińska, *Pojęcie cyberprzestrzeni we współczesnym polskim porządku prawnym*, „Przegląd Prawa Handlowego" 2012, nr 2, s. 19–38; M. Wilbrandt-Gotowicz, [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. K. Czaplicki, A. Gryszczyńska, G. Szpor, Warszawa 2019, art. 78; W.Z. Dziomdziora, *Cyberbezpieczeństwo w samorządzie terytorialnym. Praktyczny przewodnik*, Warszawa 2021, *passim*.

[2] Por. C. Banasiński, M. Rojszczak, J.M. Chmielewski, W. Hydzik, J. Łuczak, W. Nowak, K. Waćkowski, *Zarządzanie incydentami a ustawa o krajowym systemie cyberbezpieczeństwa*, [w:] C. Banasiński i in., *Cyberbezpieczeństwo*, Warszawa 2020, *passim*; J. Worona, *Regulacje pośrednio odnoszące się do cyberprzestrzeni*, [w:] *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*, Warszawa 2020; C. Zielińska, *Pojęcie cyberprzestępczości*, [w:] *Przestępczość XXI wieku. Szanse i wyzwania dla kryminologii*, red. D. Dajnowicz-Piesiecka, E. Jurgielewicz-Delegacz, E.W. Pływaczewski, Warszawa 2020, *passim*; P. Zakrzewski, *Streszczenie*, [w:] *Kradzież z włamaniem*, red. M. Mozgawa, Warszawa 2021, *passim*; P. Lewulis,

które będą swoistym wprowadzeniem do wskazanej tematyki. Następnie autor nakreśli instytucjonalne ramy systemu przeciwdziałania i zwalczania cyberprzestępczości, ze wskazaniem szczególnej roli służb specjalnych, co pozwoli na szersze osadzenie tematu w realiach prawnych. Autor wskaże wybrane zadania i uprawnienia służb w aktualnym stanie prawnym stanu prawnego oraz przedstawi propozycje *de lege ferenda*, które mogą usprawnić działalność służb oraz zwiększyć poziom bezpieczeństwa obywateli w cyberprzestrzeni. W związku z tym naturalnym wydaje się wykorzystanie metody typowej dla nauk prawnych, tj. formalno-dogmatycznej przy analizie przedmiotowego problemu[3]. Omawiane zagadnienie jest niezwykle istotne nie tylko z punktu widzenia nauk prawnych, ale także w ujęciu interdyscyplinarnym[4]. Cyberprzestrzeń to obszar, w którym każdy człowiek musi potrafić się odnaleźć. Do niedawna taka sytuacja wydawała się abstrakcyjna, ale powszechna cyfryzacja i informatyzacja sprawiła, że korzystanie z podstawowych praw i wolności oraz usług publicznych jest uzależnione od obecności w cyberprzestrzeni. Niniejsze procesy zdecydowanie przyśpieszyły z uwagi na pandemię koronawirusa COVID-19[5] i wprowadzony *lockdown*, który jeszcze bardziej uzależnił ludzi

---

O rozgraniczeniu definicyjnym pomiędzy przestępczością „cyber" i „komputerową" dla celów praktycznych i badawczych, „Prokuratura i Prawo" 2021, nr 3, s. 12–32; K. Mamak, *Uwagi wprowadzające*, [w:] *Rewolucja cyfrowa a prawo karne*, Kraków 2019, *passim*; A. Choroszewska, P. Opitek, *Uzyskiwanie dowodów cyfrowych z zagranicy w sprawach karnych – stan obecny i procedowane zmiany, cz. II*, „Prokuratura i Prawo" 2020, nr 10–11, s. 194–226; J. Kosiński, *Paradygmaty cyberprzestępczości*, Warszawa 2015, *passim*.

[3] L. Nowak, *Metodologiczne kryterium demarkacji i problem statusu teologii*, „Nauka" 2004, nr 3, s. 129–130.

[4] Por. K. Doktorowicz, *Europejski model społeczeństwa informacyjnego. Polityczna strategia Unii Europejskiej w kontekście globalnych problemów wieku informacji*, Katowice 2005, s. 23, cyt. za: A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2010, s. 25; M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni, zagrożenia i wyzwania dla Polski – zarys problemu*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego" 2014, nr 2(926), *passim*. Por. J. Łaszczyk (red.), *Komputer w kształceniu specjalnym: wybrane zagadnienia*, Warszawa 1998, *passim*; J. Łaszczyk M. Jabłonowska (red.), *Uczeń zdolny wyzwaniem dla współczesnej edukacji*, Warszawa 2008, *passim*; J. Bednarek, *Społeczeństwo informacyjne i media w opinii osób niepełnosprawnych*, Warszawa 2005, *passim*; M. Siwicki, *Cyberprzestępczość*, Warszawa 2013, s. 9–15.

[5] M. Paszkowska, *Kwarantanna i izolacja w związku z COVID-19 w świetle nowych przepisów*, LEX/el. 2020; *eadem*, *Instrumenty przymusu stosowane wobec osób podejrzanych oraz chorych na choroby zakaźne* (*w tym COVID-19*), LEX/el. 2020; P. Ostaszewski, J. Klimczak,

od dostępu do cyberprzestrzeni. W tym miejscu należy wskazać, że omawiane procesy są z jednej strony korzystne, ponieważ zwiększają dostępność do usług publicznych oraz organów administracji, a co najważniejsze ułatwiają życie ludzi na różnych płaszczyznach. Cyfryzacja i informatyzacja postępują zarówno na płaszczyźnie prywatnej jak i publicznej i nie wydaje się, aby ten trend miałby się odwrócić. Pomimo zalet i korzyści płynących z wskazanych zmian trzeba podkreślić, że niosą one za sobą ogromne zagrożenia[6]. W związku z powszechnym dostępem do Internetu coraz częściej popełniane są cyberprzestępstwa. Co więcej, ustawodawca musi stale reagować rozwój tej gałęzi przestępczości zarówno w wymiarze materialnoprawnym, jak i formalnoprawnym. W przypadku prawa materialnego reakcją ustawodawcy jest typizowanie nowych zachowań oraz zaostrzanie kar w Kodeksie karnym[7]. Aspekt formalno-prawny jest zdecydowanie bardziej złożony. Ustawodawca po pierwsze musi zapewnić organom możliwość realizacji ich ustawowych uprawnień w cyberprzestrzeni, poprzez wyposażenie ich w odpowiednie kompetencje wynikające wprost z przepisów prawa, co powinien określać Kodeks postępowania karnego[8] i ustawy szczególne. Co więcej, istotne jest, aby praca wykonana przez wskazane organy i zebrany przez nie materiał dowodowy mógł być wykorzystany przez organy procesowe tj. sądy i prokuraturę na potrzeby ewentualnego procesu karnego[9]. Jednocześnie ustawodawca musi pamiętać o normatywnie zagwarantowanych prawach człowieka, które nie mogą być naruszone w toku podejmowanych czynności. Tylko tak skonstruowany system przeciwdziałania i zwalczania cyberprzestępczości można uznać za prawidłowy. Należy wskazać, że rozważania i postulaty

J. Włodarczyk-Madejska, *Przestępczość i wymiar sprawiedliwości w pierwszym roku pandemii COVID-19*; Warszawa 2021, *passim*; K. Dobrzeniecki, B. Przywora, *Ograniczenia praw i wolności w okresie pandemii COVID-19 na tle porównawczym. Pierwsze doświadczenia*, Warszawa 2021, *passim*.

[6] M. Grewiński, *Cyfryzacja i innowacje społeczne – perspektywy i zagrożenia dla społeczeństwa*, https://econjournals.sgh.waw.pl/KNoP/article/download/1265/1117/ (dostęp: 31.10.2021 r.).

[7] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. Dz.U. z 2022 r. poz. 1138, z późn. zm.).

[8] Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (t.j. Dz.U. z 2022 r., poz. 1375, z późn. zm.).

[9] B. Oręziak, *Cyberprzestępczość w aspektach proceduralnych. Dowody elektroniczne a nowoczesne formy przestępczości*, Warszawa 2019, s. 85–120.

teoretyczne mogą się mijać z realiami praktyki i punktem widzenia praktyków[10]. Dlatego wskazany temat opracowania jest niezwykle istotny i delikatny. W celu wypracowania gotowych rozwiązań prawnych konieczne jest przeanalizowanie zagadnienia w sposób kompleksowy i interdyscyplinarny oraz skonfrontowanie rezultatów na szerszym forum akademickim.

2. Pojęcie „cyberprzestrzeni"

„Cyberprzestrzeń" w doktrynie prawniczej jest definiowana w sposób szeroki i na wiele sposobów[11]. Wynikają z tego zarówno pozytywy oraz negatywy, które rzutują na rozwój tego zjawiska. Należy wskazać, że definiowanie „cyberprzestrzeni" jest zależne od wielu zmiennych, mogą to być m.in.:

1/ okres, w którym wprowadza się daną definicję;
2/ system prawny, na podstawie którego wyprowadzana jest definicja;
3/ aktualny stopień rozwoju technologicznego;
4/ czy też nawet osobisty stosunek autora definicji to zjawiska cyberprzestrzeni.

W tym miejscu należy wskazać, że świat już od prawie 40 lat na rozmaite sposoby stara się właściwie zdefiniować „cyberprzestrzeń"; jako pierwszy dokonał tego Wiliam Gibson, autor książek science-fiction[12]. Nie ma potrzeby przytaczania jego definicji, ponieważ została ona stworzona na potrzeby pracy pisarskiej,

[10] A. Lach, *Dowody cyfrowe w postępowaniu karnym, wybrane zagadnienia praktyczne i teoretyczne*, http://www.bibliotekacyfrowa.pl/Content/24720 (dostęp: 31.10.2021 r.).

[11] Por. J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9, s. 225–234; T. Aleksandrowicz, *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, nr 15, s. 11–12; M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – Zarys problemu*, „Bezpieczeństwo Narodowe" 2012, nr 22, s. 125–139; A. Nowak, *Cyberprzestrzeń jako nowa jakość zagrożeń*, „Zeszyty Naukowe Akademii Obrony Narodowej" 2013, nr 3, s. 5–46; J. Kulesza, *Międzynarodowe prawo Internetu*, Poznań 2010, s. 57; J. Bednarek, A. Andrzejewska, *Cyberświat – możliwości i zagrożenia*, Warszawa 2009, s. 29–32; H. Babis, *Internet*, [w:] *Encyklopedia zagadnień międzynarodowych*, red. E. Cała-Wacinkiewicz, R. Podgórzański, Warszawa 2011, s. 540–541.

[12] Określał cyberprzestrzeń jako „konsensualną halucynację doświadczaną każdego dnia przez miliardy użytkowników na świecie", W. Gibson, *Neuromancer*, Katowice 2009, s. 59.

a nie nauk prawnych. Dlatego wykładnia pojęcia „cyberprzestrzeni" powinna zostać oparta wyłącznie na literaturze prawniczej[13]. Warto skupić się także na językowym aspekcie tego zagadnienia. Cyberprzestrzeń jak sama nazwa wskazuje (ang. *cyberspace*) to przestrzeń lub płaszczyzna, określana mianem wirtualnej, cyfrowej lub niematerialnej[14]. Składają się na nią wielopłaszczyznowe, wielopoziomowe i wielowarstwowe powiązania o podłożu cyfrowym[15]. Istotny jest fakt, że cyberprzestrzeń oparta jest na specjalistycznej infrastrukturze[16]. W związku z tym cyberprzestrzeń można określić mianem sieci, za pomocą której możliwa jest komunikacja pomiędzy systemami komputerowymi, obejmującymi jednostki centralne oraz ich oprogramowanie oraz dane, a także sposoby i środki przesyłu tych danych[17]. Według takiego ujęcia cyberprzestrzeń jest kojarzona przede wszystkim z siecią Internet, która jest często uznawana za synonim cyberprzestrzeni. Niemniej cyberprzestrzeń to pojęcie szersze, które może, lecz nie musi obejmować także systemy: informacyjne, telekomunikacyjne, teleinformatyczne, energetyczne, łączności, wodociągowe, przesyłu paliw kopalnych itd. Istotą cyberprzestrzeni jest szybki transfer określonych danych pomiędzy co najmniej dwoma jej uczestnikami[18]. „Cyberprzestrzeń" jest także definiowana jako zespół połączeń sieciowych, w który użytkownicy sieci (np. Internetu) mogą wchodzić określone interakcję za pomocą określonych

---

[13] M. Madej, *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*, [w:] *Bezpieczeństwo teleinformatyczne państwa*, red. M. Madej, M. Terlikowski, Warszawa 2009, s. 28; P. Tekielska, Ł. Czekaj, *Działania służb w Unii Europejskiej realizujących zadania na rzecz bezpieczeństwa cybernetycznego*, [w:] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, red. M. Górka, Warszawa 2014, s. 163; P. Levy, *Drugi potop*, [w:] *Nowe media w komunikacji społecznej w XX wieku. Antologia*, red. M. Hopfinger, Warszawa 2002, s. 380; R. Tadeusiewicz, *Wychowywanie dla cyberprzestrzeni jednym z warunków zapobiegania cyberuzależnieniom*, [w:] *Cyberuzależnienia: przeciwdziałanie uzależnieniom od komputera i Internetu*, red. E. Mastalerz, K. Pytel, H. Noga, Kraków 2007, s. 23; K. Dobrzeniecki, *Prawo a etos cyberprzestrzeni*, Toruń 2004, s. 18.

[14] Słownik języka polskiego (sjp.pl).

[15] Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016, http://bip.mswia.gov.pl/portal/bip/6/1905 (dostęp: 31.10.2021 r.).

[16] K. Dobrzeniecki, *Prawo a etos cyberprzestrzeni*, Toruń 2004, s. 18.

[17] P. Tekielska, Ł. Czekaj, *op. cit.*, s. 163.

[18] J. Janczak, *Zarządzanie sieciami teleinformatycznymi opartymi na współczesnych technologiach taktycznych WLąd*, Warszawa, 2011, *passim*.

systemów[19]. Wyżej wymienione cechy są najczęściej powtarzanymi cechami cyberprzestępczości. Dla kontrastu warto przytoczyć także definicję o charakterze interdyscyplinarnym. W tym rozumieniu „cyberprzestrzeń" jest oddzielną przestrzenią społeczną, w ramach której następuje komunikacja i wymiana gospodarcza i która nie może być pozostawiona wyłącznie oddolnej samoregulacji z uwagi m.in. na potrzebę ochrony indywidualnych interesów, takich jak np. ochrona danych osobowych, interesu publicznego, ochrona małoletnich czy penalizacja zachowań objętych regulacją prawa karnego[20]. W tym miejscu należy wskazać, że każde suwerenne państwo może przyjąć odmienną definicję, a do tych państw, które najwięcej wnoszą do rozważań prawnych należy zaliczyć m.in.: Stany Zjednoczone Ameryki[21], Wielką Brytanię[22], Francję[23] i Niemcy[24]. Co do zasady cyberprzestrzeń w każdym państwie definiowana jest na gruncie strategii lub doktryny dla cyberbezpieczeństwa. Z uwagi na to, że przedmiot

---

[19] B. Oręziak, *op. cit.*, s. 35–60.

[20] D. Lubasz, *Techniczne, ekonomiczne i prawne uwarunkowania handlu elektronicznego*, [w:] *Handel elektroniczny. Bariery prawne*, red. D. Lubasz, Warszawa 2013, *passim*.

[21] *DOD Dictionary of Military and Associated Terms 2017: A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers*, http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf (dostęp: 31.10.2021 r.).

[22] *National Cyber Security Strategy: The interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, internet connected devices and embedded processors and controllers. It may also refer to the virtual world or domain as an experienced phenomenon, or abstract concept*, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (dostęp: 31.10.2021 r.).

[23] *Information system defence and security. France's strategy: The communication space created by the worldwide interconnection of automated digital data processing equipment*, https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France _s_ strategy.pdf (dostęp: 31.10.2021 r.).

[24] *White paper on German security policy and the future of the Bundeswehr: Information, its distribution, perception, and interpretation are critical factors and resources in the knowledge society of the 21st century. The information domain is the space in which information is generated, processed, disseminated, discussed, and stored. Cyber space is the virtual space of all IT systems linked and linkable at data level on a global scale. Cyber space is based on the Internet, a publicly accessible network that can be expanded by any number of data networks*, https://www.bundeswehr.de/resource/ resource/MzEzNTM4MmUzMzMyMmUzMTM1MzMyZTM2MzIzMDMwMzAzMDMwMzAzMDY5NzE3MzM1Njc2NDYyMzMyMDIwMjAyMDIw/2016%20White%20Paper.pdf (dostęp: 31.10.2021 r.).

artykułu bazuje na polskim porządku prawnym należy skupić się na definicji wykształconej w polskim systemie prawa. Polski ustawodawca zdecydował się na zdefiniowanie „cyberprzestępczości" w następujących aktach normatywnych: ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (art. 2 ust. 1b)[25] ustawy o stanie wyjątkowym (art. 2 ust. 1a)[26] i ustawy o stanie klęski żywiołowej (art. 3 ust. 1 pkt 4)[27]. Za „cyberprzestrzeń" w myśl ustaw o stanach nadzwyczajnych, ustawodawca uznaje:

> przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne[28], wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami. W treści definicji obecne jest zarówno pojęcie „informacji", jak i pojęcie „systemów teleinformatycznych", które to pojęcia – jak się wydaje – stanowią jądro definicji cyberprzestrzeni[29].

Cyberprzestrzeń jest również rozlegle definiowana na gruncie międzynarodowym. Z tego dorobku korzysta ustawodawca konstruując regulacje krajowe. Na zakończenie warto wskazać, że cyberprzestrzeń pozostaje w silnym związku z pojęciami „cyberbezpieczeństwa", które nie będzie szerzej poruszane na kanwie niniejszego artykułu oraz zagadnieniem cyberprzestępczości, które jest jednym z istotnych elementów przedmiotowych niniejszego artykułu.

---

[25] Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz.U. z 2002 r. Nr 156, poz. 1301).

[26] Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (t.j. Dz.U. z 2017 r. poz. 1928, z późn. zm.).

[27] Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (tj. Dz.U. z 2017 r. poz. 1897, z późn. zm.).

[28] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2023 r. poz. 57, z późn. zm.).

[29] J. Taczkowska-Olszewska, K. Chałubińska-Jentkiewicz, M. Nowikowska, *Retencja, migracja i przepływy danych w cyberprzestrzeni. Ochrona danych osobowych w systemie bezpieczeństwa państwa*, Warszawa 2018, s. 4–6.

3. Pojęcie „cyberprzestępczości"

Prima facie wydaje się, że cyberprzestępczość można zdefiniować prosto. Z językowego punktu widzenia można uznać ją za ogół przestępstw popełnionych w cyberprzestrzeni (przy wykorzystaniu środków komunikacji elektronicznej)[30]. Niemniej wchodząc dalej w rozważania na temat cyberprzestrzeni w ujęciu prawnokarnym, pojawia się więcej znaków zapytania. Po pierwsze, trzeba zaznaczyć, że w polskim porządku prawnym nie ma definicji legalnej „cyberprzestępczości". Należy uznać to za celowy i słuszny zabieg ustawodawcy, z uwagi na specyfikę i prędkość zmian zachodzących w dzisiejszym świecie, który podlega regulacji prawnej. A. Završnik dokonał ciekawego rozróżnienia na generacje cyberprzestępstw, które pozwala zobrazować rozwój cyberprzestępczości[31]. Do pierwszej generacji zalicza tzw. zamachy, których celem są komputery, sieci komputerowe i różnego rodzaju dane (ang. *first generation of cybercrime*). Druga generacja jest pokłosiem rozwoju sieci teleinformatycznych i kojarzona jest głównie z atakami na ich integralność i dostępność tzw. *hacking*[32]. Trzecia generacja jest ściśle powiązana z procesem tzw. automatyzacji cyberprzestępczości będącej między innymi efektem wykorzystania specjalnego oprogramowania. Jej cechą charakterystyczną jest to, że czynu zabronionego nie musi dokonywać człowiek, a specjalnie do tego przygotowany algorytm lub oprogramowanie. Z przedstawionego rozróżnienia wynika, że postępująca cyfryzacja i informatyzacja, a dalej pojawienie się cyberprzestrzeni doprowadziło do pojawienia się nowych typów cyberprzestępstw oraz stypizowania ich w Kodeksie karnym[33]. Ustawodawca musi być niezwykle wyczulony w tym aspekcie. Co ważne, mimo usilnych starań, wiele przestępstw nadal wymyka się ustawowym znamionom i wprost nie podlega karze. Wyżej wspomniane procesy mają wpływ na zmiany w postrzeganiu cyberprzestrzeni i w efekcie w definiowaniu cyberprzestępczości.

---

[30] Słownik języka polskiego (sjp.pl).

[31] A. Završnik, *Cybercrime definitional challenges and criminological particularities*; http://www.inst–krim.si/upload/izdajanje/AZavrsnikcybercrime.pdf (dostęp: 31.10.2021 r.).

[32] F. Radoniewicz, *Odpowiedzialność karna za przestępstwo hackingu*, „Prawo w Działaniu" 2013, nr 13, s. 112–130.

[33] J. Wasilewski, *Cyberprzestępczość – wybrane aspekty prawnokarne i kryminalistyczne*, Białystok 2017, s. 4–20.

W tym kontekście konieczne jest uwypuklenie tego, że pojęcie cyberprzestępstwa nie stanowi ścisłej kategorii prawnej[34]. W celu odpowiedzi na pytanie czym w istocie jest cyberprzestępstwo niezbędne wydaje się odniesienie do konkretnych przestępstw stypizowanych w Kodeksie karnym oraz dorobku doktryny i orzecznictwa. Z pewnością za „cyberprzestępstwo" można uznać popełnienie czynu zabronionego z wykorzystaniem sieci teleinformatycznej lub dokonanie czynu, w którym komputer jest przedmiotem lub narzędziem tego przestępstwa[35]. Z innej perspektywy można na cyberprzestępczość spojrzeć jako na działalność przestępczą w określonym środowisku, tj. teleinformatycznym cyfrowym. Do rozważań definicyjnych warto wtrącić dorobek rangi międzynarodowej. Komisja Europejska, z uwagi na brak powszechnie uznawanej definicji cyberprzestępczości, zamiennie stosować takie pojęcia jak „cyberprzestępczość, przestępczość komputerowa, przestępczość związana z komputerami, przestępczość cyfrowa, przestępczość przy użyciu zaawansowanych technologii i uznawać je za tożsame"[36]. Na podstawie tego założenia za cyberprzestępczość uznaje czyny przestępcze dokonane przy użyciu sieci łączności elektronicznej i systemów informatycznych lub skierowane przeciwko takich sieciom i systemom[37]. W tym miejscu trzeba wskazać, że tak jak w przypadku cyberprzestrzeni, każde suwerenne państwo może posiadać własną definicję „cyberprzestępczości". Jednak dla nas najistotniejsze jest postrzeganie jej na gruncie polskiego systemu prawa. W dokumencie „Polityka Ochrony

[34] U. Sieber, *Przestępczość komputerowa a prawo karne informatyczne w międzynarodowym społeczeństwie informacji i ryzyka*, „Przegląd Policyjny" 1995, nr 3, s. 6.

[35] M. Siwicki, *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012, nr 7–8, s. 241–243.

[36] Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów, Bruksela, z dnia 22 maja 2007 r., KOM (2007) 267, wersja ostateczna, dostępny na http://eur–lex. euro-pa. eu/LexUriServ/LexUriServ.do?uri=COM: 2007:0267: FIN:PL:HTML (dostęp: 31.10.2021 r.). Zob. też Opinię Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie komunikatu Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: „Europejska agenda cyfrowa", COM(2010) 245, wersja ostateczna (2011/C 54/17), Dz.U.UE.C.2011.54.58. Według Rezolucji Parlamentu Europejskiego z dnia 5 maja 2010 r. w sprawie nowej agendy cyfrowej dla Europy: 2015.eu [2009/2225(INI) Dz.U.UE.C.2011.81E.45] do cyberprzestępczości zalicza się m.in. zachęcanie do ataków terrorystycznych, przestępstwa motywowane nienawiścią oraz pornografię dziecięcą.

[37] *Ibidem*.

Cyberprzestrzeni Rzeczypospolitej Polskiej" przygotowanym przez Ministerstwo Administracji i Cyfryzacji oraz Agencję Bezpieczeństwa Wewnętrznego cyberprzestrzeń definiowana jest lakonicznie jako czyny zabronione popełnione w obszarze cyberprzestrzeni[38]. Ciekawego zdekodowania tego pojęcia dokonał B. Oręziak, wyjaśniając termin „cyberprzestrzeń" i podmieniając słowo „cyberprzestrzeń" na „cyberprzestępczość". W myśl jego rozumowania „cyberprzestępstwo to czyn zabroniony popełniony w przestrzeni przetwarzania i wymiany informacji tworzonej przez systemy teleinformatyczne wraz z powiązaniami między nimi oraz relacjami z użytkownikami[39]. Wynika z tego, że na cyberprzestępstwo składa się ogół możliwych do popełnienia czynów zabronionych stypizowanych w Kodeksie karnym. Tutaj pojawia się pytanie, czy tak zbudowana definicja powinna stać się definicją legalną. Z jednej strony jest ona na tyle ogólna, że pozostawia ustawodawcy furtkę, ponieważ każdy nowy przepis typizujący będzie wpisywał się w tą definicję. Z drugiej strony z punktu widzenia praktycznego taka zmiana nie miałaby żadnego wpływu na pracę organów procesowych, więc wydaje się zbyteczna. W tym miejscu należy wskazać, że jak najbardziej słuszne jest rozumienie cyberprzestępstwa jako danego przestępstwa stypizowanego w Kodeksie karnym. Do cyberprzestępstw można zaliczyć m.in. zachowania stypizowane w następujących przepisach: art. 287 k.k. (phishing[40] i pharming[41]), art. 267 k.k., 268 k.k., 268b k.k., 165 § 1 pkt 4 k.k. (malware[42]), art. 310 k.k. (skimming[43]), art. 190a § 1 k.k., 190 § 3 k.k., 190 § 2 k.k. (kradzież

[38] *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, https://jakubow.pl/wp-content/uploads/2015/06/Polityka-Ochrony-Cyberprzestrzeni-RP_148x210_wersja-pl.768174_715482.pdf (dostęp: 31.10.2021 r.).

[39] B. Oręziak, *op. cit.*, s. 35–60.

[40] I. Protasowicki, *Phishing jako zagrożenie bezpieczeństwa osobistego w sieci*, „Zeszyty Naukowe Wyższej Szkoły Informatyki" 2016, nr 37, s. 35–46.

[41] A. Kiedrowicz-Wywiał, *Pharming i jego penalizacja*, https://docplayer.pl/40466493-Pharming-i-jego-penalizacja.html (dostęp: 31.10.2021 r.).

[42] A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 37–38.

[43] K. Mikołajczyk, *Przestępstwa związane z wykorzystaniem bankowości elektronicznej*, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiW-oGDsfTzAhUmlIsKHTVeCzoQFnoECAQQAQ&url=http%3A%2F%2Fwww.abw.gov.pl%2Fdownload%2F1%2F1304%2FSegregator5.pdf&usg=AOvVaw1TadSp3zxTpZ7PMYypi5Su (dostęp: 31.10.2021 r.).

tożsamości[44]), 200a § 1 i 2 k.k. (grooming[45]). Niniejsze określenie ram cyberprzestępstępczości pozwala nam na płynne przejście do omówienia istotnych kwestii związanych z przeciwdziałaniem i zwalczaniem cyberprzestępczości w polskim porządku prawnym.

4. Zarys strategii cyberbezpieczeństwa (w tym przeciwdziałania i zwalczania cyberprzestępczości)

Na początku należy wskazać, że istotnymi dokumentami w omawianym zakresie jest Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022 i Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024. Są to dokumenty, które wyznaczają kierunki rozwoju w zakresie polityk związanych z zapewnieniem bezpieczeństwa w cyberprzestrzeni, w tym przeciwdziałania i zwalczania cyberprzestępczości. Co istotne, zawierają one pewne postulaty prawne. Są to tylko okólniki, które nie posiadają mocy wiążącej. Pierwszy dokument w wymiarze prawnym wskazuje, że w okresie 2017–2022: „zostanie dokonany przegląd istniejących przepisów prawa w celu ich harmonizacji, zwiększenia efektywności działania i poprawy przepływu informacji pomiędzy wszystkimi interesariuszami zaangażowanymi w aktywne budowanie krajowego systemu cyberbezpieczeństwa". Podstawą wszelkich zmian ma być przede wszystkim implementacja dyrektywy NIS[46]. Z kolei strategia na lata 2019–2024 zakłada, że:

[44] K. Gorazdowski, *Kradzież tożsamości w sieci w ujęciu normatywno-opisowym*, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiRsf6IrvTzAhUCy4sKHQJLACkQFnoECAoQAQ&url=http%3A%2F%2Fcejsh.icm.edu.pl%2Fcejsh%2Felement%2Fbwmeta1.element.desklight-29e29427-b545-4fff-b71b-7591cfd605c3%2Fc%2FK._Gorazdowski.pdf&usg=AOvVaw07P3bGyQHolqse99i3XrLH (dostęp: 31.10.2021 r.).

[45] M. Dąbrowska, *Grooming – wybrane aspekty prawne i kryminologiczne*, https://brpd.gov.pl/sites/default/files/grooming_-_wybrane_aspekty_prawnokarne_i_kryminologiczne_-_marta_dabrowska_ebook.pdf (dostęp: 31.10.2021 r.).

[46] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

> podstawą rozwoju krajowego systemu cyberbezpieczeństwa jest dokonanie pełnego wdrożenia i oceny funkcjonowania przepisów ustanawiających ten system, w powiązaniu z innymi przepisami, w szczególności z ustawą z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[47] i ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych[48], także z wytycznymi zwartymi w Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej[49]. Rezultatem dokonanej oceny może być konieczność przygotowania niezbędnych zmian przepisów usuwających bariery dla skutecznej wymiany informacji oraz skoordynowanego i niezakłóconego reagowania na incydenty.

Wyszczególnione zmiany prawne mają przyczynić się do realizacji celu głównego, tj. podniesienia poziomu odporności na cyberzagrożenia oraz zwiększenia poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowania wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji. Osiągniecie tego celu niewątpliwie przyczyni się do poprawy w zwalczaniu i przeciwdziałaniu cyberprzestępczości *sensu stricto*, ale co istotne będzie możliwe jedynie poprzez realizację celów szczegółowych, do których należą:

1/ rozwój krajowego systemu cyberbezpieczeństwa;
2/ podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty;
3/ zwiększanie potencjału narodowego w zakresie bezpieczeństwa w cyberprzestrzeni;
4/ budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa;

---

[47] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. Dz.U. z 2023 r., poz. 122., z późn. zm.).

[48] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz.U. z 2019 r. poz. 742, z późn. zm.).

[49] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej – dokument zatwierdzony w Warszawie 12 maja 2020 roku*, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf (dostęp: 31.10.2021 r.).

5/ zbudowanie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa.

Wypełnienie celu głównego i celu szczegółowego będzie możliwe jedynie poprzez realizację jasno określonych zadań przez ogół organów, które posiadają kompetencje do ich realizacji. Do niniejszych zadań należy zaliczyć m.in.:

1/ zapobieganie i reagowanie w odniesieniu do incydentów oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa,
2/ stworzenie zasad dobrej współpracy pomiędzy sektorami publicznym i prywatnym,
3/ zbudowanie umiejętnego podejścia do oceny ryzyka wystąpienia ataku w cyberprzestrzeni,
4/ propagowanie edukacji, informacji i szkoleń w zakresie cyberbezpieczeństwa,
5/ podjęcie działań odnoszących się do planów badawczo-rozwojowych w zakresie bezpieczeństwa teleinformatycznego,
6/ wzmocnienie współpracy międzynarodowy w zakresie cyberbezpieczeństwa[50].

Niniejsze cele mogą być wypełniane jedynie w oparciu o uprawnienia wprost wynikające z aktów prawa powszechnie obowiązującego. Uprawnienia do realizowania określonych zadań mogą znajdować się w wielu aktach prawnych i dotyczą wielu płaszczyzn życia społecznego i są przypisane do właściwych organów administracji publicznej. W przejrzysty sposób naszkicował je T. Hoffman[51]. Do organów, które wykonują zadania związane z zapewnieniem cyberbezpieczeństwa, a w związku z tym z przeciwdziałaniem cyberprzestępczości, *sensu largo* można zaliczyć m.in.: Radę Ministrów, Minister Spraw Wewnętrznych

[50] Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022, https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022 (dostęp: 31.10.2021 r.), Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024 (dostęp: 31.10.2021 r.).

[51] T. Hoffman, *Zadania organów administracji w zakresie ochrony cyberprzestrzeni*, http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-3ce2cfd7-f402-4f92-a0e2-70b3edda5e94/c/Hoffmann.pdf (dostęp: 31.10.2021 r.).

i Administracji, Ministra Cyfryzacji (w tym Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL), Agencję Bezpieczeństwa Wewnętrznego Minister Obrony Narodowej, (w tym Pełnomocnika MON ds. Bezpieczeństwa Cyberprzestrzeni, Centrum Bezpieczeństwa Cybernetycznego, Narodowe Centrum Kryptologii), Służbę Kontrwywiadu Wojskowego Policję (w tym Komendanta Głównego Policji oraz Biuro Służby Kryminalnej, w ramach którego powołano Wydział ds. Walki z Cyberprzestępczością), ministra właściwego ds. łączności, Prezesa Urzędu Komunikacji Elektronicznej, Prokuraturę oraz sądy. Niniejsze organy działają na wielu poziomach i na różnych płaszczyznach. Z perspektywy prawnej najistotniejsze wydają się być zadania Prokuratury oraz sądów, ale niniejsze organy ograniczają się do swoich ról procesowych i ich powinnością jest przystosowanie się do aktualnych realiów. Obszarem, który wymaga analizy, są ustawowe uprawnienia procesowe wybranych organów, niezaliczanych do władzy sądowniczej, których celem jest zwalczanie i przeciwdziałanie cyberprzestępczości, tj. służby specjalne.

5. Charakterystyka wybranych uprawnień służb specjalnych w przeciwdziałaniu i zwalczaniu cyberprzestępczości

Przedmiotem dalszych rozważań będą zagadnienia ściśle związane z prawem karnym procesowym i charakterystyką wybranych uprawnień służb specjalnych. Warto nadmienić, że konkretne uprawnienia służb specjalnych związane z zwalczaniem i przeciwdziałaniem cyberprzestępczości reguluje Kodeks postępowania karnego oraz ustawy szczególne. Na początku trzeba wskazać na dwa istotne przepisy k.p.k., które są swoistą ramą dla działalności służb specjalnych w omawianym obszarze[52]. Pierwszy z nich to art. 298 k.p.k., który wprost stanowi, że:

[52] T. Kuć, *Funkcje służb specjalnych RP w świetle regulacji prawnych*, „Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach" 2016, s. 135–142.

> postępowanie przygotowawcze prowadzi lub nadzoruje prokurator, a w zakresie przewidzianym w ustawie prowadzi je Policja. W wypadkach przewidzianych w ustawie uprawnienia Policji przysługują innym organom.

Doprecyzowaniem niniejszej kwestii jest art. 312 k.p.k., który wskazuje, że:

> uprawnienia Policji przysługują także: organom Straży Granicznej, Agencji Bezpieczeństwa Wewnętrznego, Krajowej Administracji Skarbowej, Centralnego Biura Antykorupcyjnego oraz Żandarmerii Wojskowej, w zakresie ich właściwości; oraz innym organom przewidzianym w przepisach szczególnych.

Przytoczone przepisy wskazują, że służby specjalne biorą udział w postępowaniu przygotowawczym w procesie karnym tj. bezpośrednio zwalczają przestępczość, czyli w kontekście omawianego artykułu także cyberprzestępczość[53]. Już na takiej podstawie można wyprowadzić wniosek, że uprawnienia w omawianym zakresie są rozproszone tj. posiada je wiele organów oraz mogą znajdować się w różnych aktach normatywnych[54]. Rozważania na temat zwalczania i przeciwdziałania cyberprzestępczości w korelacji z uprawnieniami wybranych organów należy zacząć od wskazania na doniosłość roli odgrywanej przez Agencję Bezpieczeństwa Wewnętrznego. Jest to organ administracji publicznej właściwy w sprawach ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego. Art. 5 ust. 1 pkt 2 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu[55] wskazuje, że do zadań ABW należy rozpoznawanie, zapobieganie i wykrywanie przestępstw, z kolei art. 5 ust. 1 pkt 2a wymienia wprost, że do obowiązków ABW należy:

---

[53] M. Bożek, *Charakterystyka ustawowych uprawnień operacyjnych służb specjalnych*, „Rocznik Administracji Publicznej" 2015, nr 1, s. 27–44.

[54] K. Kraj, *Badania naukowe nad służbami specjalnymi*, http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-8fcfd4a2-33b2-4636-b345-504ba4c39c82/c/Kraj.pdf (dostęp: 31.10.2021 r.).

[55] Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j. Dz.U. z 2022 r. poz. 557, z późn. zm.).

> rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo, istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym".

ABW jest także odpowiedzialne za ściganie sprawców cyberprzestępstw pozostających w jej właściwości rzeczowej[56]. Agencja wypełnia swoje ustawowe zadania dzięki szczególnym uprawnieniom do prowadzenia czynności analityczno-informacyjnych[57], operacyjno-rozpoznawczych[58] i dochodzeniowo-śledczych[59]. Ustawodawca umożliwił także ABW prowadzenie kontroli operacyjnej. Zgodę na nią musi wyrazić sąd, na pisemny wniosek szefa Agencji złożony po uzyskaniu pisemnej zgody prokuratora generalnego. Przy składaniu takiego wnioski konieczne jest uwypuklenie bezskuteczności albo nieprzydatności innych środków pracy operacyjnej[60]. Kolejnym organem, który odgrywa istotną rolę w zwalczaniu cyberprzestępczości, ale na nieco innym odcinku jest Służba Kontrwywiadu Wojskowego. Jest ona właściwa w sprawach ochrony przed zagrożeniami wewnętrznymi dla obronności Państwa, bezpieczeństwa i zdolności bojowej Sił Zbrojnych Rzeczypospolitej Polskiej, oraz innych jednostek organizacyjnych podległych lub nadzorowanych przez Ministra Obrony

---

[56] M. Bożek, *Zwalczanie przestępstw jako ustawowe zadanie Agencji Bezpieczeństwa Wewnętrznego. Stan obecny i postulaty de lege ferenda*, https://journals.umcs.pl/sil/article/download/583/565 (dostęp: 31.10.2021 r.).

[57] A. Misiuk, *Instytucjonalny system bezpieczeństwa państwa*, Warszawa 2013, s. 198.

[58] E. Wójcik, *Czynności operacyjno-rozpoznawcze i ich rola w zwalczaniu przestępczości zorganizowane*, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwi6koK1tvTzAhWpAxAIHR1kA9MQFnoECAUQAQ&url=http%3A%2F%2Fm.wspia.eu%2Ffile%2F21440%2F44-W%25C3%2593JCIK.pdf&usg=AOvVaw21AHV2uSXxDs8hrcxBPPoU (dostęp: 31.10.2021 r.).

[59] M. Bożek, *Charakterystyka*…, s. 27–44.

[60] A Król, *Działalność operacyjna służb specjalnych w systemie bezpieczeństwa państwa*, https://www.abw.gov.pl/download/1/1291/Segregator20.pdf (dostęp: 31.10.2021 r.).

Narodowej. Zgodnie art. 5 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego[61] do zadań SKW należy m.in. rozpoznawanie, zapobieganie oraz wykrywanie, popełnianych przez żołnierzy pełniących czynną służbę wojskową, funkcjonariuszy SKW i SWW oraz pracowników SZ RP i innych jednostek organizacyjnych MON, enumeratywnie określonych przestępstw[62] oraz współdziałanie z Żandarmerią Wojskową i innymi organami uprawnionymi do ścigania enumeratywnie określonych przestępstw[63]. SKW w omawianym zakresie ma podobną pozycję co ABW, ale działa wyłącznie na wycinku wojskowym. SKW posiada także uprawnienia operacyjne, ale nie tak szerokie jak ABW. SKW prowadzi czynności operacyjno-rozpoznawcze i analityczno-informacyjne, ale nie może prowadzić czynności o charakterze dochodzeniowo-śledczym[64]. Zadania w zakresie zwalczania i przeciwdziałania cyberprzestępczości realizuje także Żandarmeria Wojskowa, co wynika wprost z ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych[65]. Art. 4 ust. 1 pkt 4 wskazuje, że do zadań Żandarmerii Wojskowej należy wykrywanie przestępstw i wykroczeń, w tym skarbowych, popełnionych przez określone osoby[66], ujawnianie i ściganie ich sprawców oraz ujawnianie i zabezpieczanie dowodów tych przestępstw i wykroczeń, art. 4 ust. 1 pkt 5, nadmienia, że „Żandarmeria Wojskowa zapobiega popełnianiu przestępstw i wykroczeń przez określone osoby[67]". Niniejsze zadania są realizowane dzięki uprawnieniom operacyjno-rozpoznawczym oraz dochodzeniowo-śledczym. Nieodzowną rolę w zwalczaniu cyberprzestępczości odgrywa także Policja. Jak wynika z ustawy

[61] Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (t.j. Dz.U. z 2023 r. poz. 81, z późn. zm.).

[62] Przestępstwa wymienione w art. 5 ust. 1 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego.

[63] Przestępstwa wymienione w art. 5 ust. 1 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego.

[64] M. Bożek, *Charakterystyka*…, s. 27–44.

[65] Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (t.j. Dz.U. z 2021 r. poz. 1214, z późn. zm.).

[66] Mowa tu o osobach wymienionych w art. 3 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych.

[67] Mowa tu o osobach wymienionych w art. 3 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych.

o Policji[68], jest ona „umundurowaną i uzbrojoną formację służącą społeczeństwu i przeznaczoną do ochrony bezpieczeństwa ludzi oraz do utrzymywania bezpieczeństwa i porządku publicznego". Z art. 1 ust. 2 pkt 3 wynika, że do zadań Policji należy „inicjowanie i organizowanie działań mających na celu zapobieganie popełnianiu przestępstw i wykroczeń oraz zjawiskom kryminogennym i współdziałanie w tym zakresie z organami państwowymi, samorządowymi i organizacjami społecznymi", a z art. 1 ust. 2 pkt 4 wynika kolejne zadanie nałożone na Policję związane z „wykrywaniem przestępstw i wykroczeń oraz ściganiem ich sprawców". W celu realizacji tych zadań Policja korzysta z szerokich uprawnień operacyjnych (art. 19 ustawy o Policji), dochodzeniowo-śledczych i analityczno-informacyjnych. W zwalczaniu cyberprzestępczości na konkretnym odcinku swoje zadania realizuje także Centralne Biuro Antykorupcyjne. Cyberprzestępstwa muszą być związane z korupcją w życiu publicznym i gospodarczym, w szczególności w instytucjach państwowych i samorządowych. Uprawnienia operacyjno-rozpoznawcze, informacyjno-analityczne i dochodzeniowo-śledcze CBA wynikają wprost z art. 2 ust. 1 ustawy o Centralnym Biurze Antykorupcyjnym[69]. Ponadto niniejsza ustaw nadmienia, że do zadań CBA, w zakresie swojej właściwości należy rozpoznawanie, zapobieganie i wykrywanie wymienionych enumeratywnie przestępstw[70]. Podsumowując rozważania w tym punkcie, należy wskazać, że uprawnienia wymienionych organów są dość podobne, ale w kilku miejscach różnią się z uwagi na cel i specyfikę powołania danej służby. W tym miejscu pojawia się pytanie, czy w zakresie cyberprzestępczości działania służb nie powinny być koordynowane przez inny podmiot[71]. Właśnie w celu zobrazowania tych zależności autor postanowił szerzej omówić konkretne uprawnienia wybranych pięciu służb specjalnych.

---

[68] Ustawa z dnia 6 kwietnia 1990 r. o Policji (t.j. Dz.U. z 2021 r. poz. 1882, z późn. zm.).

[69] Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (t.j. Dz.U. z 2022 r. poz. 1900, z późn. zm.).

[70] Mowa tu o czynach wymienionych w art. 2 ust. 1 pkt 1 ustawy o Centralnym Biurze Antykorupcyjnym.

[71] Być może taką rolę odegra Centralne Biuro Zwalczania Cyberprzestępczości. Projekt ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości, https://www.gov.pl/attachment/fd2e69e6-2e77-43cc-9251-ca6ff70aa272 (dostęp: 31.10.2021 r.).

Z niniejszej analizy wynika, że centralną rolę w systemie zwalczania i przeciwdziałania przestępczości odgrywają dwa organy, tj. Policja i Agencja Bezpieczeństwa Wewnętrznego, ponieważ dosięgają one najszerszego grona obywateli. Pozycja Służby Kontrwywiadu Wojskowego, Żandarmerii Wojskowej jest nieco inna z uwagi na sprecyzowany przedmiot działalności dotyczący głównie spraw wojskowych. W tym miejscu należałoby się zastanowić jakie zmiany można podjąć w celi wykorzystania potencjału służb specjalnych w zwalczaniu i przeciwdziałaniu cyberprzestępczości. Po pierwsze, należy się zastanowić nad tym czy organów posiadających uprawnienia operacyjne nie jest w aktualnym stanie prawnym zbyt dużo. W doktrynie można spotkać się z tezami, które wskazują, że zasadne byłoby ograniczenie liczby organów o statusie służb specjalnych do dwóch lub trzech, z uwagi na dublowanie kompetencji[72]. Podważane są także kwestie związane z nadzorem nad służbami specjalnymi – aktualnie sprawuje go Prezes Rady Ministrów, a przedstawiciele doktryny stoją na stanowisku, że zadania z tego zakresu powinien realizować właściwy minister ds. wewnętrznych – tj. postulują oni powrót rozwiązań prawnych, które już w Polsce obowiązywały. Kolejnym ważnym postulatem jest zagadnienie czynności-operacyjnych, które w zwalczaniu i przeciwdziałaniu cyberprzestępczości mają kluczowe znaczenie. Aktualnie uprawnienia operacyjne są rozproszone i zróżnicowane, lekarstwem na to mogłoby być przyjęcie ustawy o czynnościach operacyjnych, która jednolicie ujmowałaby m.in. zagadnienia terminologii, procedur operacyjnych, a także zasad i zakresu koordynacji działań, a ponadto pozwoliłaby zoptymalizować pracę służb specjalnych[73]. Jednak co do tego postulatu nie ma jednolitego stanowiska teoretyków ani praktyków. Niniejsza zmiana mogłaby podnieść efektywność współdziałania pomiędzy służbami, ale z drugiej strony mogłaby sparaliżować ich działalność i uczynić ją nieefektywną. Istotne jest także budowanie platform współpracy pomiędzy służbami specjalnymi, w szczególności w zakresie cyberprzestępczości. Ciekawym pomysłem postulat stworzenia

[72] T. Kuć, *op. cit.*, s. 135–142.

[73] J. Mąka, *Ustawa o czynnościach operacyjno-rozpoznawczych – czy jest potrzebna w obecnym stanie prawnym w Polsce?*, https://pk.gov.pl/wp-content/uploads/2013/12/2e4cfbdced59af973dd2ebd8a378e548.doc (dostęp: 31.10.2021 r.).

zintegrowanego krajowego systemu współpracy i koordynacji działań służb[74]. W zakresie przeciwdziałania cyberprzestępczości pomocne mogłoby się okazać także wdrożenie następujących zmian: usprawnienie zinstytucjonalizowanych formy wymiany informacji pomiędzy służbami poprzez stworzenie bazy danych o przestępczości na poziomie krajowym oraz powołanie współpracy publiczno-prywatnej ds. zwalczania cyberprzestępczości, wraz z opracowaniem regulacji prawnych określających obowiązki i uprawnienia podmiotów zaangażowanych we współpracę, z wyszczególnieniem źródeł finansowania, ustaleniem reguł współpracy krajowej i międzynarodowej), włącznie z oszacowaniem ilości i sposobu przetwarzanych danych i wskazaniem rozwiązań technicznych dla takiej współpracy[75]. Omawiane zmiany na pierwszy rzut oka mogą wydawać się rewolucyjne, ale w aktualnym realiach technologicznych i społecznych ustawodawca prędzej czy później będzie musiał się nad nimi pochylić.

6. Wnioski

Przedmiotowy artykuł omówił kwestie związane z istotnym zagadnieniem roli i uprawnień służb specjalnych w zakresie zwalczania i przeciwdziałania cyberprzestępczości. Wskazany temat jest istotny z punktu widzenia zmian zachodzących w dzisiejszym świecie, tj. digitalizacji i cyfryzacji. Jak już wcześniej wspomniano, omawiane zmiany mają zarówno dobre, jak i złe strony. Wraz z rozwojem technologicznym rozwija się także cyberprzestępczość, co stanowi coraz większe zagrożenie dla naszego życia codziennego. W związku z tym autor dokonał najpierw analizy pojęcia „cyberprzestrzeni" oraz „cyberprzestępczości", aby wyznaczyć potencjalny obszar działalności służb specjalnych. Należy wskazać, że są to pojęcia płynne, które zmieniają się wraz z rozwojem

[74] I. Oleksiewicz, *Rola służb specjalnych w polityce zwalczania cyberterroryzmu RP*, http://bazekon.icm.edu.pl/bazekon/element/bwmeta1.element.ekon-element-000171503089 (dostęp: 31.10.2021 r.).

[75] I. Oleksiewicz, *Institutional aspects of anti-cybernetic policy in Poland*, [w:] *Institutional and functional aspects of the national security protection*, red. I. Oleksiewicz, M. Pomykała, M. Polinceusz, Chicago 2014, s. 13–28.

technologicznym i ich sztywne definiowanie pozostaje bezcelowe. Następnie autor nakreślił zarys aktualnej strategii cyberbezpieczeństwa Rzeczypospolitej Polskiej ze szczególnym uwzględnieniem zagadnień związanych ze zwalczaniem i przeciwdziałaniem cyberprzestępczości. Dzięki temu wskazał na kierunki działań zmierzających do eliminacji cyberprzestępczości z życia publicznego oraz cele, które powinny zostać spełnione. Naświetlony został także instytucjonalny zarys systemu cyberbezpieczeństwa poprzez wymienienie organów, które realizują lub mogą realizować zadania związane ze zwalczaniem i przeciwdziałaniem cyberprzestępczości. Następnie przeanalizowane zostały wybrane uprawnienia służb specjalnych w zakresie zwalczania i przeciwdziałania cyberprzestępczości. Autor omówił najważniejsze uprawnienia, wskazał na różnicę i podobieństwa konkretnych organów. W dalszej części autor przedstawił wnioski *de lege ferenda*, które mogłyby się przyczynić do zoptymalizowania działań służb specjalnych w podanym zakresie. Wynika z tego, że służby specjalne mają szerokie uprawnienia operacyjne, co należy wykorzystać w zakresie zwalczania i przeciwdziałania cyberprzestępczości. Ujednolicenie uprawnień, skoordynowanie współpracy pomiędzy poszczególnymi służbami i tworzenie platform współpracy mogłoby się przyczynić do wyższej wykrywalności cyberprzestępstw, a to miałoby przełożenie na zwiększenie bezpieczeństwa w cyberprzestrzeni. Praca nad omawianymi zmianami powinna rozpocząć się już teraz na szczeblu badawczym w ujęciu interdyscyplinarnym. Po zebraniu odpowiedniego materiału oraz wyników należy poddać je dyskusji akademickiej oraz przystąpić do prac legislacyjnych. Przedstawione przez autora propozycje zmian mogą jawić się jako rewolucyjne, ale nie trzeba wszystkich wdrażać od razu. Należy robić to stopniowo, monitorując ich skutki. Przedmiotowe rozważania są jak najbardziej aktualne i z uwagi na zmiany zachodzące w życiu społecznym nie raz będą tematem debaty publicznej lub akademickiej. Dlatego priorytetem w omawianym zakresie powinno być podjęcie i promowanie rozmaitych badań o podłożu interdyscyplinarnym. Być może pozwoli to wypracować wzorcowe i płynne rozwiązania prawne, które zwiększą poziom cyberbezpieczeństwa obywateli i zapobiegną rozwojowi cyberprzestępczości.

Bibliografia

Adamski A., *Prawo karne komputerowe*, Warszawa 2000.

Aleksandrowicz T., *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, nr 15.

Babis H., *Internet*, [w:] *Encyklopedia zagadnień międzynarodowych*, red. E. Cała-Wacinkiewicz, R. Podgórzański, Warszawa 2011.

Banasiński C., Rojszczak M., Chmielewski J.M., Hydzik W., Łuczak J., Nowak W., Waćkowski K., *Zarządzanie incydentami a ustawa o krajowym systemie cyberbezpieczeństwa*, [w:] *Cyberbezpieczeństwo*, red. C. Banasiński i in., Warszawa 2020.

Bednarek J., Andrzejewska A., *Cyberświat – możliwości i zagrożenia*, Warszawa 2009.

Bednarek J., *Społeczeństwo informacyjne i media w opinii osób niepełnosprawnych*, Warszawa 2005.

Berdel-Dudzińska M., *Pojęcie cyberprzestrzeni we współczesnym polskim porządku prawnym*, „Przegląd Prawa Handlowego" 2012, nr 2.

Bożek M., *Charakterystyka ustawowych uprawnień operacyjnych służb specjalnych*, „Rocznik Administracji Publicznej" 2015, nr 1.

Bożek M., *Zwalczanie przestępstw jako ustawowe zadanie Agencji Bezpieczeństwa Wewnętrznego. Stan obecny i postulaty de lege ferenda*, https://journals.umcs.pl/sil/article/download/583/565 (dostęp: 31.10.2021 r.).

Choroszewska A., Opitek P., *Uzyskiwanie dowodów cyfrowych z zagranicy w sprawach karnych – stan obecny i procedowane zmiany, cz. II*, „Prokuratura i Prawo" 2020, nr 10–11.

Dąbrowska M., *Grooming – wybrane aspekty prawne i kryminologiczne*, https://brpd.gov.pl/sites/default/files/grooming_-_wybrane_aspekty_prawnokarne_i_kryminologiczne_-_marta_dabrowska_ebook.pdf (dostęp: 31.10.2021 r.).

Dobrzeniecki K., *Prawo a etos cyberprzestrzeni*, Toruń 2004.

Dobrzeniecki K., Przywora B., *Ograniczenia praw i wolności w okresie pandemii COVID-19 na tle porównawczym. Pierwsze doświadczenia*, Warszawa 2021.

Doktorowicz K., *Europejski model społeczeństwa informacyjnego. Polityczna strategia Unii Europejskiej w kontekście globalnych problemów wieku informacji*, Katowice 2005.

Dziomdziora W.Z., *Cyberbezpieczeństwo w samorządzie terytorialnym. Praktyczny przewodnik*, Warszawa 2021.

Gibson W., *Neuromancer*, Katowice 2009.

Gorazdowski K., *Kradzież tożsamości w sieci w ujęciu normatywno-opisowym*, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiRsf6IrvTzAhUCy4sKHQJLACkQFnoECA0QAQ&url=http%3A%2F%2Fcejsh.icm.edu.pl%2Fcejsh%2Felement%2Fbwmeta1.element.desklight-29e29427-b545-4fff-b71b-7591cfd605c3%2Fc%2FK._Gorazdowski.pdf&usg=AOvVaw07P3bGyQHolqse99i3XrLH (dostęp: 31.10.2021 r.).

Goździaszek Ł., *Cyberprzestrzeń spółek handlowych w kontekście prawnych problemów komunikacji elektronicznej*, „Przegląd Prawa Handlowego" 2009, nr 11.

Grewiński M., *Cyfryzacja i innowacje społeczne – perspektywy i zagrożenia dla społeczeństwa*, https://econjournals.sgh.waw.pl/KNoP/article/download/1265/1117/ (dostęp: 31.10.2021 r.).

Grzelak M., Liedel K., *Bezpieczeństwo w cyberprzestrzeni, zagrożenia i wyzwania dla Polski – zarys problemu*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego" 2014, nr 2(926).

Grzelak M., Liedel K., *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – Zarys problemu*, „Bezpieczeństwo Narodowe" 2012, nr 22.

Hoffman T., *Zadania organów administracji w zakresie ochrony cyberprzestrzeni*, http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-3ce2cfd-7-f402-4f92-a0e2-70b3edda5e94/c/Hoffmann.pdf (dostęp: 31.10.2021 r.).

Janczak J., *Zarządzanie sieciami teleinformatycznymi opartymi na współczesnych technologiach taktycznych WLąd*, Warszawa 2011.

Kiedrowicz-Wywiał A., *Pharming i jego penalizacja*, https://docplayer.pl/40466493-Pharming-i-jego-penalizacja.html (dostęp: 31.10.2021 r.).

Kosiński J., *Paradygmaty cyberprzestępczości*, Warszawa 2015.

Kraj K., *Badania naukowe nad służbami specjalnymi*, http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-8fcfd4a2-33b2-4636-b345-504ba4c-39c82/c/Kraj.pdf (dostęp: 31.10.2021 r.).

Król A., *Działalność operacyjna służb specjalnych w systemie bezpieczeństwa państwa*, https://www.abw.gov.pl/download/1/1291/Segregator20.pdf (dostęp: 31.10.2021 r.).

Kuć T., *Funkcje służb specjalnych RP w świetle regulacji prawnych*, „Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach" 2016.

Kulesza J., *Międzynarodowe prawo Internetu*, Poznań 2010.

Lach A., *Dowody cyfrowe w postępowaniu karnym, wybrane zagadnienia praktyczne i teoretyczne*, http://www.bibliotekacyfrowa.pl/Content/24720 (dostęp: 31.10.2021 r.).

Levy P., *Drugi potop*, [w:] *Nowe media w komunikacji społecznej w XX wieku. Antologia*, red. M. Hopfinger, Warszawa 2002.

Lewulis P., *O rozgraniczeniu definicyjnym pomiędzy przestępczością „cyber" i „komputerową" dla celów praktycznych i badawczych*, „Prokuratura i Prawo" 2021, nr 3.

Lipniewicz R., *Pojęcie i natura cyberprzestrzeni,* [w:] tenże, *Jurysdykcja podatkowa w cyberprzestrzeni,* Warszawa 2018.

Lubasz D., *Techniczne, ekonomiczne i prawne uwarunkowania handlu elektronicznego*, [w:] *Handel elektroniczny. Bariery prawne*, red. D. Lubasz, Warszawa 2013.

Łaszczyk J. (red.), *Komputer w kształceniu specjalnym: wybrane zagadnienia,* Warszawa 1998.

Łaszczyk J., Jabłonowska M. (red.), *Uczeń zdolny wyzwaniem dla współczesnej edukacji*, Warszawa 2008.

Madej M., *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*, [w:] *Bezpieczeństwo teleinformatyczne państwa*, red. M. Madej, M. Terlikowski, Warszawa 2009.

Mamak K., *Uwagi wprowadzające,* [w:] tenże, *Rewolucja cyfrowa a prawo karne,* Kraków 2019.

Mąka J., *Ustawa o czynnościach operacyjno-rozpoznawczych – czy jest potrzebna w obecnym stanie prawnym w Polsce?*, https://pk.gov.pl/wp-content/uploads/2013/12/2e4cfbdced59af973dd2ebd8a378e548.doc (dostęp: 31.10.2021 r.).

Mikołajczyk K., *Przestępstwa związane z wykorzystaniem bankowości elektronicznej*, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiW-oGDsfTzAhUmlIsKHTVeCzoQFnoECAQQAQ&url=http%3A%2F%2Fwww.abw.gov.pl%2Fdownload%2F1%2F1304%2FSegregator5.pdf&usg=AOvVaw1TadSp3zxTpZ7PMYypi5Su (dostęp: 31.10.2021 r.).

Misiuk A., *Instytucjonalny system bezpieczeństwa państwa*, Warszawa 2013.

Nowak A., *Cyberprzestrzeń jako nowa jakość zagrożeń*, „Zeszyty Naukowe Akademii Obrony Narodowej" 2013, nr 3.

Nowak L., *Metodologiczne kryterium demarkacji i problem statusu teologii*, „Nauka" 2004, nr 3.

Oleksiewicz I., *Institutional aspects of anti-cybernetic policy in Poland*, [w:] *Institutional and functional aspects of the national security protection*, red. I. Oleksiewicz, M. Pomykała, M. Polinceusz, Chicago 2014.

Oleksiewicz I., *Rola służb specjalnych w polityce zwalczania cyberterroryzmu RP*, http://bazekon.icm.edu.pl/bazekon/element/bwmeta1.element.ekon-element-000171503089 (dostęp: 31.10.2021 r.).

Oręziak B., *Cyberprzestępczość w aspektach proceduralnych. Dowody elektroniczne a nowoczesne formy przestępczości*, Warszawa 2019.

Ostaszewski P., Klimczak J., Włodarczyk-Madejska J., *Przestępczość i wymiar sprawiedliwości w pierwszym roku pandemii COVID-19,* Warszawa 2021.

Paszkowska M., *Instrumenty przymusu stosowane wobec osób podejrzanych oraz chorych na choroby zakaźne* (*w tym COVID-19*), LEX/el. 2020.

Paszkowska M., *Kwarantanna i izolacja w związku z COVID-19 w świetle nowych przepisów,* LEX/el. 2020.

Protasowicki I., *Phishing jako zagrożenie bezpieczeństwa osobistego w sieci*, „Zeszyty Naukowe Wyższej Szkoły Informatyki" 2016, nr 37.

Radoniewicz F., *Odpowiedzialność karna za przestępstwo hackingu*, „Prawo w Działaniu" 2013, nr 13.

Rojszczak M., *Cyberprzestrzeń jako nowa płaszczyzna budowania relacji społecznych,* [w:] *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*, Warszawa 2019.

Sieber U., *Przestępczość komputerowa a prawo karne informatyczne w międzynarodowym społeczeństwie informacji i ryzyka*, „Przegląd Policyjny" 1995, nr 3.

Siwicki M., *Cyberprzestępczość*, Warszawa 2013.

Siwicki M., *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012, nr 7–8.

Suchorzewska A., *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2010.

Taczkowska-Olszewska J., Chałubińska-Jentkiewicz K., Nowikowska M., *Retencja, migracja i przepływy danych w cyberprzestrzeni. Ochrona danych osobowych w systemie bezpieczeństwa państwa*, Warszawa 2018.

Tadeusiewicz R., *Wychowywanie dla cyberprzestrzeni jednym z warunków zapobiegania cyberuzależnieniom*, [w:] *Cyberuzależnienia: przeciwdziałanie uzależnieniom od komputera i Internetu*, red. E. Mastalerz, K. Pytel, H. Noga, Kraków 2007.

Tekielska P., Czekaj Ł., *Działania służb w Unii Europejskiej realizujących zadania na rzecz bezpieczeństwa cybernetycznego*, [w:] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, red. M. Górka, Warszawa 2014.

Wasilewski J., *Cyberprzestępczość – wybrane aspekty prawnokarne i kryminalistyczne*, Białystok 2017.

Wasilewski J., *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9.

Wilbrandt-Gotowicz M., [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz,* red. K. Czaplicki, A. Gryszczyńska, G. Szpor, Warszawa 2019, art. 78.

Worona J., *Regulacje bezpośrednio odnoszące się do cyberprzestrzeni*, [w:] *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*, Warszawa 2020.

Worona J., *Regulacje pośrednio odnoszące się do cyberprzestrzeni,* [w:] *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy,* Warszawa 2020.

Wójcik E., *Czynności operacyjno-rozpoznawcze i ich rola w zwalczaniu przestępczości zorganizowane*, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwi6koK1tvTzAhWpAxAIHR1kA9MQFnoECAUQAQ&url=http%3A%2F%2Fm.wspia.eu%2Ffile%2F21440%2F44-W%25C3%2593JCIK.pdf&usg=AOvVaw21AHV2uSXxDs8hrcxBPP0U (dostęp: 31.10.2021 r.).

Zakrzewski P., *Streszczenie*, [w:] *Kradzież z włamaniem*, red. M. Mozgawa, Warszawa 2021.

Završnik A., *Cybercrime definitional challenges and criminological particularities*; http://www.inst–krim.si/upload/izdajanje/AZavrsnikcybercrime.pdf (dostęp: 31.10.2021 r.).

Zielińska C., *Pojęcie cyberprzestępczości,* [w:] *Przestępczość XXI wieku. Szanse i wyzwania dla kryminologii,* red. D. Dajnowicz-Piesiecka, E. Jurgielewicz-Delegacz, E.W. Pływaczewski, Warszawa 2020.

Klaudia Łuniewska

Analiza prawna zjawiska cyberprzestępczości popełnianej przy wykorzystaniu mediów społecznościowych i platform cyfrowych – wybrane zagadnienia

1. Wprowadzenie

Dwudziesty pierwszy wiek to okres przemian społeczno-gospodarczych oraz gwałtownego postępu technologicznego. Postęp technologiczny przysporzył światu narzędzi wyręczających prace ludzi, jak również ułatwiających codzienne życie, a także umożliwił kontakt użytkownikom znajdującym się w najdalszych zakątkach kuli ziemskiej. Obecnie większość ludzi na świecie korzysta z nowoczesnych rozwiązań technologicznych w codziennym funkcjonowaniu, w tym służących do komunikacji. Rozwój nowych technologii doprowadził do upowszechnienia się metod komunikacji zdalnej. Według portalu Statista najpopularniejszą platformą społecznościową na świecie według stanu na styczeń 2022 r. jest Facebook z liczbą 2 910 mln aktywnych użytkowników miesięcznie. Kolejne miejsce w rankingu zajmuje YouTube (2 562 mln), WhatsApp (2 000 mln), Instagram (1,478 mln), Weixin/WeChat (1,263 mln), a następnie TikTok (1 000 mln)[1]. Coraz więcej obszarów naszego życia przenosi się do cyberprzestrzeni[2]. Obecnie możemy mówić o istnieniu społeczeństwa informacyjnego, które powstało za sprawą rozwoju nowoczesnych technologii informacyjno-komunikacyjnych, które przyspieszają rozwój gospodarczy i przenoszą coraz to więcej obszarów

[1] *Most popular social networks worldwide as of January 2022, ranked by number of monthly active users,* https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (dostęp: 8.03.2022 r.).

[2] K. Gawkowski, *Wpływy nowoczesnych technologii informatycznych na zdrowie i jakość życia*, „Technika, Informatyka, Inżynieria Bezpieczeństwa" 2018, s. 185–197.

życia człowieka do przestrzeni wirtualnej[3]. W 2021 r. dostęp do Internetu posiadało 92,4% gospodarstw domowych w Polsce, co stanowiło o 2,0 punktów procentowych więcej niż w 2020 r.[4] Pandemia COVID-19 oraz towarzyszący jej *lockdown* zmusił społeczeństwo do korzystania z narzędzi komunikacji zdalnej. Doświadczenia pandemii COViD-19 pokazały jak wiele spraw możliwych jest do załatwienia online, zarówno tych prywatnych, jak i służbowych, począwszy od zakupów internetowych po sprawy urzędowe. W 2021 r. osoby korzystające w ciągu ostatnich 12 miesięcy z usług administracji publicznej przez Internet stanowiły ponad 47% populacji osób w wieku 16–74 lata[5]. Dostęp do Internetu stwarza wiele możliwości, ale i również zagrożeń dla przeciętnego człowieka[6]. Rozwój cywilizacyjny doprowadził do wytworzenia się nowych form przestępczości, do których popełnienia wykorzystuje się nowoczesne rozwiązania technologiczne, w tym sprzęt komputerowy, Internet, systemy informatyczne i teleinformatyczne. Z uwagi na obecność nowoczesnych technologii w niemalże każdej sferze naszego życia wzrasta liczba zagrożeń obecnych w przestrzeni wirtualnej. Przy pomocy Internetu dokonujemy transakcji handlowych, korzystamy z bankowości elektronicznej, sklepów internetowych, portali aukcyjnych i ogłoszeniowych. Internet może posłużyć jako narzędzie do dokonywania czynów zabronionych. Do popełniania cyberprzestępstw wykorzystuje się również media społecznościowe i platformy cyfrowe. W ramach niniejszego rozdziału omówione zostaną nowoczesne formy popełniania przestępstw przy wykorzystaniu technologii informacyjnych z uwzględnieniem specyfiki mediów społecznościowych i platform cyfrowych, jak również przedstawione zostaną mechanizmy współpracy organów ścigania z administratorami tychże portali. W ramach niniejszego rozdziału zostaną omówione zasady współdziałania ze sobą organów ścigania oraz administratorów sieci społecznościowych i platform

[3] M. Czyżak, *Cyberprzestępczość a rozwój społeczeństwa informacyjnego*, „Ekonomiczne Problemy Usług" 2015, nr 117, s. 665–673.

[4] Główny Urząd Statystyczny, *Społeczeństwo informacyjne w Polsce w 2021 roku*, Warszawa 2021, s. 2.

[5] *Ibidem*, s. 3.

[6] *Krajobraz cyberprzestępczości w dobie COViD-19*, https://policja.pl/pol/aktualnosci/201028,Krajobraz-cyberprzestepczosci-w-dobie-COVID-19.html (dostęp: 19.12.2021 r.).

cyfrowych w zakresie dotyczącym gromadzenia dowodów z popełnionych za ich pośrednictwem przestępstw i usuwania nielegalnych treści.

2. Cyberprzestępstwo – ustalenie znaczenia

Cyberprzestępstwo jako specyficzną formę popełnienia przestępstwa, którą wyróżnia się z uwagi na wykorzystanie cyberprzestrzeni do popełnienia przestępstwa. Do najpopularniejszych przestępstw popełnianych w przestrzeni cyfrowej zalicza się *hacking*, organizowanie ataków mających na celu przerwanie świadczenia określonych usług (tzw. ataki Dos oraz Ddos – odmowy dostępu), szpiegowanie w sieci czy stosowanie nowoczesnych metod inżynierii społecznej umożliwiających podszywanie si pod podmioty prowadzące określone rodzaje działalności za pośrednictwem Internetu[7]. Na potrzeby niniejszych rozważań zostanie przyjęta definicja „cyberprzestępczości", zgodnie z którą cyberprzestępstwami są czyny zabronione, skierowane przeciwko systemom informatycznym, w których komputer jest celem samym w sobie, oraz czyny dokonane z użyciem komputera, w których stanowi on jedynie narzędzie[8].

W polskim porządku prawnym nie funkcjonuje jednolita definicja legalna „cyberprzestępczości" lub „cyberprzestępstwa". Nawet przepisy Kodeksu karnego nie wprowadzają do słowniczka pojęć znaczenia tego zjawiska. Chcąc ustalić zakres definicyjny „cyberprzestępstwa", należy odwołać się do najważniejszych aktów międzynarodowych regulujących kwestię cyberprzestępczości, które wprowadziły definicje na własne potrzeby. Warto tutaj wymienić chociażby Konwencję Rady Europy o cyberprzestępczości z dnia 23 listopada 2001 r.[9] (dalej: Konwencja), według której polega to zjawisko na umyślnym i bezprawnym

[7] J. Wasilewski, *Cyberprzestępczość – wybrane aspekty prawnokarne i kryminalistyczne*, Białystok 2017, s. 40–43.

[8] M. Stefanowicz, *Cyberprzestępczość – próba diagnozy zjawiska*, „Kwartalnik Policyjny" 2017, nr 4, s. 19–23.

[9] Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz.U. z 2015 r. poz. 728); Polska przyjęła Konwencję na podstawie ustawy z dnia 12 września 2014 r. o ratyfikacji Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie w dniu 23 listopada 2001 r. (Dz.U. z 2014 r. poz. 1514).

dostępie do całości lub części systemu informatycznego; umyślnym i bezprawnym przechwytywaniu za pomocą urządzeń technicznych niepublicznych transmisji danych informatycznych do, z, lub w ramach systemu informatycznego, łącznie z emisjami elektromagnetycznymi pochodzącymi z systemu informatycznego przekazującego takie dane informatyczne; umyślnym i bezprawnym niszczeniu, wykasowywaniu, uszkadzaniu, dokonywaniu zmian lub usuwania danych informatycznych, poważnym zakłócaniu funkcjonowania systemu informatycznego poprzez wprowadzanie, transmisji, niszczeniu, wykasowywaniu, uszkadzaniu, dokonywaniu zmian lub usuwaniu danych informatycznych; produkcji, sprzedaży, pozyskiwaniu z zamiarem wykorzystania, importowaniu, dystrybucji lub innego udostępniania urządzenia, w tym także programu komputerowego, przeznaczonego lub przystosowanego przede wszystkim dla celów popełnienia któregokolwiek z przestępstw lub hasła komputerowego, kodu dostępu lub podobnych danych, dzięki którym całość lub część systemu informatycznego jest dostępna z zamiarem wykorzystania dla celów popełnienia któregokolwiek z przestępstw[10]. Konwencja wprowadza również podział cyberprzestępstw na przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów (czego przykładem jest chociażby nielegalny dostęp, nielegalne przechwytywanie danych, naruszenie integralności danych, naruszenie integralności systemu oraz niewłaściwe użycie urządzeń), przestępstwa komputerowe (m.in. fałszerstwo komputerowe, oszustwo komputerowe), przestępstwa ze względu na charakter zawartych informacji (przykładem są przestępstwa związane z pornografią dziecięcą, a także rozpowszechnianie materiałów o treściach rasistowskich i ksenofobicznych przez systemy komputerowe, groźby motywowane rasizmem lub ksenofobią, zaprzeczanie, rewidowanie albo usprawiedliwianie ludobójstwa oraz zbrodni przeciwko ludzkości), a także przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych[11]. Przepisy Konwencji zostały

[10] M. Stefanowicz, *op. cit.*, s. 19–23.

[11] K. Buczkowski, *Skuteczność zwalczania przestępstw przeciwko bezpieczeństwu elektronicznie przetwarzanej informacji na podstawie badań aktowych przestępstwa z art. 287 k.k.*, Warszawa 2015, https://iws.gov.pl/wp-content/uploads/2018/08/kolor_IWS_Buczkowski-K._Oszustwo-komputerowe.pdf (dostęp: 13.11.2021 r.).

implementowane do polskiego porządku prawnego poprzez wprowadzenie ich do ustawy z dnia 6 czerwca 1997 r. – Kodeks karny[12], a także ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych[13], jak również ustawy z dnia 30 marca 2002 r. Prawo własności przemysłowej[14].

Z kolei Międzynarodowa Organizacja Policji Kryminalnych „Interpol" cyberprzestępstwa dzieli na następujące kategorie: zamachy polegające na naruszeniu praw dostępu do zasobów (np. *hacking*), oszustwa przy użyciu komputera (np. oszustwa bankomatowe, fałszowanie urządzeń wejścia lub wyjścia, oszustwa w systemach telekomunikacyjnych), powielanie programów, sabotaż sprzętu i oprogramowania, przechowywanie zabronionych prawem zbiorów, przestępstwa popełnione w sieci[15].

3. Przestępstwa popełniane za pośrednictwem mediów społecznościowych – perspektywa dowodowa

W ramach niniejszej części zostanie ukazana specyfika przestępstw popełnianych przy wykorzystaniu mediów społecznościowych, a także ich dopuszczalności w postępowaniu karnym. Media społecznościowe stanowią przestrzeń, w ramach której może dochodzić do popełniania przestępstw, jak również mogą one posłużyć jako środek do ich popełnienia. Media społecznościowe i platformy cyfrowe podobnie jak systemy teleinformatyczne oraz sieci mogą posłużyć zarówno do popełnienia tradycyjnie rozumianych przestępstw takich jak oszustwo czy zniewaga, jak i cyberprzestępstw, które pojawiły się dopiero z upowszechnieniem się Internetu, a więc np. kradzieży kont do mediów społecznościowych, ingerowaniem w dane. Media społecznościowe dają możliwość szerokiego zastosowania metod socjotechnicznych, które mają na celu

[12] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. Dz.U. z 2021 r. poz. 2447).

[13] Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz.U. z 2021 r. poz. 1062).

[14] Ustawa z dnia 30 marca 2002 r. Prawo własności przemysłowej (t.j. Dz.U. z 2021 r. poz. 324).

[15] M. Siwicki, *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012, nr 7–8, s. 241–252.

zmanipulowanie użytkownika i wprowadzenie go w błąd, a także zmuszenie do określonych zachowań[16]. Przykładem przestępstw popełnianych w przestrzeni cyfrowej za pośrednictwem mediów społecznościowych i platform cyfrowych może być chociażby stalking, oszustwo w sieci, kradzież tożsamości w sieci, nawoływanie do nienawiści na tle różnic etnicznych, zakłócanie pracy systemu informatycznego przy użyciu złośliwego oprogramowania, jak również znieważanie innych użytkowników[17]. W ramach projektu badawczego pt. „Media społecznościowe w pracy organów ścigania"[18], przeprowadzono szczegółowe badania aktowe, z których wynika, że analiza dowodów z mediów społecznościowych przez organy wymiaru sprawiedliwości dotyczyła w większości postępowań, gdzie głównym zarzutem było popełnienie przestępstwa przeciwko życiu i zdrowiu: zabójstwo, w tym usiłowanie zabójstwa oraz spowodowanie uszczerbku na zdrowiu. Kolejne dziesięć spraw dotyczyło przestępstw przeciwko wolności seksualnej i obyczajności. siedem spraw dotyczyło popełnienia przestępstw przeciwko mieniu, a sześć przeciwko porządkowi publicznemu. W zestawieniu wskazano również sprawy przeciwko wolności oraz z ustawy o przeciwdziałaniu narkomanii, przestępstwa przeciwko pokojowi, ludzkości oraz zbrodni wojennych, sprawy dotyczące zakłócenia pracy systemu informatycznego[19]. Media społecznościowe mogą być dla organów wymiaru sprawiedliwości źródłem informacji na temat popełnionych przestępstw. Media społecznościowe mogą posłużyć bezpośrednio do popełnienia czynu zabronionego, mogą zostać wykorzystane jako narzędzie popełnienia lub przygotowania przestępstwa. Media społecznościowe mogą zostać również wykorzystywane do ustalenia wiarygodności osobowych źródeł dowodowych, tj. oskarżonych, pokrzywdzonych oraz świadków, jak również mogą posłużyć do ustalenia roli

[16] J. Wasilewski, *Przestępczość w cyberprzestrzeni – zagadnienia definicyjne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, nr 15, s. 149–173.

[17] K. Skraba, I. Strzałkowski, *Media społecznościowe jako źródło dowodu w polskim procesie karnym. Badanie orzecznictwa sądów apelacyjnych i Sądu Najwyższego*, [w:] *Media społecznościowe w pracy organów ścigania*, red. P. Waszkiewicz, Warszawa 2021, s. 129–150.

[18] Projekt badawczy pt. „Media społecznościowe w pracy organów ścigania" (o nr 2018/31/B/HS5/01876) kierowany przez dra hab. Pawła Waszkiewicza finansowany ze środków Narodowego Centrum Nauki.

[19] K. Skraba, I. Strzałkowski, *op. cit.*, s. 129–150.

oskarżonego w sprawie. Informacje zamieszczone w mediach społecznościowych mogą posłużyć do określenia relacji między uczestnikami zdarzeń (powiązań osobowych)[20]. W polskim procesie karnym dowody pochodzące z mediów społecznościowych zabezpieczane są w sposób zróżnicowany. Wprowadza się je do postępowania karnego w postaci przeprowadzania oględzin rzeczy albo sporządzenia notatki urzędowej. Co istotne, pierwsza z nich jest przedmiotem krytyki ze strony części doktryny z uwagi na fakt, że treść wyświetlana na ekranie nie może zostać uznana za rzecz, wobec czego nie może stanowić obiektu oględzin. Postuluje się wprowadzenie do polskiego procesu karnego czynności procesowej dedykowanej zabezpieczaniu dowodów cyfrowych lub też możliwości prowadzenia oględzin treści cyfrowych w sposób tożsamy jak w przypadku przeszukania czy zatrzymania rzeczy. Wskazuje się na występowanie powszechnej praktyki polegającej na przedstawianiu jako dowodu z dokumentu wydruków ze stron internetowych i portali społecznościowych. Warto wskazać na zagrożenie związane z brakiem możliwości uwierzytelnienia takiego wydruku, czy też jego podatności na manipulację[21]. Ograniczone możliwości ścigania sprawców cyberprzestępstw wynikają ze specyfiki tychże przestępstw, które polegają na m.in. ponadnarodowym charakterze, możliwości zdalnego działania sprawców, krótkim czasie popełnienia przestępstwa, możliwości łatwego kamuflowania czynu, potrzebie wyspecjalizowanej kadry i specjalistycznej techniki wykrywania i zbierania dowodów[22].

---

[20] *Ibidem*.

[21] P. Waszkiewicz, H. Dębniak, S. Rabczuk, *Wybrane aspekty dopuszczalności dowodów pochodzących z mediów społecznościowych w postępowaniu karnym – ujęcie porównawcze*, [w:] *Media społecznościowe w pracy organów ścigania*, red. P. Waszkiewicz, Warszawa 2021, s. 107–128.

[22] R. Jedlińska, *Problem przestępczości elektronicznej*, „Ekonomiczne Problemy Usług" 2017, nr 1(126), t. 2, s. 185–194.

4. Wykorzystanie mediów społecznościowych i platform cyfrowych przez organy ścigania

Stały rozwój technologii sprawia, że większość metod zwalczania przestępczości internetowej stosunkowo szybko staje się przestarzała i nieskuteczna. Zagrożenie cyberprzestępstwami znacząco wzrosło w ostatnich latach. Stosowanie różnorodnych metod i dynamiczny rozwój technologii, dzięki którym przestępcy ukrywają swoją tożsamość sprawiają, że zwalczanie cyberprzestępczości jest coraz większym wyzwaniem dla organów ścigania, dlatego tak istotne znaczenie ma unowocześnianie metod służących do wykrywania i walki z przestępczością komputerową[23]. Perspektywa wykorzystania mediów społecznościowych i platform cyfrowych przez organy ścigania może się jawić dwojnasób. Pierwszy sposób dotyczy czerpania informacji o popełnionych przestępstwach lub zamiarze ich popełniania przy pomocy ogólnodostępnych źródeł informacji, a więc za pomocą tzw. „białego wywiadu". Drugi sposób dotyczy uzyskania dostępu do treści znajdujących się na portalach internetowych za pomocą administratorów tychże stron. Możliwe jest również zastosowanie przez organy ścigania i służby specjalne metod niezgodnych z prawem (tzw. „szarego" i „czarnego wywiadu"), ale nie będzie on przedmiotem niniejszych rozważań[24]. Charakterystycznym narzędziem i jednym z elementów ww. wywiadu jawnoźródłowego (ang. *Open Source Intelligence*, OSINT) jest inteligencja mediów społecznościowych (ang. *Social Media Intelligence*, SOCMINT), która jest również elementem inteligencji cyfrowej. Odnosi się do zbiorczych narzędzi i rozwiązań, pozwalających odpowiednim instytucjom monitorować kanały społecznościowe i rozmowy, reagować na sygnały społeczne i syntetyzować dane w logiczne kategorie i analizy oparte na potrzebach użytkownika. SOCMINT definiowany jest z uwagi na wykorzystanie mediów społecznościowych. SOCMINT może

[23] Zob. P. Ciszek, *Cyberprzestępczość i jej zwalczanie z innej perspektywy*, [w:] *Przestępczość Teleinformatyczna*, red. J. Kosiński, Szczytno 2015, s. 25–26; M. Wróbel, *Cyberprzestępczość w polskim systemie prawnym*, „Wiedza Obronna" 2014, nr 4, s. 72–90; P. Lewulis, *O rozgraniczeniu definicyjnym pomiędzy przestępczością „cyber" i „komputerową" dla celów praktycznych i badawczych*, „Prokuratura i Prawo" 2021, nr 3, s. 12–34.

[24] B. Saramak, *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy*, Warszawa 2015, *passim*.

być źródłem informacji dla organów ścigania, jak również wywiadu, na temat tożsamości osób podejrzanych, ich lokalizacji i przepływu środków finansowych pomiędzy nimi. Nowoczesne programy tworzone do walki z cyberprzestępczością wyposażone w geolokalizację mogą ustalić miejsce pochodzenia obrazu, ale i równię buforowanie danych i rozpoznawanie twarzy[25].

Kluczowym aspektem jest określenie sposobu współpracy organów ścigania z właścicielami platform cyfrowych i administratorów mediów społecznościowych. Niekiedy zdarza się, że portale tego typu posiadają uregulowaną procedurę udostępniania informacji o swoich użytkownikach na żądanie odpowiednich instytucji państwowych. Przykładowo, politykę taką przyjął Facebook, który posiada specjalną zakładkę, w której wskazuje sposób udostępniania informacji organom ścigania. Podobną praktykę w tym zakresie przyjął Instagram, WhatsApp, jak również Twitter.

W regionie europejskim usługodawcą i administratorem danych zamieszczanych na platformach Facebook, Instagram i WhatsApp jest *Meta Platforms Ireland Ltd* z siedzibą w Dublinie w Irlandii[26].

Podstawą prawną ujawnienia danych kont funkcjonujących na platformie społecznościowej Facebook jest jego regulamin oraz stosowane przepisy prawa. W przypadku Stanów Zjednoczonych Ameryki ramy prawne wyznaczają postanowienia ustawy federalnej *Stored Communications Act*, 18 U.S.C., sekcje 2701-2712 (dalej: SCA)[27]. W oparciu o wymogi dotyczące amerykańskich procedur prawnych, do tego, aby móc ujawnić podstawowe dane użytkownika wymagane jest ważne wezwanie sądowe, które zostało wystawione w związku z toczącym się śledztwem w sprawie karnej. Może ono zawierać dane identyfikujące profil, w tym m.in. imię i nazwisko, czas korzystania z serwisu, dane karty kredytowej, adres(y) e-mail i adresy IP, z których po raz ostatni logowano się i wylogowywano, o ile pozostają one dostępne[28].

---

[25] Definicja hasła „SOCMINT", [w:] *Vademecum bezpieczeństwa informacyjnego,* t. 2, N-T, Kraków 2020, s. 362–370.

[26] *Informacje dla organów ścigania*, https://www.facebook.com/safety/groups/law/guidelines/ (dostęp: 2.03.2022 r.).

[27] The Stored Communications Act (SCA, 18 U.S.C., Chapter 121 §§ 2701–2712).

[28] *Informacje dla organów ścigania*, https://www.facebook.com/safety/groups/law/guidelines/ (dostęp: 2.03.2022 r.); *Facebook i organy ścigania*, https://pl-pl.facebook.com/safety/groups/law (dostęp: 2.03.2022 r.).

W zakresie dotyczącym współpracy międzynarodowej ujawnienie zawartości konta może być uzależnione od przedstawienia nakazu ujawnienia danych, powołującego się na traktat o wzajemnej pomocy prawnej lub wniosku o udzielenie pomocy prawnej. Facebook zastrzega sobie prawo do rozpatrywania wniosków przesyłanych wyłącznie przez osoby będące funkcjonariuszami organów ścigania. Facebook w przeciągu 90 dni od otrzymania oficjalnego wniosku od organów ścigania podejmuje odpowiednie kroki w celu zachowania danych konta w związku z toczącym się postępowaniem karnym. Facebook stworzył specjalny formularz na swojej stronie do internetowego zgłaszania żądań ze strony organów ścigania[29]. W sytuacjach wymagających szybkiej reakcji, a więc wiążących się z bezpośrednią możliwością wyrządzenia krzywdy dziecku lub bezpośrednim zagrożeniem śmiercią, albo poważnym uszkodzeniem ciała jakiejkolwiek osoby i wymagających niezwłocznego udostępnienia informacji również powinny przesyłać wnioski za pośrednictwem internetowego systemu obsługi wniosków od organów ścigania[30]. Co ciekawe, W pierwszej połowie 2021 r. najwięcej wniosków o dane użytkownika wysyłanych do Facebook od agencji federalnych i rządów skierowały odpowiednio: Stany Zjednoczone Ameryki (63 657 wniosków), Indie (45 275 wniosków), Niemcy (15 554 wnioski), Francja (13 822 wnioski), Brazylia (12 989 wniosków), Wielka Brytania (10 678 wniosków), Turcja (7 825 wniosków), Polska (5 033 wnioski)[31].

Tożsame procedury w tym zakresie stworzył Instagram[32], jak również WhatsApp[33], należące do tego samego amerykańskiego konglomeratu technologicznego[34].

---

[29] *Internetowe zgłaszanie dla organów ścigania*, https://www.facebook.com/records/login/ (dostęp: 2.03.2022 r.).

[30] *Polityka prywatności Facebook*, https://www.facebook.com/about/privacy (dostęp: 20.01.2022 r.)

[31] *Number of user data requests issued to Facebook from federal agencies and governments during 1st half 2021, by country,* https://www.statista.com/statistics/287845/global-data-requests-from-facebook-by-federal-agencies-and-governments/ (dostęp: 2.03.2022 r.).

[32] *Informacje dla przedstawicieli organów ścigania*, https://pl-pl.facebook.com/help/instagram/494561080557017 (dostęp: 2.03.2022 r.).

[33] *Informacje dla organów ścigania*, https://faq.whatsapp.com/general/security-and-privacy/information-for-law-enforcement-authorities/?lang=pl (dostęp: 2.03.2022 r.).

[34] *About Meta*, https://about.facebook.com/meta/ (dostęp: 3.03.2022 r.).

Niezwiązany z *Meta Platforms* Twitter przyjął podobne standardy współpracy z organami ścigania co Facebook, Instagram i WhatsApp. Twitter odpowiada na żądania skierowane przez organy ścigania, które mają swoją podstawę w przepisach prawa. W regionie europejskim do rozpatrywania żądań właściwy jest *Twitter International Unlimited Company* z siedzibą w Dublinie. Co istotne, żądania udostępnienia treści komunikacji (np. tweetów, prywatnych wiadomości, zdjęć) wymagają przedstawienia stosownego nakazu przeszukania lub równoważnego dokumentu wystawionego przez sąd właściwy dla spółki Twitter. Podobnie jak Facebook wprowadzonych standardów jest SCA. Przewidziano procedury dotyczące maksymalnego czasu oczekiwania na odpowiedź, czasu i okoliczności poinformowania użytkownika o wpłynięciu żądania dotyczącego jego konta, jak również natychmiastowego działania w nagłych sytuacjach obejmujących bezpośrednie zagrożenie życia lub wyrządzenia krzywdy dziecku[35]. Podobnie jak w przypadku Instagrama, WhatsApp'a, a także Facebooka uruchomiono formularz internetowy służący do zgłaszania żądań ze strony organów ścigania[36].

5. Polska polityka dotycząca walki z cyberprzestępczością

Opracowanie *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej* wydane przez Ministerstwo Administracji i Cyfryzacji oraz Agencję Bezpieczeństwa Wewnętrznego[37], zawierało omówienie kluczowych aspektów z punktu widzenia przeciwdziałania i zwalczania czynów zabronionych popełnionych w obszarze cyberprzestrzeni[38]. Dokument ten był dokumentem o strategicznym znaczeniu w zakresie cyberbezpieczeństwa w państwie polskim. Został

[35] *Wskazówki dla organów ścigania*, https://help.twitter.com/pl/rules-and-policies/twitter-law-enforcement-support (dostęp: 2.03.2022 r.).

[36] *Law Enforcement Request*, https://help.twitter.com/en/forms/law-enforcement (dostęp: 3.03.2022 r.).

[37] Uchwała nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022.

[38] *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, Ministerstwo Administracji i Cyfryzacji oraz Agencję Bezpieczeństwa Wewnętrznego*, Warszawa 2013, s. 5.

on w 2017 r. zastąpiony przez *Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022*[39], które z kolei zostały zastąpione przez *Strategię Cyberbezpieczeństwa RP na lata 2019–2024*[40] (dalej: Strategia). Strategia zawiera omówienie kwestii dotyczących zwiększenia zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa i zdarzeń o charakterze terrorystycznym. Według tego dokumentu istotne jest zapewnienie wsparcia dla operatorów usług kluczowych, dostawców usług cyfrowych oraz operatorów infrastruktury krytycznej w wykrywaniu oraz zwalczaniu incydentów we wszystkich fazach. W tym celu powinno zapewnić się współpracę oraz koordynację działań organów ścigania w tym zakresie, a w szczególności należy zwrócić szczególną uwagę na prawidłowe zabezpieczanie dowodów cyfrowych[41]. Jednym z najpoważniejszych zagrożeń dla bezpieczeństwa państwa i jednostek jest cyberterroryzm[42], co również znalazło potwierdzenie w Strategii.

W państwie polskim tworzone są osobne komórki ścigania, których działalność koncentruje się jedynie na ściganiu cyberprzestępczości. Przykładowo, w Prokuraturze Krajowej w ramach Departamentu do Spraw Przestępczości Gospodarczej utworzono Dział do Spraw Cyberprzestępczości, w Komendzie Głównej Policji utworzono Biuro do Walki z Cyberprzestępczością, a w każdej komendzie wojewódzkiej Policji funkcjonują Wydziały do Walki z Cyberprzestępczością[43]. Ministerstwo Spraw Wewnętrznych i Administracji we współpracy z Komendą Główną Policji stworzyło projekt ustawy o powołaniu jednolitej w skali kraju jednostki Policji do zwalczania cyberprzestępczości, który zyskał przyjęty przez Radę Ministrów, a następnie przeszedł pozytywnie

[39] Uchwała nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2017–2022.

[40] Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024.

[41] Ministerstwo Cyfryzacji, *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*, Warszawa 2019, *passim*.

[42] Zob. K. Bielski, *Cyberterroryzm – nowe zagrożenie bezpieczeństwa państwa w XXI wieku*, „Acta Politica Polonica" 2015, nr 4(34), s. 93–110; I. Oleksiewicz, *Cyberterroryzm jako realne zagrożenie dla Polski*, „Rocznik Bezpieczeństwa Międzynarodowego" 2018, t. 12, nr 1, s. 53–67; M. Musiejko, *Zjawisko cyberterroryzmu w polskim prawie karnym*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 8, s. 261–274.

[43] Ł. Krysiński, *Identyfikacja cyberprzestępców*, „Prokuratura i Prawo" 2020, nr 2, s. 120–135.

ścieżkę legislacyjną[44]. Na skutek tego, dnia 12 stycznia 2022 r. weszła w życie ustawa z dnia 17 grudnia 2021 r. o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości[45]. Ustawą z dnia 17 grudnia 2021 r. o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości zmieniono łącznie 11 ustaw istotnych z punktu widzenia spraw wewnętrznych państwa, w tym ustawę z dnia 6 kwietnia 1990 r. o Policji[46]. Na mocy tej ustawy w ramach istniejącej struktury Policji zostało powołane Centralne Biuro Zwalczania Cyberprzestępczości (dalej: CBZC), które stanowi jednostkę organizacyjną Policji służby zwalczania cyberprzestępczości. CBZC ma realizować na obszarze całego kraju zadania z zakresu rozpoznawania i zwalczania przestępstw popełnionych przy użyciu systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej oraz zapobiegania tym przestępstwom, a także wykrywania i ścigania sprawców tych przestępstw, jak również ma być wykorzystywana do wspierania w niezbędnym zakresie jednostek organizacyjnych Policji w rozpoznawaniu, zapobieganiu i zwalczaniu przestępstw popełnionych przy użyciu systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej, a także wykrywaniu i ściganiu sprawców tych przestępstw[47]. Do zadań CBZC

[44] *Rada Ministrów przyjęła projekt ustawy o powołaniu Centralnego Biura Zwalczania Cyberprzestępczości,* https://www.gov.pl/web/mswia/rada-ministrow-przyjela-projekt-ustawy-o-powolaniu-centralnego-biura-zwalczania-cyberprzestepczosci (dostęp: 9.11.2021 r.), *Powstanie Centralne Biuro Zwalczania Cyberprzestępczości,* https://www.gov.pl/web/mswia/powstanie-centralne-biuro-zwalczania-cyberprzestepczosci (dostęp: 9.11.2021 r.).

[45] Ustawa z dnia 17 grudnia 2021 r. o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości (Dz.U. z 2021 r. poz. 2447).

[46] Ustawą z dnia 17 grudnia 2021 r. o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości (Dz.U. z 2021 r. poz. 2447) zmieniono 11 ustaw, w tym ustawę z dnia 6 kwietnia 1990 r. o Policji, ustawę z dnia 16 września 1982 r. o pracownikach urzędów państwowych, ustawę z dnia 6 czerwca 1997 r. – Kodeks karny, ustawę z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego, ustawę z dnia 29 sierpnia 1997 r. – Prawo bankowe, ustawę z dnia 29 lipca 2005 r. o nadzorze nad rynkiem kapitałowym, ustawę z dnia 21 listopada 2008 r. o służbie cywilnej, ustawę z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych, ustawę z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, ustawę z dnia 4 kwietnia 2014 r. o świadczeniach odszkodowawczych przysługujących w razie wypadku lub choroby pozostających w związku ze służbą oraz ustawę z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

[47] Art. 5d ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz.U. z 2021 r. poz. 1882 z późn. zm.).

należeć będzie m.in. zapobieganie i przeciwdziałanie przestępstwom popełnianym przy użyciu systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej, a więc przykładowo walką z pedofilią popełnianą w przestrzeni cyfrowej, zwalczanie przestępstw związanych z kradzieżą tożsamości w sieci oraz walka z oszustwami w sieci[48]. Istotne jest to, iż funkcjonariuszom CBZC na mocy art. 14 ustawy o Policji w pełni przysługuje możliwość prowadzenia działań operacyjno-rozpoznawczych, dochodzeniowo-śledczych oraz administracyjno-porządkowych[49], co stwarza pole do skutecznego działania przeciwko cyberprzestępczości. Odnosząc się do struktury CBZC, należy wskazać, iż pracami CBZC kieruje Komendant Centralnego Biura Zwalczania Cyberprzestępczości, podlegający Komendantowi Głównemu Policji[50]. Zauważalną zmianą w strukturze Policji w zakresie dotyczącymi walki z cyberprzestępczością jest to, iż pracownicy zatrudnieni w Biurze do Walki z Cyberprzestępczością Komendy Głównej Policji oraz pracownicy zatrudnieni w wydziałach do walki z cyberprzestępczością komend wojewódzkich Policji albo Komendy Stołecznej Policji stają pracownikami Centralnego Biura Zwalczania Cyberprzestępczości z zachowaniem dotychczasowych warunków pracy i płacy oraz z zachowaniem ciągłości pracy[51]. Ustawa w dalszej części w art. 15 dookreśla, iż sprawy wszczęte i niezakończone w Biurze do Walki z Cyberprzestępczością Komendy Głównej Policji albo w wydziałach do walki z cyberprzestępczością komend wojewódzkich Policji albo Komendy Stołecznej Policji, albo w stosunku do policjantów lub pracowników tych jednostek i komórek organizacyjnych Policji, do czasu powołania Komendanta Centralnego Biura Zwalczania Cyberprzestępczości prowadzone będą zgodnie z dotychczasową właściwością, natomiast od dnia powołania Komendanta Centralnego Biura Zwalczania Cyberprzestępczości odpowiednio we właściwości Centralnego

[48] *Prezydent Andrzej Duda podpisał ustawę o powołaniu Centralnego Biura Zwalczania Cyberprzestępczości,* https://www.gov.pl/web/mswia/prezydent-andrzej-duda-podpisal-ustawe-o-powolaniu-centralnego-biura-zwalczania-cyberprzestepczosci (dostęp: 29.12.2021 r.).

[49] Art. 14 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz.U. z 2021 r. poz. 1882 z późn. zm.).

[50] Art. 5d ust. 2 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz.U. z 2021 r. poz. 1882 z późn. zm.).

[51] Art. 13 ustawy z dnia 17 grudnia 2021 r. o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości (Dz.U. z 2021 r. poz. 2447).

Biura Zwalczania Cyberprzestępczości przed Komendantem Głównym Policji albo przed właściwym komendantem wojewódzkim Policji, albo przed Komendantem Stołecznym Policji, chyba że dalsze prowadzenie tych spraw należeć będzie wyłącznie do Komendanta Głównego Policji lub komendy, przy której pomocy wykonuje on swoje zadania[52]. Co ciekawe, ustawa z dnia 17 grudnia 2021 r. o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości w art. 20 przewiduje maksymalny limit wydatków z budżetu państwa na realizację zadań określonych w ustawie w wysokości 4 430 000 tys. zł, przy czym budżet na 2022 r. stanowi 117 000 tys. zł, natomiast już w 2031 r. będzie to 486 000 tys. zł[53]. Wysokość budżetu przewidziana na funkcjonowanie CBZC niewątpliwie wiąże się z koniecznością poczynienia inwestycji w odpowiednią infrastrukturę technologiczną umożliwiającą skuteczną walkę z cyberprzestępczością, jak również zatrudnieniem ekspertów z zakresu wiedzy informatycznej i teleinformatycznej.

Warto w tym miejscu wspomnieć również o powołanym Zespole Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV (dalej: CSIRT GOV) prowadzonym przez Szefa Agencji Bezpieczeństwa Wewnętrznego na podstawie ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa[54]. CSIRT GOV reguluje również ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych[55], a także ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu[56]. W ramach krajowego systemu cyberbezpieczeństwa funkcjonują jeszcze CSIRT MON i CSIRT NASK, które współpracują ze sobą, z CSIRT GOV, z organami właściwymi do spraw cyberbezpieczeństwa, ministrem właściwym ds. informatyzacji oraz Pełnomocnikiem, zapewniając spójny i kompletny system zarządzania ryzykiem

[52] Art. 15 ust. 1 ustawy z dnia 17 grudnia 2021 r. o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości (Dz.U. z 2021 r. poz. 2447).

[53] Art. 20 ustawy z dnia 17 grudnia 2021 r. o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości (Dz.U. z 2021 r. poz. 2447).

[54] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2020 r. poz. 1369).

[55] Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (t.j. Dz.U. z 2021 r. poz. 2234).

[56] Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j. Dz.U. z 2022 r. poz. 557).

na poziomie krajowym, realizując zadania na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym, a także zapewniając koordynację obsługi zgłoszonych incydentów. Jednym z podstawowych zadań należących do CSIRT GOV określonych w art. 26 ust. 7 ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa[57] jest rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo, istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o której mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[58]. Co roku CSIRT GOV przedstawia raport o stanie bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej, którego celem jest podnoszenie świadomości użytkowników o aktualnych zagrożeniach i podatnościach, a także skutkach ich ewentualnego wystąpienia dla systemów teleinformatycznych. Ujęte w raporcie informacje, w tym dane statystyczne, mają dostarczyć wiedzy niezbędnej dla procesów planowania i wdrażania w instytucjach rozwiązań przyczyniających się do podwyższenia odporności jawnych systemów teleinformatycznych[59]. W 2020 r. Zespół CSIRT GOV odnotował 246 107 zgłoszeń, które zostały zakwalifikowane jako zdarzenia dotyczące potencjalnego wystąpienia incydentu teleinformatycznego w ramach obszaru kompetencyjnego CSIRT GOV[60]. Raport za 2020 r. uwzględnia również uwarunkowania wynikające z COVID-19 i *lockdown*'u. Wskazuje, iż cyberprzestępstwa popełnione w 2020 r. przy użyciu zabiegów socjotechnicznych często wykorzystywały motyw pandemii COViD-19 w celu

[57] Art. 26 ust. 7 ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2020 r. poz. 1369).

[58] Art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. Dz.U. z 2022 r. poz. 261).

[59] Raporty o stanie bezpieczeństwa cyberprzestrzeni RP, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi, (dostęp: 14.02.2022 r.).

[60] Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2020 roku, Warszawa 2021, s. 9.

oddziaływania użytkowników sieci teleinformatycznych, czego przykładem jest chociażby stosowanie kampanii phishingowych, czy podszywanie się pod znane instytucje państwowe i podmioty, z których usług powszechnie korzysta społeczeństwo, np. Pocztę Polską[61].

Warto tutaj również wskazać na działania podejmowane w ramach Unii Europejskiej (dalej: UE) na rzecz przeciwdziałania i zwalczania cyberprzestępczości wśród państw członkowskich. W grudniu 2020 r. Komisja Europejska przedstawiła Strategię Unii Europejskiej w zakresie cyberbezpieczeństwa na cyfrową dekadę (dalej: Strategia UE)[62]. UE dostrzega zagrożenia wynikające z przenoszenia się części życia człowieka do przestrzeni wirtualnej, a więc do Internetu oraz systemów teleinformatycznych. Wskazuje w Strategii UE, że zapobieganie i zwalczanie cyberprzestępczości jest obecnie, a także będzie w przyszłości wyzwaniem dla organów unijnych chcących zapewnić bezpieczeństwo wewnętrzne UE. W tym celu niezbędne jest podejście wielosektorowe i multidyscyplinarne, obejmujące m.in. działania z zakresu prewencji, budowania świadomości i postępowania w sytuacjach kryzysowych, a przede wszystkim wypracowania ram prawnych w sposób umożliwiających efektywniejsze prowadzenie dochodzeń, a także powołanie grupy zadaniowej na szczeblu międzynarodowym, która zmierzyłaby się z wyzwaniami dotyczącymi *Dark Web*[63].

6. Wnioski

Rozwój nowych technologii przyniósł wiele korzyści, ale również i zagrożeń dla przeciętnych użytkowników Internetu. Przemiany cywilizacyjne, do jakich doszło na przestrzeni ostatnich dziesięcioleci, doprowadziły do rozwoju nowych form przestępczości, czego efektem było powstanie zjawiska cyberprzestępczości.

---

[61] *Ibidem*, s. 23–36.

[62] *Joint Communication to the European Parliament and the Council the EU's Cybersecurity Strategy for the Digital Decade*, (CELEX:52020JC0018), https://eur-lex.europa.eu/legal-content/ga/TXT/?uri=CELEX:52020JC0018 (dostęp: 12.02.2022 r.).

[63] Ł. Olszewski, *Unia Europejska wobec zapobiegania i zwalczania cyberprzestępczości – wybrane aspekty*, [w:] *Informacyjny wymiar bezpieczeństwa państw i jednostek*, red. W. Fehler, Siedlce 2021, s. 243–264.

Należy pamiętać, iż digitalizacja społeczeństwa doprowadziła do sytuacji, w której część życia jednostek przenosi się do przestrzeni wirtualnej. Nie każda jednostka pozostaje świadoma zagrożeń czyhających w świecie cyfrowym, dlatego kluczowa jest edukacja społeczeństwa. Niezbędne jest organizowanie szeroko zakrojonych kampanii medialnych i społecznych, które będą miały na celu uwrażliwianie i uświadamianie społeczeństwa na zagrożenia obecne w cyberprzestrzeni. M. Grzelak oraz K. Liedel zauważają, że zapewnienie bezpieczeństwa w cyberprzestrzeni nie będzie możliwe do osiągnięcia bez edukacji społeczeństwa co do istniejących zagrożeń w przestrzeni wirtualnej, ale i również odpowiedniego wyszkolenia specjalistów od bezpieczeństwa teleinformatycznego, a także pracowników aparatu państwowego, których rolą będzie ściganie przestępstw popełnianych w cyberprzestrzeni[64]. Zapewnienie odpowiedniej infrastruktury technicznej niezbędnej do ścigania przestępczości w przestrzeni cyfrowej jest kluczowym aspektem w jej zwalczaniu. Należy pochwalić dążenie władzy państwa polskiego do tworzenia specjalistycznych komórek działania organów ścigania ukierunkowanych na zwalczanie i wykrywanie cyberprzestępczości. Powstanie organów scentralizowanych, które będę zajmowały się przestępczością w cyberprzestrzeni wydaje się być rozwiązaniem, które pozwoli na odpowiednie skoordynowanie działań i środków podejmowanych w walce przeciwko cyberprzestępczości. Z uwagi na specyfikę sieci informatycznych i teleinformatycznych, a więc jej charakter zdalny i międzynarodowy powinny istnieć mechanizmy współpracy międzynarodowej ułatwiające ściganie sprawców tych przestępstw, a także współdzielenie się wiedzą dotyczącą sposób walki z cyberprzestępczością oraz dzieleniem się dobrymi praktykami w tym zakresie, co dostrzegła również Komisja Europejska. Wobec nieustającego rozwoju nowych technologii, przenoszenia się coraz to większej ilości obszarów życia człowieka do przestrzeni wirtualnej oraz upowszechnienia się portali społecznościowych, to wykorzystanie mediów społecznościowych w pracy śledczej polskich organów ścigania będzie coraz częstszą praktyką, wobec czego kluczowe będzie wypracowanie jednolitych mechanizmów pozwalających gromadzić

[64] M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu,* „Bezpieczeństwo Narodowe" 2012, nr 22, s. 138.

i zabezpieczać dowody z mediów społecznościowych do celów procesu karnego, a także przeciwdziałać przestępstwom popełnianym przy ich wykorzystaniu.

Bibliografia

Bielski K., *Cyberterroryzm – nowe zagrożenie bezpieczeństwa państwa w XXI wieku*, „Acta Politica Polonica" 2015, nr 4(34).

Buczkowski K., *Skuteczność zwalczania przestępstw przeciwko bezpieczeństwu elektronicznie przetwarzanej informacji na podstawie badań aktowych przestępstwa z art. 287 k.k.*, Warszawa 2015.

Ciszek P., *Cyberprzestępczość i jej zwalczanie z innej perspektywy*, [w:] *Przestępczość Teleinformatyczna*, red. J. Kosiński, Szczytno 2015.

Czyżak M., *Cyberprzestępczość a rozwój społeczeństwa informacyjnego*, „Ekonomiczne Problemy Usług" 2015, nr 117.

Definicja hasła „SOCMINT", [w:] *Vademecum bezpieczeństwa informacyjnego,* t. 2 N-T, Kraków 2020.

Gawkowski K., *Wpływy nowoczesnych technologii informatycznych na zdrowie i jakość życia*, „Technika, Informatyka, Inżynieria Bezpieczeństwa" 2018.

Główny Urząd Statystyczny, *Społeczeństwo informacyjne w Polsce w 2021 roku*, Warszawa 2021.

Grzelak M., Liedel K., *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe" 2012, nr 22.

Jedlińska R., *Problem przestępczości elektronicznej*, „Ekonomiczne Problemy Usług" 2017, nr 1(126), t. 2.

Krysiński Ł., *Identyfikacja cyberprzestępców*, „Prokuratura i Prawo" 2020, nr 2.

Lewulis P., *O rozgraniczeniu definicyjnym pomiędzy przestępczością „cyber" i „komputerową" dla celów praktycznych i badawczych*, „Prokuratura i Prawo" 2021, nr 3.

Ministerstwo Administracji i Cyfryzacji oraz Agencja Bezpieczeństwa Wewnętrznego, *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, Warszawa 2013.

Ministerstwo Cyfryzacji, *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*, Warszawa 2019.

Musiejko M., *Zjawisko cyberterroryzmu w polskim prawie karnym*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 8.

Oleksiewicz I., *Cyberterroryzm jako realne zagrożenie dla Polski*, „Rocznik Bezpieczeństwa Międzynarodowego" 2018, t. 12, nr 1.

Olszewski Ł., *Unia Europejska wobec zapobiegania i zwalczania cyberprzestępczości – wybrane aspekty*, [w:] *Informacyjny wymiar bezpieczeństwa państw i jednostek*, red. W. Fehler, Siedlce 2021.

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2020 roku, Warszawa 2021.

Saramak B., *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy*, Warszawa 2015.
Siwicki M., *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012, nr 7–8.
Skraba K., Strzałkowski I., *Media społecznościowe jako źródło dowodu w polskim procesie karnym. Badanie orzecznictwa sądów apelacyjnych i Sądu Najwyższego*, [w:] *Media społecznościowe w pracy organów ścigania*, red. P. Waszkiewicz, Warszawa 2021.
Stefanowicz M., *Cyberprzestępczość – próba diagnozy zjawiska*, „Kwartalnik Policyjny" 2017, nr 4.
Wasilewski J., *Cyberprzestępczość – wybrane aspekty prawnokarne i kryminalistyczne*, Białystok 2017.
Wasilewski J., *Przestępczość w cyberprzestrzeni – zagadnienia definicyjne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, nr 15.
Waszkiewicz P., Dębniak H., Rabczuk S., *Wybrane aspekty dopuszczalności dowodów pochodzących z mediów społecznościowych w postępowaniu karnym – ujęcie porównawcze*, [w:] *Media społecznościowe w pracy organów ścigania*, red. P. Waszkiewicz, Warszawa 2021.
Wróbel M., *Cyberprzestępczość w polskim systemie prawnym*, „Wiedza Obronna" 2014, nr 4.

Akty prawne

Joint Communication to the European Parliame't and the Council the EU's Cybersecurity Strategy for the Digital Decade, (CELEX:52020JC0018), https://eur-lex.europa.eu/legal-content/ga/TXT/?uri=CELEX:52020JC0018 (dostęp: 12.02.2022 r.).
Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz.U. z 2015 r. poz. 728).
Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz.U. z 2021 r. poz. 1882 z późn. zm.).
Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz.U. z 2021 r. poz. 1062).
Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. Dz.U. z 2021 r. poz. 2447).
Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j. Dz.U. z 2022 r. poz. 557).
Ustawa z dnia 30 marca 2002 r. Prawo własności przemysłowej (t.j. Dz.U. z 2021 r. poz. 324).
Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. Dz.U. z 2022 r. poz. 261).
Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (t.j. Dz.U. z 2021 r. poz. 2234).

Ustawa z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2020 r. poz. 1369).
Ustawa z dnia 17 grudnia 2021 r. o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości (Dz.U. z 2021 r. poz. 2447).
Uchwała nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2017–2022.
Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024.
The Stored Communications Act (SCA, 18 U.S.C., Chapter 121 §§ 2701–2712).

Netografia

About Meta, https://about.facebook.com/meta/ (dostęp: 3.03.2022 r.).
Facebook i organy ścigania, https://pl-pl.facebook.com/safety/groups/law (dostęp: 3.03.2022 r.).
Informacje dla organów ścigania, https://www.facebook.com/safety/groups/law/guidelines/ (dostęp: 3.03.2022 r.).
Informacje dla organów ścigania, https://faq.whatsapp.com/general/security-and-privacy/information-for-law-enforcement-authorities/?lang=pl (dostęp: 3.03.2022 r.).
Informacje dla przedstawicieli organów ścigania, https://pl-pl.facebook.com/help/instagram/494561080557017 (dostęp: 3.03.2022 r.).
Internetowe zgłaszanie dla organów ścigania, https://www.facebook.com/records/login/ (dostęp: 3.03.2022 r.).
Krajobraz cyberprzestępczości w dobie COViD-19, https://policja.pl/pol/aktualnosci/201028,Krajobraz-cyberprzestepczosci-w-dobie-COVID-19.html (dostęp: 3.03.2022 r.).
Law Enforcement Request, https://help.twitter.com/en/forms/law-enforcement (dostęp: 3.03.2022 r.).
Most popular social networks worldwide as of January 2022, ranked by number of monthly active users, https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (dostęp: 3.03.2022 r.).
Number of user data requests issued to Facebook from federal agencies and governments during 1st half 2021, by country, https://www.statista.com/statistics/287845/global-data-requests-from-facebook-by-federal-agencies-and-governments/ (dostęp: 3.03.2022 r.).
Polityka prywatności Facebook, https://www.facebook.com/about/privacy (dostęp: 3.03.2022 r.).

Powstanie Centralne Biuro Zwalczania Cyberprzestępczości, https://www.gov.pl/web/mswia/powstanie-centralne-biuro-zwalczania-cyberprzestepczosci (dostęp: 3.03.2022 r.).

Prezydent Andrzej Duda podpisał ustawę o powołaniu Centralnego Biura Zwalczania Cyberprzestępczości, https://www.gov.pl/web/mswia/prezydent-andrzej-duda-podpisal-ustawe-o-powolaniu-centralnego-biura-zwalczania-cyberprzestepczosci (dostęp: 3.03.2022 r.).

Rada Ministrów przyjęła projekt ustawy o powołaniu Centralnego Biura Zwalczania Cyberprzestępczości, https://www.gov.pl/web/mswia/rada-ministrow-przyjela-projekt-ustawy-o-powolaniu-centralnego-biura-zwalczania-cyberprzestepczosci (dostęp: 3.03.2022 r.).

Wskazówki dla organów ścigania, https://help.twitter.com/pl/rules-and-policies/twitter-law-enforcement-support (dostęp: 3.03.2022 r.).

Agata Wróbel

Perspektywy i zagrożenia dla telemedycyny w Polsce z punktu widzenia cyberbezpieczeństwa

1. Wprowadzenie

Telemedycyna w polskich realiach prawnych i ustrojowych miała swój okres intensywnego rozwoju zaraz po wybuchu pandemii COVID-19. Jak wiele innych dziedzin, także medycyna była zmuszona skoncentrować swoje funkcjonowanie wokół formy zdalnej lub hybrydowej. Co prawda, telemedycyna nie jest rozwiązaniem nowym dla świata – tak jak większość milowych wynalazków, było to początkowo rozwiązanie przeznaczone dla astronautów czy żołnierzy. Zalążki telemedycyny powstały w Polsce natomiast dopiero po 2000 r.[1] Rozpowszechnienie takiego typu usług drogą telekomunikacji znacznie poszerzyło możliwości korzystania z podstawowej opieki społecznej, zoptymalizowało ten proces i ułatwiło go wielu pacjentom[2]. Z drugiej jednak strony mówi się o wykluczeniu osób nieposługujących się sprawnie technologią, zagrożeniu dla wrażliwych danych lekarzy i pacjentów czy o lukach w infrastrukturze umożliwiającej tego typu usługi. Nad tematem telemedycyny można dyskutować na wielu płaszczyznach, na każdej z nich pojawiają się pewne wątpliwości i kontrowersje[3]. Szczególnie istotne jest ukazanie potrzeby zapewnienia odpowiednich szkoleń i procesów służących przygotowaniu personelu medycznego

[1] I. Wrześniewska-Wal, D. Hajdukiewicz, *Telemedycyna w Polsce – aspekty prawne, medyczne i etyczne*, „Studia Prawnoustrojowe" 2020, nr 50, *passim*.

[2] I. Iakovidis, P. Wilson, J.C. Healy, E-Health, Current Situation and Examples of Implemented and Beneficial E-Health Applications, „Studies in Health Technology and Informatics" 2004, nr 100, s. 230–237.

[3] Więcej na ten temat patrz: W.M. Maziarz, *Problemy rozwoju telemedycyny w Polsce*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego" 2010, nr 25, *passim*.

do świadczenia usług telemedycyny, a także pacjentów do umiejętnego czerpania korzyści z tychże usług.

2. Polska regulacja prawna

Analizę warto zacząć od zasygnalizowania heterogeniczności usług telemedycznych w Polsce. Działania te opierają się przede wszystkim na profilaktyce, diagnostyce i monitorowaniu stanu zdrowia[4], prowadzeniu e-dokumentacji i telerehabilitacji. Finansowane przez Narodowy Fundusz Zdrowia są na ten moment tylko nieliczne usługi, głównie telekonsylium kardiologiczne oraz telekonsylium geriatryczne[5]. Doktryna kategoryzuje nowoczesne technologie używane w medycynie na m.in. cyfrową medycynę (przełożenie tradycyjnej medycyny na cyberprzestrzeń, pojęcie zakresowo najszersze)[6], e-Zdrowie (pojęcie szersze od pojęcia „telemedycyny", obejmuje bowiem także e-administrację czy elektroniczną dokumentację), m-Zdrowie (praktyki zdrowotne z użyciem urządzeń mobilnych) czy informatykę medyczną (systemy zarządzania jednostkami oraz danymi pacjentów)[7]. W porządku prawnym brak jest definicji legalnej „telemedycyny" czy nawet szerzej pojętej „e-medycyny". W obiegu funkcjonują definicje opracowane przez stowarzyszenia, np. definicja Amerykańskiego Stowarzyszenia Telemedycznego: „telemedycyna jest formą wymiany informacji medycznych pomiędzy dwoma stronami,

[4] Więcej na temat możliwości telemedeycyny patrz: J. Barlow, D. Singh, S. Bayer, R. Curry, *What are the benefits of home telecare for frail elderly people and those with long-term conditions? A systematic review of the evidence*, „Journal of Telemedicine and Telecare" 2007, nr 13, s. 172–179.

[5] M. Malczewska, *Wydawanie orzeczeń po osobistym zbadaniu za pośrednictwem systemów teleinformatycznych lub systemów łączności*, [w:] *System Prawa Medycznego. Tom I. Pojęcie, źródła i zakres prawa medycznego*, red. R. Kubiak, L. Kubicki, E. Zielińska, Warszawa 2018, s. 807–810.

[6] A. Allen, M. Maheu, P. Whitten, *E-Health, Telehealth, and Telemedicine: A Guide to Startup and Success*, Jossey-Bass Health Series 2001, s. 27–28.

[7] Więcej na ten temat można zaleźć w dostępnym na platformie YouTube nagraniu Wirtualnej Katedry Etyki i Prawa, zebranie naukowe PNT #6: Prawo a telemedycyna w UE, referat B. Oręziaka (zebranie naukowe dostępne pod linkiem: https://www.youtube.com/watch?v=sKP24zH1d1A&t=1329s).

przebiegająca przy wykorzystaniu narzędzi telekomunikacyjnych, której celem jest poprawa stanu zdrowia pacjenta"[8]. Pośród czynności dokonywanych w ramach telemedycyny, Krajowa Izba Gospodarcza w raporcie „Uwarunkowania telemedycyny w Polsce" z 2016 r. wskazała: teleopiekę, telediagnostykę (w tym teleradiologię, teleEKG, KTG, EMG, teleendoskopię, teleUSG, telepatologię), telekonsultację, a nawet telezabiegi i teleoperacje[9] przy użyciu zdalnie sterowanego robota. Definicja WHO jest bardziej rozbudowana, zgodnie z nią telemedycyną jest:

> świadczenie usług opieki zdrowotnej, w których odległość jest czynnikiem krytycznym, przez wszystkich pracowników służby zdrowia wykorzystujących technologie informacyjne do wymiany ważnych informacji. profesjonalistów wykorzystujących technologie informacyjne i komunikacyjne do wymiany ważnych informacji do diagnozowania, leczenia i zapobiegania chorobom i urazom, badań i oceny oraz do kształcenia ustawicznego pracowników służby zdrowia, a wszystko to w interesie poprawy stanu zdrowia osób i ich społeczności[10].

W związku z brakiem normatywnej regulacji definicji „telemedycyny" pojawia się oczywisty problem w tym, gdzie zlokalizować tę dyscyplinę. Jak słusznie wskazuje G. Glanowski[11], możemy ją rozpatrywać jako alternatywną wobec standardowej medycyny albo jako kategorię zbiorczą dla nowych procedur medycznych wykorzystujących łączność na odległość i nowe technologie informatyczne. Podstawową regulacją prawną jest art. 42 ust. 1 ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty, zgodnie z którym:

---

[8] American Telemedicine Association, https://www.americantelemed.org/resource/why-telemedicine/ (dostęp: 6.07.2022 r.).

[9] Krajowa Izba Gospodarcza, *Raport Uwarunkowania Rozwoju Telemedycyny w Polsce. Potrzeby, bariery, korzyści, analiza rynku, rekomendacje*, wyd. 3, *passim*.

[10] WHO.3, *A health telematics policy in support of WHO's Health-For-All strategy for global health development: report of the WHO group consultation on health telematics*, 11–16 December, Geneva, 1997, Geneva 1998, *passim*.

[11] G. Glanowski, *Telemedycyna w świetle ustawy o zawodach lekarza i lekarza dentysty*, „Monitor Prawniczy" 2015, nr 18, s. 977.

> lekarz orzeka o stanie zdrowia określonej osoby po uprzednim, osobistym jej zbadaniu lub zbadaniu jej za pośrednictwem systemów teleinformatycznych lub systemów łączności, a także po analizie dostępnej dokumentacji medycznej tej osoby[12].

Regulację znajdziemy też w ustawie o działalności leczniczej, gdzie art. 3 ust. 1 określa iż:

> Działalność lecznicza polega na udzielaniu świadczeń zdrowotnych. Świadczenia te mogą być udzielane za pośrednictwem systemów teleinformatycznych lub systemów łączności[13].

Analogiczne odniesienie znajdziemy w art. 11 ust. 1 ustawy z dnia 15 lipca 2011 r. o zawodach pielęgniarki i położnej:

> pielęgniarka i położna wykonują zawód, z należytą starannością, zgodnie z zasadami etyki zawodowej, poszanowaniem praw pacjenta, dbałością o jego bezpieczeństwo, wykorzystując wskazania aktualnej wiedzy medycznej oraz pośrednictwo systemów teleinformatycznych lub systemów łączności[14].

Niestety prawo pozostaje lakoniczne co do rodzajów czy konkretnych propozycji systemów, za pomocą których powinno się przeprowadzać świadczenia telemedyczne, a „decyzja w tym zakresie pozostawiona jest zasadniczo świadczeniodawcy, co znacząco go obciąża i przerzuca na niego ryzyko wystąpienia ewentualnych błędów czy naruszeń"[15].

---

[12] Ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (Dz.U. z 1997 r. Nr 28, poz. 152 z późn. zm.).

[13] Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz.U. z 2011 r. Nr 112, poz. 654 z późn. zm.).

[14] Ustawa z dnia 15 lipca 2011 r. o zawodach pielęgniarki i położnej (Dz.U. z 2011 r. Nr 174, poz. 1039 z późn. zm.).

[15] M. Czaplińska, M. Sakowska-Baryła, *Telemedycyna i teleporady w dobie pandemii – aspekty prawne i organizacyjne*, „Monitor Prawniczy" 2022, nr 12, *passim*.

Telemedycyna jest jednak potencjalną bazą rozwoju dla polskiej medycyny. Przeszkodą w pełnym wykorzystywaniu jej efektywności są wciąż luki legislacyjne. Temat jest dla polskiego prawodawcy stosunkowo nowy, jednak warto zacząć pracę nad taką regulacją. Telemedycyna nie zastąpi nigdy standardowej formy medycyny, ale z pewnością może stworzyć komfortowe warunki do monitorowania i profilaktyki[16], a przede wszystkim też odciążyć medyków i rozładować natężone kolejki do specjalistów, pozostawiając miejsca w kolejkach dla pacjentów wymagających takiej wizyty.

3. Czy telemedycyna jest skuteczna?

Kwestią sporną jest to, jak bardzo rzetelnie można zdalnie ustalić rzeczywisty stan zdrowia i zdiagnozować problemy zdrowotne pacjenta i w ilu przypadkach rzeczywiście można pomóc pacjentowi, a w ilu przypadkach jedynie dać mu ogólne zalecenia. Przykładowo można przytoczyć wyrok WSA w Krakowie, który rozstrzygał kwestię skargi na indywidualną interpretację Ministra Finansów w przedmiocie podatku od towarów i usług. Wnioskodawca, będący podmiotem leczniczym w rozumieniu ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej, zaskarżył interpretację podatkową, w której Minister Finansów uznał, że odpłatne świadczenia usług telemedycyny, które zamierzał zacząć świadczyć wnioskodawca, nie będą zwolnione z podatku VAT[17]. Bowiem z ustawy o podatkach od towarów i usług jednoznacznie wynika, że dla zastosowania zwolnienia od VAT istotny jest cel wykonywanych świadczeń. Ze zwolnienia będą generalnie korzystać tylko te czynności, które mają charakter diagnostyczny lub terapeutyczny (leczniczy). Jeśli świadczenie nie będzie służyć profilaktyce, zachowaniu, ratowaniu, przywracaniu i poprawie zdrowia,

[16] Więcej na temat sposobów wykorzystania telemedycyny patrz: *Market study on telemedicine*, Luxembourg: Publications Office of the European Union, 20, s. 45–46.

[17] A. Wesołowska, *Zwolnienie z VAT dla usług medycznych na odległość/przez telefon. Glosa do wyroku TS z dnia 5 marca 2020 r., C-48/19*, LEX/el. 2022, teza trzecia, https://https-sip-lex-pl.pulpit.uksw.edu.pl/#/publication/386245691/wesolowska-agnieszka-zwolnienie-z-vat-dla-uslug-medycznych-na-odleglosc-przez-telefon-glosa-do…?cm=URELATIONS (dostęp: 15.08.2022 r.).

to wówczas nie będzie objęte zwolnieniem podatkowym. Sąd przychylił się do prawidłowości interpretacji odmawiającej zwolnienia. Jak argumentowano w orzeczeniu:

> usługi telemedycyny, świadczone za pośrednictwem Internetu są w istocie udzielaniem porad, wykładów, stanowią wskazówki co do sposobu wykonywania ćwiczeń, ich oceny i monitorowania, konsultacje w zakresie edukacji zdrowotnej. Tych działań nie można uznać za opiekę medyczną. Usługa w zakresie opieki medycznej wymaga przynajmniej, co wynika nawet z zasad doświadczenia, rzetelnego ustalenia, że czy jest konieczna dla osiągnięcia zamierzonego celu. Niezbędna jest więc możliwość oceny stanu zdrowia pacjenta w celu postawienia prawidłowej diagnozy oraz zaordynowania odpowiedniego, dostosowanego do wymogów konkretnej osoby postępowania terapeutycznego. Usługi dokonywane na podstawie otrzymanych od klientów informacji, nie zawsze będą oparte na wiarygodnych, konkretnych danych, które umożliwiają właściwą opiekę medyczną. Utrwalanie prawidłowych wzorców postępowania nie może być utożsamiane z opieką medyczną[18].

Z powyższego przypadku można wysnuć wnioski, że w istocie efektywność telemedycyny zależy od tego, w jakim zakresie podmiot zobowiąże się ją wykonywać i jaki jest cel wykonywania usług. W kwestii zwolnienia z podatku VAT pojawiały się także interpretacje i wyroki pozytywne, szczególny wpływ na to miała popularyzacja telemedycyny w okresie pandemii, gdzie okoliczności zmusiły wiele podmiotów do pełnego działania w takiej formie. Przede wszystkim jednak, nadal nie jest jasne jakie kwalifikacje zawodowe powinny mieć osoby świadczące telefoniczne konsultacje medyczne, aby świadczone usługi mogły korzystać ze zwolnienia z VAT. TSUE w wyroku w sprawie C-48/19[19] lakonicznie i niejednoznacznie stwierdził, że mają to być kwalifikacje

[18] Wyrok WSA w Krakowie z dnia 22 czerwca 2015 r., I SA/Kr 721/15, LEX nr 1813436.

[19] Wyrok TSUE z dnia 5 marca 2020 r., C-48/19, *X-GmbH v. Finanzamt Z.*, LEX nr 2797480.

gwarantujące „odpowiedni poziom świadczonych usług"[20]. Jest to stwierdzenie dalece nieostre, przez co nadal interpretowane na różne sposoby.

Nie mniej, funkcjonują usługi, które z pewnością ułatwiają leczenie, diagnozowanie i monitorowanie stanu pacjenta na odległość. Wiele ma w tym temacie do zaproponowania telekardiologia czy teleonkologia, gdzie pacjent powinien być pod stałym nadzorem lekarza. Taka pomoc medyczna jest realizowana m.in. przez Mobile Holter, który dyskretniej i mniej inwazyjnie monitoruje stan pacjenta, nawet podczas snu, Lifenet („Sieć Życia"), który zapewnia sprawny przepływ informacji o stanie zdrowia w trakcie transportowania pacjenta w stanie krytycznym czy też nowatorska telerehabilitacja kardiologiczna, polegająca na przeprowadzaniu cykli ćwiczeń, badań EKG i odpoczynków w domu pacjenta z jednoczesnym połączeniem telefonicznym z medykiem[21]. Jak widzimy, telemedycyna pomaga głównie w przypadkach, gdzie pacjent wymaga monitorowania. Dzięki takim rozwiązaniom chory nie musi uzależniać się od fizycznych wizyt u lekarza. Telemedycyna ma także ogromne znaczenie w diabetologii. U pacjentów poddanych insulinoterapii konieczne jest dostosowywanie dawek insuliny do poziomu glikemii, ale wizyta bezpośrednia wymaga czasu i często wiąże się z koniecznością nieobecności w pracy, co może być problemem dla osoby zawodowo aktywnej, zwłaszcza o niskim statusie ekonomicznym[22]. Innym przykładem jest kamizelka kardiologiczna, która rejestruje zapis EKG i jednocześnie umożliwia prowadzenie wszystkich codziennych czynności.

Powstały platformy i aplikacje, dzięki którym możemy weryfikować i zarządzać swoim leczeniem oraz załatwiać sprawy w NFZ, np. Elektroniczna Weryfikacja Uprawnień Świadczeniobiorców (eWUŚ), czyli system umożliwiający natychmiastowe potwierdzenie prawa pacjenta do świadczeń opieki zdrowotnej finansowanych ze środków publicznych, Internetowe Konto Pacjenta (IKP) w którym można rejestrować się na wizyty, realizować recepty i kontaktować się

[20] R. Bujalski, *Product manager LEX Prawo Europejskie, Zwolnienie z VAT telemedycyny*, LEX/el. 2020.

[21] A. Kubicka-Mącznik, J. Makuch, *Korzyści wynikające ze stosowania rozwiązań telemedycznych w świetle badań naukowych – wybrane zagadnienia*, „Choroby Serca i Naczyń" 2017, nr 14(1), s. 9–14.

[22] M. Długaszek, J. Gumprecht, S. Berdzik-Kalarus, A. Chodkowski, K. Nabrdalik, *Telemedicine in response to challenges of modern diabetology*, „Clin Diabet" 2016, nr 5(1), s. 22–25.

z placówką podstawowej opieki zdrowotnej, czy system e-ZLA (elektroniczne zlecenie lekarskie), umożliwiający szybsze uzyskanie zwolnienia lekarskiego. Skuteczność telemedycyny odzwierciedla się nie tylkow relacji chory–lekarz, ale także w relacjach środowiska medycznego[23]. Telemedycyna to szybki przepływ wiedzy i informacji, standaryzacja usług w sektorze e-zdrowia, wyższy poziom wykształcenia lekarzy pierwszego kontaktu i jednostek świadczących usługi podstawowej opieki zdrowotnej.

Przy ocenie efektywności telemedycyny należałoby brać pod uwagę fakt, że polskie społeczeństwo się starzeje[24]. W Polsce po 1983 r. utrzymuje się niski odsetek urodzeń, azmniejszenie udziałów dzieci i dorosłych oznacza wzrost odsetka ludzi starszych w wieku 65 lat i więcej. Zgodnie z danymi GUS w prognozie na 2050 r. udział osób starszych przekroczy 30% na obszarach wiejskich, natomiast w miastach zbliży się do 35%[25]. Oznacza to, że zapotrzebowanie na opiekę i usługi medyczne będzie coraz większe. Z tego powodu rozwój telemedycyny wydaje się być jedynym słusznym rozwiązaniem. Trudno mówić tu o wykluczeniu z powodu braku umiejętności posługiwania się technologią[26].W Polsce spośród osób, które w ciągu ostatnich 3 miesięcy 2021 r. korzystały z Internetu, 98,0% używało go regularnie. Odsetek osób, które łączyły się z Internetem codziennie lub prawie codziennie, wyniósł 86,3%, a korzystających z Internetu rzadziej niż raz w tygodniu – 2,0%[27]. Wyszczególniając w tym osoby starsze, odsetek osób w wieku 65–74 lata, regularnie korzystających z Internetu, wzrósł w latach 2017–2021 aż o 19,9% (z 26,0% w 2017 r. do 45,9% w 2021 r.)[28]. Kolejne pokolenia będą coraz sprawniej posługiwać się technologią ze względu

[23] T. Karkowski, *Telemedycyna i eHealth w sektorze opieki zdrowotnej*, LEX/el. 2022.

[24] GUS, *Sytuacja demograficzna osób starszych i konsekwencje starzenia się ludności Polski w świetle prognozy na lata 2014–2050*, Warszawa 2014, https://stat.gov.pl/obszary-tematyczne/ludnosc/ludnosc/sytuacja-demograficzna-osob-starszych-i-konsekwencje-starzenia-sie-ludnosci-polski-w-swietle-prognozy-na-lata-2014-2050,18,1.html (dostęp: 26.07.2022 r.).

[25] GUS, *Prognoza ludności na lata 2014–2050*, Warszawa 2014.

[26] Szersza analiza na temat wykluczenia cyfrowego patrz: B. Oręziak, *Telemedycyna a konstytucyjne prawo do opieki zdrowotnej w kontekście wykluczenia cyfrowego*, „Zeszyty Prawnicze UKSW" 2018, nr 18.1, s. 117–141.

[27] Baza danych Eurostatu, dane z 2019 r.

[28] GUS, *Społeczeństwo informacyjne w Polsce w 2021 r.*, https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2021-roku,1,15.html (dostęp: 26.07.2022 r.).

na jej rosnącą powszechność i łatwą dostępność. Zjawisko *generation gap* zaciera się coraz bardziej z kolejnymi pokoleniami i właściwym jest sądzić, że w perspektywie czasu kwestia wykluczenia cyfrowego nie będzie stanowić problemu.

4. Teleporada – problemy prawne

Kwestię teleporad reguluje rozporządzenie Ministra Zdrowia z dnia 12 sierpnia 2020 r. w sprawie standardu organizacyjnego teleporady w ramach podstawowej opieki zdrowotnej. Akt ten reguluje definicję „teleporady" jako świadczenie zdrowotne udzielane na odległość przy użyciu systemów teleinformatycznych lub systemów łączności. Zgodnie z rozporządzeniem, osobami uprawnionymi do udzielania teleporad są lekarz, pielęgniarka lub położna. Zakres podmiotowy rozporządzenia wyłącza możliwość udzielania teleporady dzieciom do ukończenia 6. roku życia, a także pacjentom powyżej 65. roku życia, tu pojawia się pierwszy problem. Z bieżącego uregulowania wynika, że pacjenci w tych grupach wiekowych (czy też, biorąc pod uwagę grupę dzieci do lat 6 – ich opiekunowie) są wyłączeni z możliwości korzystania z teleporad bez uwzględnienia swojej woli. Kryterium wieku jest kryterium formalistycznym, w większym stopniu administracyjnym niż medycznym, a może się przecież zdarzyć, że pacjent będzie wolał skorzystać z teleporady, np. ze względu na wolę nienarażania się na przebywanie wśród innych chorych. Z rozporządzenia wynika jednak możliwość skorzystania z usług teleporady dla celów obejmujących uzyskanie recepty niezbędnej do kontynuacji leczenia czy uzyskania zalecenia na zaopatrzenie w wyroby medyczne jako kontynuację, oraz związanych z wydaniem zaświadczeń, niewymagających bezpośredniej wizyty pacjenta w przychodni. Co do małoletnich do 6. roku życia także mamy pewne wyjątki. Bowiem z mocy art. 17 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, pozostaje prawo opiekuna prawnego do zgody lub sprzeciwu[29]. Wynika to z hierarchii

[29] T. Rek, *Zasady interpretacji*, [w:] *Dziecko – pacjent i świadczeniobiorca*, red. M. Dercz, H. Izdebski, Warszawa 2015, *passim*.

aktów prawnych, ustawa bowiem jest aktem wyższej rangi od rozporządzenia[30]. Mimo to arbitralne określenie formy świadczenia usług medycznych dla pewnej grupy społecznej może być postrzegane jako naruszenie praw pacjenta i prawa obywatela do samodecydowania[31].

Innym problemem może okazać się sama w sobie dostępność teleusługi. Jedną z takich sytuacji rozpatrywał Wojewódzki Sąd Administracyjny w Warszawie, gdzie pewna przychodnia pełniła swoje obowiązki świadczenia teleporady jedynie formalnie. Jak czytamy w stanie faktycznym:

> zdaniem RPP, podmiot leczniczy wykonuje wprawdzie telefoniczną rejestrację pacjentów, niemniej jednak nie sposób jest się telefonicznie zarejestrować na świadczenia zdrowotne realizowane w Przychodni, co potwierdzają działania weryfikacyjne przeprowadzone przez organ w dniach od 11 do 15 stycznia 2021 r. Wskazany jako właściwy do rejestracji telefonicznej numer telefonu jest zajęty bądź pojawia się komunikat o wewnętrznych problemach uniemożliwiających dokonanie rejestracji. Tylko w jednym przypadku na 15 wykonanych prób połączeń (w różnych godzinach, w różnych dniach), udało się skutecznie uzyskać połączenie z pracownikiem rejestracji. Natomiast zdaniem RPP, możliwość rejestracji telefonicznej musi mieć charakter faktyczny, a nie tylko formalny[32].

Problemy tej natury często wiążą się z ubogą infrastrukturą teleinformatyczną lub brakiem wystarczającej liczby personelu medycznego. Te luki w szczególny sposób ukazała nam pandemia. W sytuacjach kryzysowych ujawnia się rzeczywisty deficyt zasobów, narzędzi i błędy w strukturach organizacyjnych. Cytując wypowiedź dr Małgorzaty Gałązki-Sobotki z okresu pandemii:

---

[30] A. Sieńko, *Obowiązki placówki medycznej w związku udzielaniem świadczeń dzieciom do 6 r.ż.*, *passim*.

[31] J.P. Olejarczyk, M. Young, *Patient Rights And Ethics, Treasure Island* (*FL*), StatPearls Publishing 2022, https://www.ncbi.nlm.nih.gov/books/NBK538279/ (dostęp: 12.07.2022 r.).

[32] Wyrok WSA w Warszawie z dnia 10 sierpnia 2021 r., V SA/Wa 2536/21, LEX nr 3311108.

> w normalnej sytuacji wprost wiążemy je [błędy] z brakiem odpowiedniego finansowania, ale – paradoksalnie – ostatnie miesiące ukazały, że pod ciężarem pandemii uginają się także systemy, które od lat traktowaliśmy jako wzorcowe, również pod względem poziomu inwestycji w ochronę zdrowia. Za wcześnie mówić o wygranych i przegranych, ale nie ma wątpliwości, że właśnie przechodzimy jeden z najważniejszych sprawdzianów zarówno w obszarze opieki zdrowotnej, jak i polityk kryzysowych państw. Bilans strat, mierzony ludzkim zdrowiem i życiem, nie może być niczym kompensowany i musi zmuszać do konstruktywnych zmian, wyciągania wniosków na przyszłość[33].

Jak zostało wskazane w powyższych wywodach, na jakość opieki zdrowotnej wpływa wiele czynników, od liczby i poziomu wykształcenia personelu, przez procesy leczenia, aż po jakość samego wyniku i rezultatów oraz ogólną liczbę zachorowań czy śmiertelności. Dla weryfikacji jakości świadczonych usług często wprowadza się standaryzację i weryfikację jakości zgodnie z normami Międzynarodowej Organizacji Normalizacyjnej (ISO)[34]. Zakłady opieki zdrowotnej poddają się standaryzacji norm dla utrzymywania i polepszania jakości świadczonych usług. W Polsce placówki medyczne najczęściej zewnętrznie weryfikują zgodność z normą ISO 9001[35]. Normę tę mogą stosować wszystkie organizacje, niezależnie od ich wielkości i rodzaju. Certyfikat systemu ISO 9001 jest potwierdzeniem, że organizacja posiada odpowiednie procedury zarządzania jakością i stale je doskonali. Określa ona system prowadzenia dokumentacji, poziomuje jakość świadczonych usług, określa pożądany poziom efektywności organizacji i jest zorientowana na beneficjenta.

---

[33] M. Gałązka-Sobotka, *Po pandemii trzeba utrzymać szybkie tempo realizacji projektów e-zdrowia, opinia dla portalu medycznego*, „Puls medyczny",https://pulsmedycyny.pl/po-pandemii-trzeba-utrzymac-szybkie-tempo-realizacji-projektow-e-zdrowia-opinia-987135 (dostęp: 12.07.2022 r.).

[34] M. Kwiatkowska, *Wdrożenie systemów zarządzania jakością i bezpieczeństwem w ochronie zdrowia drogą do zmniejszenia liczby zdarzeń niepożądanych w szpitalach i POZ*, [w:] *Zdarzenia niepożądane w lecznictwie szpitalnym i podstawowej opiece zdrowotnej*, Warszawa 2020, *passim*.

[35] A. Czerw, U. Religion, *Systemy oceny jakości w ochronie zdrowia*, „Problemy Zarządzania", t. 10, nr 2(37), s. 195–210, https://www.researchgate.net/publication/310475467_Systemy_oceny_jakosci_w_ochronie_zdrowia (dostęp: 1.08.2022 r.).

5. E-recepty – problemy prawne

E-recepta ma status dokumentu elektronicznego. Łączy się z Internetowym Kontem Pacjenta (IKP), gdzie pacjent może w zdalny sposób weryfikować informacje dotyczące jego wizyt, recept i ostatnich badań. IKP ułatwia administracyjną ścieżkę komunikacji z podmiotem medycznym w sposób zdalny. Elektroniczna recepta usprawnia proces uzyskania leków[36], ale przede wszystkim daje pewność, że przepisany lek będzie prawidłowy, ponieważ zawsze jest czytelna. Równie istotna jest możliwość realizowania w różnym czasie kilku leków przepisanych na jednej recepcie, co pozytywnie wpływa na proces protekcji farmakoterapii pacjenta uniemożliwiając wydanie leku po raz kolejny przez pomyłkę[37]. Obecnie standaryzuje się elektroniczną formę recept jako formę docelową. Zgodnie z art. 56 ust. 2 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, recepty w postaci papierowej mogły być wystawiane tylko do dnia 7 stycznia 2020 r. Przepisy natomiast nie przewidują kar dla lekarzy, którzy mimo tego obowiązku wciąż wystawiają receptę w postaci papierowej. Nad receptami elektronicznymi wciąż przeprowadzany jest proces udoskonalania i legislacyjnej weryfikacji przyjętych rozwiązań. Świadczą o tym zmiany z 2021 r., kiedy to 1 stycznia 2021 r. weszło w życie rozporządzenie Ministra Zdrowia z dnia 23 grudnia 2020 r. w sprawie recept. Rozporządzenie przyjęło zmiany w delegacji ustawowej rozszerzającej zakres regulacji o przepisy związane z realizacją recepty transgranicznej w postaci elektronicznej wystawionej w innym państwie członkowskim UE lub EFTA. Istotna i bardzo praktyczna zmiana pojawiła się również w kwestii zasad liczenia obowiązywania terminów realizacji recepty papierowej. Wcześniej termin ważności recepty był liczony dla każdego produktu z recepty osobno. Po zmianach został wprowadzony obowiązek umieszczania na jednej recepcie jedynie produktów, które mają taki sam termin realizacji[38].

---

[36] A. Twarowski, *Wpływ ustawy o funkcjonowaniu ochrony zdrowia w związku z epidemią COVID-19 na świadczeniodawców – informatyzacja ochrony zdrowia, Komentarz praktyczny*, LEX/el. 2020, *passim*.

[37] K. Urban, E. Warmińska-Friberg, *E-recepty w praktyce funkcjonowania podmiotów leczniczych*, LEX/el. 2018.

[38] K. Urban, E. Warmińska-Friberg, *Zmiany w wystawianiu i realizacji recept w 2021 r.*, LEX/el. 2021.

6. Cyberbezpieczeństwo a telemedycyna

Kluczowym problemem dziedziny telemedycyny jest bezpieczeństwo przechowywania i przetwarzania wrażliwych danych pacjenta, które są niezbędne do udzielania świadczeń zdrowotnych. Cyberprzestępczość przybiera różne formy, jej celem zwykle jest pozyskanie danych personalnych, które cyberprzestępca wykorzystuje do różnych celów. Z raportu OSOZ Polska na rok 2022 wynika, że w 2020 r. ofiarą hakerów padło ok. 18 mln kartotek pacjentów, co stanowi wzrost o 470% w odniesieniu do 2019 r.[39] Cyberataki mogą zagrażać bezpośrednio życiu pacjenta. Paraliż pracy systemów placówek medycznych wywołany przez hakera może bowiem zadecydować o udzieleniu lub nieudzieleniu pomocy pacjentowi wymagającemu natychmiastowej opieki medycznej czy hospitalizacji. Przestępcy mogą mieć na celu wymuszenie okupu, kradzież dokumentacji medycznej czy własności intelektualnej, zdarzają się jednak także ataki, które mają na celu ukazanie słabości systemów teleinformatycznych państwa dla podważenia zaufania publicznego i wprowadzenia w społeczeństwie poczucia niepewności. Podstawową i najważniejszą regulację w polskim systemie prawnym w tej kwestii stanowi ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych[40]. Zgodnie z jednym z wymogów ustanowionych w RODO[41] dane osobowe muszą być przetwarzane za pomocą odpowiednich środków technicznych i organizacyjnych w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym

[39] Raport czasopisma OSOZ Polska z 2022 pt. „Bezpieczeństwo danych w placówkach ochrony zdrowia", https://blog.osoz.pl/wideo-jak-wzmocnic-ochrone-przed-cyberatakami/ (dostęp: 1.08.2022 r.).

[40] Ustawa służy stosowaniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych); ustawa wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającą decyzję ramową Rady 2008/977/WSiSW.

[41] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (*General Data Protection Regulation*).

ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem[42]. Fundamentalny jest tu System Zarządzania Bezpieczeństwem Informacji, czyli strategia działania w zakresie zapewniania właściwej ochrony informacji poufnych[43]. Informuje on w jaki sposób raportować o incydentach bezpieczeństwa i jak zarządzać bezpieczeństwem informacji. W tych kwestiach warto wspomnieć o prawach pacjenta, w szczególności o prawie do poszanowania intymności i godności pacjenta[44]. Istota tego prawa obejmuje stworzenie warunków do rozmowy pacjenta z personelem medycznym na osobności, jak i przyjęcia każdego z pacjentów na wizytę pojedynczo. Problem ukazuje się w braku świadomości pacjenta o tym, że podczas usług telemedycznych on także powinien dbać o bezpieczeństwo swoich danych, co można zauważyć w nastawieniu społeczeństwa do teleporad. Teleporada umożliwia odbycie wizyty w każdym miejscu, z pewnością mogą zdarzyć się sytuacje, w których pacjent odbywa teleporadę w tramwaju czy na przystanku. W celu weryfikacji podaje przez telefon wszystkie swoje dane osobowe i nawet nie zdaje sobie sprawy z tego, że któraś z przypadkowo słyszących to osób może wykorzystać pozyskane, nawet przez przypadek, informacje. Brak świadomości i odpowiedniego wykształcenia jest czynnikiem hamującym rozwój technologii teleinformatycznych, co zwraca uwagę na istotnie szczególną rolę profilaktyki i edukacji[45]. Ważne jest też uświadamianie i doszkalanie samego personelu medycznego, by zwiększać jego wiedzę na temat prawidłowej reakcji w przypadku cyberataku. Warto też zadbać o czynności tak podstawowe jak wprowadzanie segmentacji sieci, zapewnianie skutecznych sposobów tworzenia kopii zapasowych i przywracania systemu czy zgłoszenie ataku do odpowiednich jednostek[46].

[42] Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679, Grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych.

[43] Rekomendacje centrum systemów informacyjnych ochrony zdrowia w zakresie bezpieczeństwa oraz rozwiązań technologicznych stosowanych podczas przetwarzania dokumentacji medycznej w postaci elektronicznej.

[44] Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta.

[45] S. Waseh, A.P. Dicker, *Telemedicine Training in Undergraduate Medical Education: Mixed-Methods Review*, JMIR Med Educ 2019, nr 5(1), *passim*.

[46] Przykładowe wytyczne dotyczące systemów bezpieczeństwa w ochronie zdrowia przygotowało Centrum e-Zdrowia, patrz: Plan działania w zakresie cyberbezpieczeństwa

Modele ataków i sposoby cyberprzestępców wciąż ewoluują, jednak można wyróżnić dwa pojawiające się często schematy. Pierwszy z nich jest przeprowadzany przez *ransomware*, czyli oprogramowanie, które ogranicza dostęp do danych i systemów komputera, jednocześnie wymagając zapłacenia okupu by te systemy odblokować. Zainfekować komputer można choćby przez wiadomość phishingową, zawierającą link do oprogramowania. Nieuświadomiony personel medyczny z wysokim prawdopodobieństwem nie zobaczy nic podejrzanego w takiej wiadomości i kliknie link, tym samym dając hakerowi dostęp do zdalnego pulpitu lub instalując oprogramowanie. Zaszyfrowane pliki paraliżują pracę jednostki medycznej realnie zagrażając życiu lub zdrowiu pacjentów. Jeśli jednostka jest dobrze zabezpieczona, możliwe będzie odzyskanie działania systemu przez kopie zapasowe. Jeżeli jednak jednostka jest podatna na ataki i brak jest przeszkolenia personelu oraz odpowiednich systemów bezpieczeństwa danych – możliwe jest, że okup zostanie opłacony. Nie ma jednak żadnej pewności, że ofiara otrzyma dane do deszyfrowania, ani tym bardziej nie ma gwarancji, że atak się nie powtórzy. Drugi model opiera się na podwójnym wymuszeniu. Grupa przestępcza doprowadza do szeregu ataków poprzedzających atak właściwy. Uprzednia eksfiltracja danych sugeruje, że te dane są celem ataku, tymczasem po serii kradzieży danych systemy są infekowane i blokowane przez *ransomware*[47]. Ten model jest bardziej niebezpieczny[48] ze względu na to, że poza blokadą i wymuszeniem okupu przestępca dysponuje jeszcze danymi uzyskanymi w pierwszych atakach i istnieje ryzyko spieniężenia tych danych na czarnym rynku.

w ochronie zdrowia, https://ezdrowie.gov.pl/portal/artykul/zestaw-rekomendacji-w-zakresie-cyberbezpieczenstwa-w-ochronie-zdrowia (dostęp: 1.08.2022 r.).

[47] M. Patil, *A brief study of Wannacry Threat: Ransomware Attack*, „International Journal of Advanced Research in Computer Science" 2017, vol. 8, *passim*.

[48] S. Song, B. Kim, S. Lee, *The Effective Ransomware Prevention Technique Using Process Monitoring on Android Platform*, „Hindawi Publishing Corporation Mobile Information Systems" 2016, s. 3–7.

7. Wnioski

Telemedycyna ma wiele do zaoferowania, jednak jak za każdym rewolucyjnym rozwiązaniem, tu także pojawiają się pasma zagrożeń. Jak zostało wskazane powyżej, cyberprzestępczość w zakresie telemedycyny jest dla cyberprzestępców łupem niezwykle lukratywnym, ze względu na niską wykrywalność tego typu naruszeń bezpieczeństwa. Z tego powodu niezwykle ważne jest ciągłe ulepszanie i kontrolowanie systemów bezpieczeństwa i przeprowadzanie testów na aktualnie eksploatowanych urządzeniach i systemach. Jako że większość ataków opiera się na powtarzalnym schemacie wykorzystania braku świadomości osoby „z wewnątrz" danej organizacji, zwiększeniu bezpieczeństwa mogą służyć testy socjotechniczne i próby phishingowe. Takie audyty przeprowadzają zewnętrzne podmioty, a próba polega na przygotowaniu danego scenariusza ataku, przeprowadzeniu go na danej jednostce i przygotowaniu statystyk podatności pracowników. Test może obejmować kontakt mailowy z próbą pozyskania danych do logowania, próbą aktywowania złośliwych linków i załączników. Co więcej próba może obejmować podszycie się pod konkretną osobę lub instytucję czy stworzenie fikcyjnego podmiotu w celu nakłonienia do określonych działań. Test bezpieczeństwa może stanowić też rekonesans informacyjny (OSINT – *open-source intelligence*, tzw. biały wywiad). Z informacji ogólnodostępnych można bowiem wyselekcjonować informacje, które ułatwiają sprofilowanie ataku. Można sądzić, że takie audyty przyczyniłyby się znacząco do zwiększenia poziomu bezpieczeństwa poprzez natężenie świadomości personelu. Jednocześnie należy pamiętać o implementacji szkoleń personelu, obejmujących:

1/ uświadomienie warietyzacji i ewaluacji technik działania cyberprzestępców,
2/ wskazanie prawidłowego sposobu reagowania na zaistniałe naruszenia bezpieczeństwa,
3/ ukazanie istotnej roli tworzenia kopii zapasowych,
4/ uświadomienie w kontekście selekcjonowania informacji publikowanych w sieci.

Co więcej, w związku z brakiem dedykowanego systemu do świadczenia usług telemedycznych, wskazanym byłoby działanie w kierunku stworzenia

wiarygodnego systemu, którego działanie byłoby jednolite dla placówek w całym kraju. Droga do stworzenia takiej technologii naturalnie nie jest rzeczą nieskomplikowaną. Zwiększenie bezpieczeństwa można zapewnić poprzez odizolowanie od sieci systemów z dostępem do wrażliwych danych pacjentów, tworząc scentralizowany system zarządzania treścią z automatyczną synchronizacją danych. Taki system przesyłałby zaktualizowane treści między centralą a poszczególnymi jednostkami medycznymi. Kontakt między placówkami powinien być zapewniony przez wirtualną sieć prywatną (VPN – *virtual private network*), tworząc tym samym wirtualny tunel prywatny do synchronizacji danych odizolowany od sieci. Przesyłane dane powinny być jednocześnie opatrzone hasłem czy zabezpieczeniami biometrycznymi. Nie można pomijać także konieczności zaimplementowania skutecznych rozwiązań technicznych do tworzenia kopii zapasowych celem odzyskania danych w sytuacji kryzysowej. Stworzenie bazy do systemu teleinformatycznego dałoby ponadto możliwości do jego modyfikacji poprzez dodawanie funkcjonalności, zapewniających np. uefektywnienie wcześniej wspomnianej wymiany informacji między medykami, co niewątpliwie przyczyniłoby się do rozwoju i rozpowszechniania nowych rozwiązań w dziedzinie medycyny.

Bibliografia

Allen A., Maheu M., Whitten P., *E-Health, Telehealth, and Telemedicine: A Guide to Startup and Success*, Jossey-Bass Health Series 2001.

Barlow J., Singh D., Bayer S., Curry R., *What are the benefits of home telecare for frail elderly people and those with long-term conditions? A systematic review of the evidence*, „Journal of Telemedicine and Telecare" 2007, nr 13.

Bujalski R., *Product manager LEX Prawo Europejskie, Zwolnienie z VAT telemedycyny*, LEX/el. 2020.

Czaplińska M., Sakowska-Baryła M., *Telemedycyna i teleporady w dobie pandemii – aspekty prawne i organizacyjne*, „Monitor Prawniczy" 2022, nr 12.

Czerw A., Religion U., *Systemy oceny jakości w ochronie zdrowia*, „Problemy Zarządzania", t. 10, nr 2(37).

Długaszek M., Gumprecht J., Berdzik-Kalarus S., Chodkowski A., Nabrdalik K., *Telemedicine in response to challenges of modern diabetology*, „Clin Diabet" 2016, nr 5(1).

Glanowski G., *Telemedycyna w świetle ustawy o zawodach lekarza i lekarza dentysty*, „Monitor Prawniczy" 2015, nr 18.

Iakovidis I., Wilson P., Healy J.C., *E-Health, Current Situation and Examples of Implemented and Beneficial E-Health Applications*, „Studies in Health Technology and Informatics" 2004, nr 100.

Karkowski T., *Telemedycyna i eHealth w sektorze opieki zdrowotnej*, LEX/el. 2022.

Kubicka-Mącznik A., Makuch J., *Korzyści wynikające ze stosowania rozwiązań telemedycznych w świetle badań naukowych – wybrane zagadnienia*, „Choroby Serca i Naczyń" 2017, nr 14(1).

Kwiatkowska M., *Wdrożenie systemów zarządzania jakością i bezpieczeństwem w ochronie zdrowia drogą do zmniejszenia liczby zdarzeń niepożądanych w szpitalach i POZ*, [w:] *Zdarzenia niepożądane w lecznictwie szpitalnym i podstawowej opiece zdrowotnej*, Warszawa 2020.

Olejarczyk J.P., Young M., *Patient Rights And Ethics, Treasure Island* (*FL*), StatPearls Publishing 2022.

Oręziak B., *Telemedycyna a konstytucyjne prawo do opieki zdrowotnej w kontekście wykluczenia cyfrowego*, „Zeszyty Prawnicze UKSW" 2018, nr 18.1.

Rek T., *Zasady interpretacji*, [w:] *Dziecko – pacjent i świadczeniobiorca*, red. M. Dercz, H. Izdebski, Warszawa 2015.

Sieńko A., *Obowiązki placówki medycznej w związku udzielaniem świadczeń dzieciom do 6 r.ż.*

Twarowski A., *Wpływ ustawy o funkcjonowaniu ochrony zdrowia w związku z epidemią COVID-19 na świadczeniodawców – informatyzacja ochrony zdrowia, Komentarz praktyczny*, LEX/el. 2020.

Urban K., Warmińska-Friberg E., *E-recepty w praktyce funkcjonowania podmiotów leczniczych*, LEX/el. 2018.

Urban K., Warmińska-Friberg E., *Zmiany w wystawianiu i realizacji recept w 2021 r.*, LEX/e. 2021.

Waseh S., Dicker A.P., *Telemedicine Training in Undergraduate Medical Education: Mixed-Methods Review*, JMIR Med Educ 2019, nr 5(1).

Wesołowska A., *Zwolnienie z VAT dla usług medycznych na odległość/przez telefon. Glosa do wyroku TS z dnia 5 marca 2020 r., C-48/19*, LEX/el. 2022.

Wrześniewska-Wal I., Hajdukiewicz D., *Telemedycyna w Polsce – aspekty prawne, medyczne i etyczne*, „Studia Prawnoustrojowe" 2020, nr 50.

Akty prawne

Ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (Dz.U. z 1997 r. Nr 28, poz. 152 z późn. zm.).
Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz.U. z 2011 r. Nr 112, poz. 654 z późn. zm.).
Ustawa z dnia 15 lipca 2011 r. o zawodach pielęgniarki i położnej (Dz.U. z 2011 r. Nr 174, poz. 1039 z późn. zm.).
Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000).
Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. z 2009 r. Nr 52, poz. 417).
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Orzecznictwo

Wyrok WSA w Krakowie z dnia 22 czerwca 2015 r., I SA/Kr 721/15, LEX nr 1813436.
Wyrok WSA w Warszawie z dnia 10 sierpnia 2021 r., V SA/Wa 2536/21, LEX nr 3311108.
Wyrok TSUE z dnia 5 marca 2020 r., C-48/19, *X-GmbH v. Finanzamt Z.*, LEX nr 2797480.

Raporty

A health telematics policy in support of WHO's Health-For-All strategy for global health development: report of the WHO group consultation on health telematics, 11–16 December, Geneva, 1997. Geneva, World Health Organization, 1998.
Market study on telemedicine, Luxembourg: Publications Office of the European Union, 20.
Raport czasopisma OSOZ Polska z 2022 r. pt. „Bezpieczeństwo danych w placówkach ochrony zdrowia".
Raport Uwarunkowania Rozwoju Telemedycyny w Polsce – Potrzeby, bariery, korzyści, analiza rynku, rekomendacje, wydanie 3, Krajowa Izba Gospodarcza.
Prognoza ludności na lata 2014–2050, Studia i Analizy Statystyczne, GUS, Warszawa 2014.
Społeczeństwo informacyjne w Polsce w 2021 roku, GUS, Warszawa, Szczecin 2021 r.
Sytuacja demograficzna osób starszych i konsekwencje starzenia się ludności Polski w świetle prognozy na lata 2014–2050, GUS, Warszawa 2014.

Alan Kosecki

Prawo wobec zjawiska fałszywej pornografii. Nowe zagrożenia w cyberprzestrzeni

1. Wprowadzenie

Wraz z postępującym rozwojem technologicznym, powszechnym użytkowaniem Internetu, serwisów społecznościowych oraz komunikatorów, na użytkowników technologii informacyjno-komunikacyjnych czekają nowe zagrożenia. Procesy cyfryzacji mają swoje przełożenie nie tylko na zmiany w życiu społeczno-gospodarczym, ale także na zmiany w zakresie przestępczości. W ostatnich latach największy problem stanowiły cyberprzestępstwa takie jak phishing[1], smishing[2] czy CLI spoofing[3]. Warto jednak zwrócić uwagę, że wszystkie te czyny mogą być obecnie karane na podstawie przepisów kodeksu karnego[4], m.in. art. 190a k.k., art. 286 k.k. czy art. 287 k.k., a smishing oraz CLI spoofing najprawdopodobniej doczekają się własnej ustawy, która będzie penalizowała działania wypełniające znamiona tych czynów[5].

---

[1] Phishing jest metodą oszustwa, w której przestępca podszywa się pod inną osobę lub instytucje w celu wyłudzenia poufnych informacji takich jak dane logowania, numer karty kredytowej. Zwykle są to działania podejmowane przez wiadomości e-mail bądź komunikatory.

[2] Smishing to działanie polegające na wysyłaniu SMS, w których nadawca podszywa się pod inny podmiot w celu nakłonienia odbiorcy tej wiadomości do określonego działania. Jest rodzajem phishingu podejmowanym jednak za pomocą krótkich wiadomości tekstowych SMS.

[3] CLI spoofing to nieuprawnione posłużenie się przez użytkownika wywołującego połączenie głosowe informacją adresową wskazującą na osobę lub jednostkę organizacyjną inną niż ten użytkownik, służące podszyciu się pod inny podmiot w celu nakłonienia odbiorcy tego połączenia do określonego działania. Innymi słowy jest to działanie polegające na wprowadzaniu odbiorcy w błąd co do tego, że połączenie zostało wykonane na przykład z numeru instytucji rządowej.

[4] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz.U. 2022 r. poz. 1138), dalej: k.k.

[5] Projekt ustawy o zwalczaniu nadużyć w komunikacji elektronicznej, https://legislacja.rcl.gov.pl/projekt/12360854 (dostęp: 27.07.2022 r.).

Zagadnieniem, które wymaga głębszej analizy są cyberzagrożenia w obszarze wolności seksualnej oraz obyczajności, a dokładniej preparowania pornografii. Odpowiedzialna za rozwój działań przestępczych w tej dziedzinie jest technologia *deepfake*.

Chociaż tematyka technologii *deepfake* jest niezwykle szeroka i może być rozpatrywana w odniesieniu do wielu gałęzi prawa, to na potrzeby niniejszego opracowania przedstawiona zostanie jedynie skrócona charakterystyka tego zjawiska, powiązania z pornografią oraz wskazane zostaną najbardziej palące problemy wymagające podjęcia pilnych działań legislacyjnych. Przedmiotowe założenie zostanie osiągnięte poprzez zastosowanie przez autora metodologii w postaci analizy teoretycznej przepisów prawnych zarówno krajowych, jak i unijnych. Ponadto w celu sformułowania wniosków *de lege ferenda* konieczne będzie odwołanie się do sfery aksjologicznej poprzez poddanie pod rozważania zagadnienia związanego z wartościami, jakie prawo wyraża oraz jakie powinno wyrażać.

Przechodząc zatem do charakterystyki głównego zagadnienia, wskazać należy, że terminem *deepfake* określa się wykorzystanie sztucznej inteligencji do wytwarzania bądź edytowania obrazu lub filmu w celu przekazania fałszywej treści[6]. Jak powszechnie wiadomo, manipulacja informacją w dzisiejszym świecie nie jest zjawiskiem nowym. Zaczyna ona nabierać jednak nowego wymiaru w związku ze stale rozwijającymi się możliwościami w cyberprzestrzeni. *Deepfake* to zespół algorytmów składający się na program komputerowy, który poprzez poprzednio wspomnianą sztuczną inteligencję jest w stanie stworzyć bądź zmodyfikować zdjęcie lub wideo poprzez łączenie i nakładanie istniejących obrazów i filmów w taki sposób, że finalnie powstanie ultra-realistyczny fałszywy film, w którym ludzie mówią i robią rzeczy nie mające miejsca w rzeczywistości[7]. Ponieważ sztuczna inteligencja wykorzystywana w ramach *deepfake* ma zdolność uczenia maszynowego i wykorzystywania

[6] A. Ziobroń, *Deepfake a prawo karne. Uwagi de lege lata i de lege ferenda dotyczące fałszywej pornografii*, „Studenckie Prace Prawnicze, Administratywistyczne i Ekonomiczne" 2012, nr 37, s. 226.

[7] O. Wasiuta, S. Wasiuta, *Deepfake jako skomplikowana i głęboko fałszywa rzeczywistość*, „Studia de Securitate" 2019, nr 9(3), s. 20.

technologii mapowania twarzy, jest w stanie manipulować głosem, ciałem, twarzą człowieka w taki sposób, że sfałszowany film jest wyjątkowo trudny do odróżnienia od prawdziwych zdjęć i filmów.

Mając na uwadze powyższe, należy wskazać, że z technologią *deepfake* wiążą się kolejne zagrożenia. Wynika to z – co prawda – umownego podziału na przeróbki o charakterze rozrywkowym, edukacyjnym, dezinformacyjnym oraz dyskredytacyjnym[8]. Trzeba podkreślić, że nie każdy *deepfake* jest zły, bowiem te o charakterze rozrywkowym, często odwołujące się do popkultury, mają na celu wywołanie pozytywnych bądź neutralnych wrażeń w odbiorcach. Podobnie jest z tymi o charakterze edukacyjnym, które mają przestrzegać odbiorców przed zagrożeniami jakie niewłaściwe korzystanie z technologii wykorzystujących sztuczną inteligencję może za sobą nieść. Fałszywe filmy bądź zdjęcia mogą mieć charakter dezinformacyjny oraz dyskredytacyjny. Oba te rodzaje są niebezpieczne zarówno dla osób będących bezpośrednimi ofiarami takiego działania jak i dla odbiorców[9]. *Deepfake* o charakterze dyskredytacyjnym ma na celu przede wszystkim osłabienie pozycji osoby lub podmiotu ukazanego na sfałszowanym filmie bądź zdjęciu. Do tej kategorii należy zaliczyć wszelkie *deepfake'i* skierowane w polityków, a także te o charakterze pornograficznym, o czym mowa będzie w dalszej części opracowania. Fałszywy film o charakterze dezinformacyjnym zasadniczo ma wywołać niepokój i dezinformację w szerokim gronie odbiorców – jest to jedna z form *fake news*.

Z technologią *deepfake* bardzo silnie związane jest zjawisko *deepfake porn* bądź zamiennie nazywane *deep porn*. Wydaje się być to kluczowym zagadnieniem mając na uwadze raport *Deeptrace Labs*, które w 2019 r. prześledziło 15 tys. filmów o charakterze *deepfake* znajdujących się online w tamtym czasie. Potrzebę podjęcia zdecydowanych i szybkich działań pokazuje po pierwsze fakt, że liczba tych filmów podwoiła się w ciągu ostatnich 9 miesięcy przed badaniami stanowiącymi przedmiot omawianego raportu. Wskazuje to zatem na bardzo szybki przyrost przestępstw popełnianych przy użyciu tej technologii. Po drugie,

[8] I. Dąbrowska, *Deepfake – nowy wymiar internetowej manipulacji*, „Zarządzanie Mediami" 2020, nr 8(2), s. 96.

[9] *Ibidem*, s. 97.

aż 96% filmów stanowiło pornografię i zawierało podmienione twarze kobiet, które nigdy nie wyraziły na to zgody[10].

Deep porn bardzo często wiąże się ze zjawiskiem występującym powszechnie już znacznie wcześniej, a mianowicie *revenge porn*. Problem stanowi również wykorzystywanie technologii *deepfake* w pornografii dziecięcej. Zważając na obszerność tych zagadnień oraz potrzebę odniesienia do przepisów penalizujących dane działanie, dalsze rozważania zostaną podjęte w podrozdziale poświęconym wyłącznie fałszywej pornografii.

2. Fałszywa pornografia

2.1. Fałszywa pornografia w odniesieniu do ofiar dorosłych

Jak zostało powyżej wskazane, fałszywa pornografia stworzona przy pomocy technologii *deepfake* stała się palącym problemem w obszarze zapobiegania oraz zwalczania cyberprzestępczości. Głównym celem opracowania jest analiza tego zjawiska w odniesieniu do przepisów prawa karnego zarówno *de lege lata*, jak i *de lege ferenda*.

Dokonując przedmiotowej analizy, przede wszystkim konieczne jest uwypuklenie faktu, że *deep porn* zawdzięcza swoją powszechność dzięki stosunkowo łatwej obsłudze technologii *deepfake*. W obecnych czasach, kiedy udostępniamy w Internecie swoje zdjęcia oraz nagrania, dokumentując przy tym prawie każdą chwilę swojego życia, dostęp do materiałów, które posłużą następnie do stworzenia *deepfake porn* jest niesamowicie łatwy. Sprawa ulega uproszczeniu, jeżeli mamy przy tym do czynienia z *revenge porn*, czyli pornografią odwetową. Zachodzi ona przede wszystkim wtedy gdy publikowane są zdjęcia bądź filmy o charakterze erotycznym, które przedstawiają osobę, która nie wyraziła na to zgody. Takiego działania dopuszczają się najczęściej byli partnerzy. Często przy publikacji dołączane są dane osoby, którą nagranie czy zdjęcie przedstawia.

[10] https://sciencemediahub.eu/2021/10/13/fighting-abusive-deepfakes-the-need-for-a--multi-layered-action-plan/ (dostęp: 27.07.2022 r.).

W powiązaniu z *deep porn* takie zdjęcia bądź nagrania są w pełni sfałszowane, jednak motyw jest ten sam – „złamane serce" oraz zazdrość.

Jak zatem na gruncie polskiego prawa karnego wygląda odpowiedzialność karna za tworzenie, rozpowszechnianie i wszelkie inne działania powiązane z *deepfake porn*?

Analizę tego zagadnienia należy rozpocząć od tego, że obecnie nie mamy w polskim prawie aktu prawa powszechnie obowiązującego, który *strice* definiowałby *deepfake* oraz je penalizował. Co prawda Kodeks karny zawiera kilka przepisów, których znamiona mogą odpowiadać częściowo temu zjawisku, jednakże wątpliwości budzi to, czy owe przepisy są wystarczające przy zapewnieniu funkcji sprawiedliwościowej oraz gwarancyjnej prawa karnego.

Nie powinno budzić wątpliwości, że przestępstw, które dotyczą czynów zabronionych mogących posiadać znamiona *deepfake porn* należy w Kodeksie karnym szukać w rozdziale dotyczącym przestępstw przeciwko wolności seksualnej i obyczajności, a także rozdziale o przestępstwach przeciwko wolności oraz przeciwko czci i nietykalności cielesnej.

Pierwszą rzeczą, która pozwoli zidentyfikować przepisy odnoszące się do *deepfake porn*, to uproszczenie tego, czym taki sfałszowany materiał jest, a mianowicie jest pornografią, czy też treścią pornograficzną. Polskie prawo nie zawiera obecnie definicji „treści pornograficznych", zatem jest to zagadnienie podlegające ocenie, interpretacji. W doktrynie wskazuje się, że treści pornograficzne charakteryzują się przedstawianiem w dowolnej formie autentycznych lub jedynie wyobrażonych przejawów płciowości lub życia seksualnego człowieka w wymiarze sprowadzonym do funkcji fizjologicznych oraz aspektów techniczno-biologicznych[11]. Z drugiej strony pojęcie to może być rozumiane jako przedstawienie czynności seksualnych (obcowania płciowego lub innej czynności seksualnej). Wskazuje się, że jest to pojęcie prawne, a nie medyczne, seksuologiczne czy psychologiczne, zatem nie powinno podlegać w procesie ocenie biegłego, a wyłącznie orzekającego w sprawie sądu. Ocena ta powinna

[11] A. Ziobroń, *op. cit.*, s. 227.

uwzględniać różnicę między pornografią a treściami erotycznymi, przekazem naukowym czy artystycznym[12].

Przepisem, który odnosi się do treści pornograficznych, jest art. 202 § 1 k.k. penalizujący co do zasady publiczne prezentowanie treści pornograficznych. Prezentowanie to musi jednak narzucać odbiór tych treści osobie, która sobie tego nie życzy. Publikacja materiałów stworzonych przy użyciu technologii *deepfake* następować będzie prawdopodobnie wyłącznie w Internecie. Jednakże wypełnienie przesłanek czynu zabronionego określonego w opisywanym przepisie wymagałoby udostępnienia takiego filmu bądź zdjęcia poza stronami pornograficznymi. W takim przypadku wydaje się być jasne, że publikacja wiązałaby się z prezentowaniem takich treści osobom, które sobie tego nie życzą. Przesłanka jednak, w mojej ocenie, nie jest spełniona, gdy treści *deep porn* zostaną udostępnione na stronach pornograficznych, gdyż osoba odwiedzająca takie strony ma na celu obejrzenie takich treści. Nie można zatem stwierdzić, że przepis art. 202 § 1 chroni przed zastosowaniem czy też skutkami wynikającymi z technologii *deepfake* w pornografii. Jeśli chodzi o przestępstwa przeciwko wolności seksualnej i obyczajności w odniesieniu do ofiar będących osobami dorosłymi, to na tym ochrona się kończy. Już w tym miejscu warto zatem zwrócić uwagę na braki w rzeczywistej ochronie ofiar.

Poza skojarzeniem fałszywej pornografii ze sferą *stricte* seksualną na myśl przychodzi przede wszystkim kradzież tożsamości. Czym bowiem, jak nie kradzieżą tożsamości, jest wykorzystanie wizerunku osoby trzeciej do stworzenia fałszywego zdjęcia lub filmu? Mamy zatem do czynienia z przestępstwem uregulowanym w art. 190a § 2 k.k., penalizującym podszywanie się pod inną osobę, wykorzystując jej wizerunek lub inne dane osobowe w celu wyrządzenia jej szkody majątkowej lub osobistej. Wątpliwości budzi jednak samo znamię podszywania się, które niejako wprost obliguje związek z podmiotem dokonującym kradzieży tożsamości. Dokonując interpretacji przy zastosowaniu wykładni językowej, należy stanąć na stanowisku, iż podszywanie się dotyczy sytuacji, w której kradzież tożsamości przez sprawcę jest dokonywana w celu wywarcia błędnego

[12] K. Lipiński, [w:] *Kodeks karny. Część szczególna. Komentarz*, red. J. Giezek, Warszawa 2021, art. 202.

wrażenia na odbiorcy co do swojej własnej tożsamości. Zatem to sprawca przejmuje czyjąś tożsamość i przedstawia ją jako własną. Również z literatury przedmiotu wynika taki wniosek. Prof. Marian Filar wprost stwierdza, że podszywanie się to wszelkie wyobrażalne formy czynu, które mają wytworzyć przekonanie, że „podszywacz" jest tą osobą, której wizerunek czy dane zostały wykorzystane[13]. Identyczne stanowisko zostało wyrażone również przez Prof. Marka Mozgawę[14]. Wyklucza to zatem penalizację *deepfake pornography* na podstawie tego przepisu, gdyż twórca takiego materiału nie używa czyjejś tożsamości jako własnej.

Być może rozwiązania szukać należy na gruncie art. 191a § 1 k.k., który kryminalizuje naruszenie intymności seksualnej w postaci utrwalania wizerunku nagiej osoby lub osoby w trakcie czynności seksualnej, używając w tym celu wobec niej przemocy, groźby bezprawnej lub podstępu albo w postaci rozpowszechniania wizerunku nagiej osoby lub osoby w trakcie czynności seksualnej bez jej zgody. Czy przepis ten znajdzie jednak zastosowanie w przypadku, gdy do stworzenia zdjęcia lub filmu wykorzystany został wyłącznie wizerunek w postaci twarzy? Nagie ciało w takich filmach przecież należy do kogoś innego bądź mogło zostać stworzone całkowicie komputerowo przy użyciu sztucznej inteligencji. Osoba pokrzywdzona *deepfake* nie uczestniczy rzeczywiście w czynności seksualnej, która została ukazana na zdjęciu czy materiale wideo. Specyfika prawa karnego dodatkowo zakazuje dokonywania wykładni rozszerzającej, która prowadziłaby do rozszerzającego wyznaczenia zakresu zastosowania norm zawartych w kodeksie karnym. Wobec tego, choć powołując się na holistyczność wykładni, tj. zastosowanie wszystkich reguł wykładni (językowej, systemowej, a przede wszystkim w tym wypadku celowościowej), nie wydaje się by można było przepis ten interpretować w taki sposób, żeby karalność czynu obejmowała *deep porn*.

Dla całościowego spojrzenia na przedstawiany problem konieczne jest przeanalizowanie również przepisów dotyczących zniesławienia oraz znieważenia. Zniesławienie znajduje się w art. 212 § 1 k.k. i zachodzi wtedy, gdy ktoś pomawia

[13] M. Filar, M. Berent, [w:] *Kodeks karny. Komentarz*, red. M. Filar, LEX/el. 2016, art. 190(a).

[14] M. Mozgawa, [w:] *Kodeks karny. Komentarz aktualizowany*, red. M. Mozgawa, LEX/el. 2022, art. 190(a).

inną osobę o takie postępowanie lub właściwości, które mogą poniżyć ją w opinii publicznej lub narazić na utratę zaufania potrzebnego dla danego stanowiska, zawodu lub rodzaju działalności[15]. Zastosowanie tego przepisu wydaje się być najbardziej adekwatne do przedstawianego zjawiska. Dobrem chronionym przez przepis jest cześć. Przesłanka poniżenia w opinii publicznej zależy oczywiście w dużej mierze od społeczeństwa i tego co jest w nim akceptowane, a co nie. Jest to przesłanka bardzo ocenna. Co do zasady natomiast można tu zaliczyć prowadzenie niemoralnego trybu życia, brak przyzwoitości czy zboczenie seksualne. Do takiej kategorii z pewnością będzie można zakwalifikować *deepfakes*, które przedstawiają czynności seksualne nieakceptowane społecznie takie jak zgwałcenie czy parafilie. Na co jednak warto zwrócić uwagę to fakt, że poza zakresem penalizacji mogą pozostawać te filmy i zdjęcia, które spełniają normy konsensualnego stosunku seksualnego. W takiej sytuacji przesłanka poniżenia w opinii publicznej może nie być spełniona[16]. *Deep porn* może być szczególnie niebezpieczne dla osób, które zobowiązane są do zachowania nieskazitelności charakteru w związku np. z zajmowanym stanowiskiem czy pełnioną funkcją. W takiej sytuacji spełniona zostanie druga przesłanka z przepisu. Przestępstwo to jest jednak prywatnoskargowe, a wymiar sankcji stosunkowo niski – obejmujący górną granicę do pięciu lat pozbawienia wolności.

Słusznym wydaje się również penalizowanie *deepfake porn* na podstawie art. 216 k.k., tj. przestępstwa znieważenia. Dobro chronione przez prawo jest właściwie tożsame z dobrem chronionym przez poprzednio omawiany przepis, jednakże różnica polega m.in. na tym, że w przypadku zniewagi nie jest wymagane występowanie przekazu informacyjnego w znieważającym zachowaniu sprawcy[17]. W tym przypadku jednak mamy do czynienia z niezwykle niskim wymiarem kary, tj. grzywną, ograniczeniem wolności lub karą pozbawienia wolności do roku, jeśli zniewaga została dokonana przez środki masowego komunikowania się. W odniesieniu do *deepfake* kara ta z pewnością nie spełnia funkcji prewencyjnej oraz represyjnej.

---

[15] http://criminalfuture.com/fake-porn-czy-wklejenie-czyjejs-twarzy-do-filmu-porno-jest-przestepstwem/ (dostęp: 27.07.2022 r.).

[16] A. Ziobroń, *op. cit.*, s. 232.

[17] *Ibidem*.

2.2. Fałszywa pornografia dziecięca

Niezwykle delikatną, ale wydaje się, że poważniejszą, kwestią jest odniesienie technologii *deepfake* do tworzenia i rozpowszechniania pornografii dziecięcej. Dzięki zastosowaniu możliwości, jakie daje *deepfake*, możliwe jest tworzenie pornografii dziecięcej szybciej, bezpieczniej i łatwiej niż do tej pory. Technologia ta może być wykorzystywana w stosunku do już istniejących materiałów (zdjęć czy nagrań) bądź tworzyć takie materiały od początku wykorzystując przy tym wizerunek dzieci, które nigdy wcześniej nie były seksualnie wykorzystywane. Nie należy jednak bagatelizować takiego działania ze względu na brak rzeczywistego nadużycia seksualnego wobec dziecka, ponieważ *child sexual abuse material*[18] może nieść za sobą poważne konsekwencje w postaci zniesławienia, nagabywania[19], wymuszania i prześladowania[20].

Niebagatelną rolę będzie odgrywała tutaj Unia Europejska (dalej: UE), a przede wszystkim dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej[21]. Ustanawia ona minimalne normy dotyczące określania przestępstw i kar dotyczących niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci, pornografii dziecięcej oraz nagabywania dzieci dla celów seksualnych[22]. Niezwykle ważna jest definicja pornografii dziecięcej, gdyż wpływać ona będzie na możliwość zakwalifikowania materiałów *deepfake* do zakresu penalizacji bądź nie. Zgodnie z art. 2 pkt c przedmiotowej dyrektywy, „pornografia dziecięca" to wszelkie materiały ukazujące dziecko uczestniczące

[18] Wszelkie materiały mające charakter seksualnego wykorzystywania dzieci.

[19] Nagabywanie dzieci do celów seksualnych (ang. *grooming*), wykorzystując przy tym środki komunikacji elektronicznej.

[20] T. Kirchengast, *Deepfakes and image manipulation: criminalization and control*, „Information & Communications Technology Law" 2020, nr 29(3), s. 308–323.

[21] Dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej (Dz.Urz. UE L Nr 335, s. 1), dalej: dyrektywa.

[22] Art. 1 dyrektywy Parlamentu Europejskiego i Rady 2011/93/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej.

w rzeczywistych lub symulowanych zachowaniach o wyraźnie seksualnym charakterze, wszelkie przedstawienia organów płciowych dziecka w celach głównie seksualnych. Ponadto są to wszelkie materiały ukazujące osobę wyglądającą na dziecko uczestniczącą w rzeczywistych lub symulowanych zachowaniach o wyraźnie seksualnym charakterze oraz przedstawienia organów płciowych osób wyglądających jak dziecko, w celach głównie seksualnych lub realistyczne obrazy dziecka uczestniczącego w zachowaniach o wyraźnie seksualnym charakterze lub realistyczne obrazy organów płciowych dziecka, w celach głównie seksualnych.

Konsekwencję tego przepisu stanowi nowelizacja Kodeksu karnego, w tym art. 202. Niezbędne w kontekście *deepfake* jest odniesienie się do § 4b tego przepisu. Penalizowane jest bowiem produkowanie, rozpowszechnianie, prezentowanie, przechowywanie i posiadanie treści pornograficznych przedstawiających wytworzony albo przetworzony wizerunek małoletniego uczestniczącego w czynności seksualnej. Wytworzony wizerunek małoletniego należy rozumieć jako obraz spreparowany, który przedstawia małoletniego nieistniejącego w realnym świecie, a więc stworzony komputerowo. Przetworzony wizerunek to obraz osoby istniejącej realnie, ale zmieniony na tyle, że przypomina inną osobę, niż ta którą w rzeczywistości jest. W praktyce dotyczy to właśnie wizerunków stworzonych komputerowo bądź animowanych filmów pornograficznych[23]. Dr Konrad Lipiński w komentarzu do tego przepisu również wskazuje, że wizerunek jest przetworzony wtedy, gdy postać rzeczywistego człowieka charakteryzowana lub przerabiana jest w taki sposób, aby stwarzać pozór, że jest on małoletni[24]. Dotyczyć to będzie przede wszystkim dorosłych aktorów filmów pornograficznych charakteryzowanych na osoby małoletnie. Czy odnieść można to również do technologii *deepfake*? Należy na ten problem spojrzeć z dwóch stron.

Po pierwsze, za zakwalifikowaniem *deepfake pornography* do kategorii wytworzonego bądź przetworzonego wizerunku małoletniego uczestniczącego w czynności seksualnej przemawia postulat dokonywania wykładni celowościowej, racjonalności ustawodawcy oraz sama aksjologia prawa. Celem wprowadzenia

[23] M. Mozgawa, *op. cit.*, art. 202.
[24] K. Lipiński, *op. cit*, art. 202.

takiego brzmienia przepisu oraz generalnie penalizacji czynu w nim zawartego jest przecież zwalczanie jak największej liczby przestępstw, w tym wydaje się cyberprzestępstw, biorąc m.in. pod uwagę dyrektywę UE. Prawo powinno być jasne, spójne, zupełne i niesprzeczne oraz zapewniać adresatom norm stabilność i poczucie bezpieczeństwa. Takie podejście przemawia za włączeniem *deepfake child porn* do definicji „wytworzonego bądź przetworzonego wizerunku małoletniego". Również przemawia za tym fakt, że prawo karne nie może być nazbyt kazuistyczne, szczególnie w odniesieniu do cyberprzestępstw, które rozwijają się we wręcz niemożliwym do pojęcia tempie. Prawodawca, zarówno unijny, jak i krajowy, musi mieć na uwadze, że przepisy stanowione dzisiaj muszą być równie skuteczne za rok, pięć czy dziesięć lat.

Z drugiej strony, jak już zostało wskazane powyżej, w prawie karnym funkcjonuje zakaz wykładni rozszerzającej. Przyjęcie innego stanowiska narażałoby system prawa na chaos. Co więcej, przedstawiciele doktryny, dokonując analizy powyższego przepisu, w tym przesłanek czynu zabronionego określonego w art. 202 § 4b, nie wspominają o *deepfake*. Pojawiają się stwierdzenia o komputerowym wytworzeniu danego wizerunku np. postaci z gier komputerowych, filmów animowanych (*hentai*), oraz charakteryzacja osoby dorosłej na dziecko.

Co więcej, należy w tym kontekście również zastanowić się czy jako treści pornograficzne można zakwalifikować materiał przerobiony w ten sposób, że pokazuje twarz dziecka na ciele wytworzonym komputerowo, a więc nie pokazuje jego narządów płciowych i nie ukazuje dziecka nago.

Niezwykle ważne w przyjmowaniu jednego bądź drugiego podejścia jest stanowisko (a może raczej jego brak) wyrażone przez zespół Dyżurnet.pl, powołany w 2005 r. przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy, wpisany od 2018 r. w ustawę o krajowym systemie cyberbezpieczeństwa[25] i realizujący zadania CSIRT NASK[26].

[25] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 156 z późn. zm.).

[26] CSIRT NASK to Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy z siedzibą w Warszawie.

Zespół Dyżurnet.pl jest jedynym w Polsce zespołem reagującym na nielegalne i szkodliwe treści w Internecie, który w ramach swojej działalności, na podstawie ustawy o krajowym systemie cyberbezpieczeństwa, przyjmuje zgłoszenia dotyczące materiałów przedstawiających seksualne wykorzystywanie dzieci[27]. Najwięcej incydentów zgłoszonych w 2021 r. dotyczyło *child sexual abuse materials*, czyli właśnie tych określonych w art. 202 § 3, 4, 4a oraz 4b k.k. Sześćdziesiąt jeden incydentów z ogólnej liczby 2069 dotyczyło treści przedstawiających wytworzony lub przetworzony wizerunek małoletniego uczestniczącego w czynności seksualnej. Dyżurnet.pl wskazuje, że takie wygenerowane komputerowo i względnie realistycznie wyglądające treści w wielu państwach nie są uznawane za nielegalne, dlatego ciągle są obecne w Internecie[28]. Co więcej, zespół ten w swoich publikacjach wielokrotnie wskazuje na nieadekwatność definicji „pornografii dziecięcej" oraz brak definicji „treści pornograficznych" co utrudnia poprawne i pełne zastosowanie przepisu w niektórych sytuacjach. Uwagę zwraca jednak fakt, że w publikacji „Ryzykowne zachowania seksualne i seksualizujące młodych użytkowników Internetu. Zarys problematyki" zespół Dyżurnet.pl odniósł się do przestępstwa z art. 202 § 4b k.k., opowiadając się za karalnością przetwarzania czyjegoś zdjęcia nadającego materiałowi cechy pornograficzne. Jest to właściwie definicja opisowa *deepfake pornography*.

Wniosek jednak płynie stąd taki, że dopóki kwestia ta nie zostanie uregulowana wprost, wątpliwości interpretacyjne pozostaną, a przepis nie będzie zapewniał wystarczającej ochrony ofiar. Obecnie mamy do czynienia ze zbyt dużą rozbieżnością interpretacyjną lub po prostu zbyt małą ilością literatury z kategorii *deepfake* oraz *deep porn*.

2.3. Zapobieganie i zwalczanie *deepfake porn* w przyszłości

Nie można rzecz jasna pominąć w niniejszym opracowaniu tematu pandemii COVID-19, która zasadniczo przeniosła większość życia społecznego do Internetu. Również dzieci, ze względu na naukę zdalną, większość tego czasu spędzały

[27] Raport dyżurnet.pl z 2021 r., s. 6.
[28] *Ibidem*, s. 19.

korzystając ze środków komunikacji elektronicznej. Pandemia naraziła dzieci na znacznie większą liczbę niechcianych kontaktów w Internecie. W związku z tym Unia Europejska zauważyła potrzebę przyjęcia takich przepisów, które pozwoliłyby na szybsze i efektywniejsze zwalczanie oraz zapobieganie niegodziwemu traktowaniu dzieci w celach seksualnych. Rozpoczęto zatem prace nad rozporządzeniem Parlamentu Europejskiego i Rady[29] ustanawiającego przepisy mające na celu powyższe. Projekt ten w szczególności nakłada na dostawców odpowiednich usług w sieci obowiązki w zakresie minimalizowania ryzyka, że usługi przez nich dostarczane zostaną wykorzystane w niewłaściwy sposób skutkując niegodziwym traktowaniem dzieci w celach seksualnych. Dostawcy usług hostingu oraz łączności interpersonalnej obowiązani będą do wykrywania oraz zgłaszania przypadków niegodziwego traktowania dzieci w celach seksualnych, a także do usuwania takich materiałów. Projekt ten, jako złożony w maju 2022 r. jest projektem na bardzo wczesnym etapie prac, obecnie trwają konsultacje publiczne do unijnego projektu rozporządzenia, zatem przepisy wchodzące w jego skład mogą się zmienić. Na co należy jednak zwrócić uwagę, to fakt, że projekt odwołuje się w zakresie przestępstw do dyrektywy przedstawianej przeze mnie wcześniej, tj. dyrektywy Parlamentu Europejskiego i Rady 2011/93/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej. Nie wprowadza zatem nowych kategorii seksualnego wykorzystywania dzieci.

Analizując obecnie zaproponowane w projekcie rozporządzenia rozwiązania, problematycznych wydaje się być kilka kwestii.

Po pierwsze, nieścisłości zachodzą już w zakresie definicji legalnych, jakimi posługiwać się ma rozporządzenie. Akt ten rozróżnia dziecko od użytkownika będącego dzieckiem. Definicje te zostały zawarte w art. 2 odpowiednio lit. i oraz j. „Dziecko", zgodnie z projektem rozporządzenia, oznacza każdą osobę fizyczną w wieku poniżej 18 lat, a „użytkownik będący dzieckiem" to osoba

[29] Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające przepisy mające na celu zapobieganie niegodziwemu traktowaniu dzieci w celach seksualnych i jego zwalczanie, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52022PC0209&from=EN (dostęp: 30.07.2022 r.).

fizyczna korzystająca z odpowiedniej usługi społeczeństwa informacyjnego w wieku poniżej 17 lat. Zauważalna jest zatem niekonsekwencja, która może mieć daleko idące skutki w zakresie zarówno wykonywania obowiązków przez dostawców usług, ale przede wszystkim w zakresie ochrony ofiar przestępstw seksualnych w Internecie. Pojawia się pytanie, dlaczego dzieckiem ma być określona osoba poniżej 18. roku życia, a użytkownikiem będącym dzieckiem ma być osoba w wieku poniżej 17 lat? Taki przepis odmawia ochrony osobom, które ukończyły 17 lat, a jednocześnie – według prawa polskiego[30], ale też zgodnie z rozporządzeniem – nadal jest dzieckiem.

Po drugie, w związku z zapobieganiem oraz zwalczaniem niegodziwego traktowania dzieci w celach seksualnych należy odnieść się do przestępstw seksualnych przeciwko dzieciom, które zostały określone w powyższej dyrektywie 2011/93/UE. Jak już w toku opracowania wielokrotnie było przedstawiane, powstają istotne wątpliwości do co zakresu penalizacji *deepfake pornography*. Brak dokładnego określenia, że przestępstwo stanowi również tworzenie, przy pomocy sztucznej inteligencji, fałszywych filmów bądź zdjęć o charakterze erotycznym, pornograficznym z wykorzystaniem wizerunku (m.in. twarzy) dziecka nie rozwiązuje w żaden sposób problemów interpretacyjnych obecnych na gruncie dyrektywy 2011/93/UE, Kodeksu karnego w art. 202 § 4b oraz obecnie w projekcie rozporządzenia. Ponadto brak takiego dookreślenia może stanowić przeszkodę dla realizowania obowiązków, które mają być nałożone na dostawców usług. Zachodzi bowiem problem identyfikacji rzeczywistych ofiar. Technologia może być użyta do ukrycia twarzy dziecka na zdjęciu bądź nagraniu, które stanowi prawdziwe nadużycie. Konieczne jest podkreślenie, że takie działanie, choć nie wykorzystujące dziecka w ścisłym tego słowa znaczeniu, jest formą seksualizacji dziecka, przed którą państwo jest zobowiązane, na mocy art. 34 Konwencji o prawach dziecka, je chronić.

[30] W prawie polskim pełnoletność uzyskuje się – co do zasady – wraz z ukończeniem przez osobę fizyczną 18. roku życia. Ponadto kodeks karny w odniesieniu do treści pornograficznych posługuje się dwoma pojęciami, które stanowią o zakresie ochrony – jest to małoletni przed ukończeniem 15. roku życia oraz – tak jak w art. 202 § 4b k.k. – małoletni, a więc osoba fizyczna, która nie ukończyła 18. roku życia.

Po trzecie, zagrożenie występuje również przy ochronie osób dorosłych. W kontekście dzieci technologia *deepfake* może zostać wykorzystana przeciwko dorosłemu poprzez użycie jego wizerunku do sfałszowania nagrania (lub zdjęcia) przedstawiającego wykorzystanie seksualne dziecka. Brak penalizacji *deepfake* będzie wiązał się z preparowaniem nagrań i zdjęć, które następnie mogą być przedstawiane w postępowaniu dowodowym przeciwko niewinnej osobie, której wizerunek został wykorzystany.

3. Wnioski

Aby sprostać wyzwaniu, jakim jest stale rozwijająca się cyberprzestępczość polegająca na wykorzystywaniu coraz to nowszej technologii konieczne są zdecydowane i konkretne działania mające na celu zarówno skuteczne zapobieganie, jak i zwalczanie takiej działalności, szczególnie w odniesieniu do przestępstw wykorzystujących technologię *deepfake*. Tworzenie fałszywych zdjęć bądź filmów wykorzystując do tego możliwości, jakie daje sztuczna inteligencja, jest zagrożeniem, które nie może pozostawać bez regulacji. Analiza niniejszego zjawiska pozwoliła na sformułowanie wniosków w postaci niewystarczającej ochrony ofiar, jeśli chodzi o spreparowaną pornografię dorosłych oraz nieco skuteczniejszą, lecz w mojej ocenie niepozostającą bez poważnych wątpliwości, ochronę dzieci. Z całą pewnością konieczne jest doprecyzowanie przepisów w sposób umożliwiający ściganie za popełnienie czynu wykorzystującego w pornografii technologię *deepfake*.

Nie należy jednak ulegać złudnemu wrażeniu, że sprawcy obecnie pozostają całkowicie bezkarni. Z uwagi na cel, jak i konieczność zapewnienia jak najdłuższej i skutecznej stosowalności przepisów, zarówno te obecnie obowiązujące, jak i te w projekcie rozporządzenia, które nakładają obowiązki na dostawców usług czy hostingu, dają się wykorzystywać w praktyce. Każde nagranie czy zdjęcie, nieważne czy sfałszowane, przedstawiające osobę poniżej 18. roku życia będzie musiało być wykryte oraz usunięte przez dostawcę usług. Zupełnie inną kwestią pozostaje to, kto jest ofiarą przy tworzeniu takiego materiału – dziecko, którego wizerunek wykorzystano, dziecko realnie wykorzystane, przedstawione

na nagraniu, obie te osoby? W celu wyeliminowania tych oraz innych, wskazanych w toku opracowania, wątpliwości konieczne jest podjęcie działań legislacyjnych, które odpowiedziałyby na te nowe zagrożenia w cyberprzestrzeni.

Bibliografia

Dąbrowska I., *Deepfake – nowy wymiar internetowej manipulacji*, „Zarządzanie Mediami" 2020, nr 8(2).

Filar M., Berent M., [w:] *Kodeks karny. Komentarz*, red. M. Filar, LEX/el. 2016.

Kirchengast T., *Deepfakes and image manipulation: criminalization and control*, „Information & Communications Technology Law" 2020, nr 29(3).

Lipiński K., [w:] *Kodeks karny. Część szczególna. Komentarz*, red. J. Giezek, Warszawa 2021.

Mozgawa M., [w:] *Kodeks karny. Komentarz aktualizowany*, red. M. Mozgawa, LEX/el. 2022.

Wasiuta O., Wasiuta S., *Deepfake jako skomplikowana i głęboko fałszywa rzeczywistość*, „Studia de Securitate" 2019, nr 9(3).

Ziobroń A., *Deepfake a prawo karne. Uwagi de lege lata i de lege ferenda dotyczące fałszywej pornografii*, „Studenckie Prace Prawnicze, Administratywistyczne i Ekonomiczne" 2012, nr 37.

Akty prawne

Dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej (Dz.Urz. UE L Nr 335, s. 1).

Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające przepisy mające na celu zapobieganie niegodziwemu traktowaniu dzieci w celach seksualnych i jego zwalczanie, https://eur-lex.europa.eu/legal- content/PL/TXT/HTML/?uri=CELEX:52022PC0209&from=EN (dostęp: 30.07.2022 r.).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 156 z późn. zm.).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. Dz.U. z 2022 r. poz. 1138).

Netografia

http://criminalfuture.com/fake-porn-czy-wklejenie-czyjejs-twarzy-do-filmu-porno-jest-przestepstwem/ (dostęp: 27.07.2022 r.).
https://sciencemediahub.eu/2021/10/13/fighting-abusive-deepfakes-the-need-for-a-multi-layered-action-plan/ (dostęp: 27.07.2022 r.).
Projekt ustawy o zwalczaniu nadużyć w komunikacji elektronicznej, https://legislacja.rcl.gov.pl/projekt/12360854 (dostęp: 27.07.2022 r.).
Raport dyżurnet.pl z 2021 r. (dostęp: 27.07.2022 r.).

Autorzy

Dr hab. Marek Bielecki, prof. ASzWoj – profesor Akademii Sztuki Wojennej i Instytutu Wymiaru Sprawiedliwości w Warszawie. Autor licznych publikacji i monografii z zakresu prawa wyznaniowego, praw dziecka i prawa administracyjnego. Członek stowarzyszeń naukowych. Aktualnie pełni funkcję prezesa Polskiego Towarzystwa Prawa Wyznaniowego.
ORCID: 0000-0003-3880-017X

Mgr Tomasz Bojanowski – doktorant w Szkole Doktorskiej Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie. Absolwent prawa na Wydziale Prawa i Administracji UKSW. Laureat Stypendium Ministra Nauki i Szkolnictwa Wyższego za wybitne osiągnięcia w nauce na rok akademicki 2021/2022 oraz Stypendium Prezydenta m. st. Warszawy im. Jana Pawła II. Członek międzynarodowych i krajowych projektów badawczych, a także prelegent i organizator międzynarodowych oraz krajowych konferencji naukowych. Główne zainteresowania: prawo karne, kryminalistyka, prawo operacyjne, ochrona praw człowieka, prawo konstytucyjne, prawo administracyjne.
ORCID: 0000-0001-8294-0968

Dr Maciej Domański – doktor nauk prawnych, adiunkt w Katedrze Prawa Cywilnego Wydziału Prawa i Administracji Uniwersytetu Warszawskiego oraz Instytucie Wymiaru Sprawiedliwości w Warszawie. Autor publikacji z zakresu prawa cywilnego, w szczególności rodzinnego.
ORCID: 0000-0002-9155-8354

Dr László Dornfeld – absolwent studiów prawniczych w Uniwersytecie w Moszkolcu (2015) oraz studiów doktoranckich (2018). Od 2020 r. współprzewodniczący Sekcji Doktoranckiej Węgierskiego Towarzystwa Kryminologicznego. W latach 2019–2022 pracował jako badacz w Ferenc Mádl Institute of Comparative Law. Od 2022 r. główny analityk w dziedzinie prawa UE w Centrum Praw Podstawowych.

Dr Katarzyna Grzelak-Bach – adiunkt w Katedrze Ochrony Praw Człowieka i Prawa Międzynarodowego Humanitarnego Wydziału Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego. Autorka licznych publikacji naukowych, wykładowca, szkoleniowiec KSAP, radca prawny Okręgowej Izby Radców Prawnych w Warszawie. Doświadczenie zawodowe zdobywała w Naczelnym Sądzie Administracyjnym, Wojewódzkim Sądzie Administracyjnym w Warszawie, Departamencie Prawnym i Postępowań przed Trybunałem Konstytucyjnym Rządowego Centrum Legislacji, Departamencie Spraw Parlamentarnych oraz Departamencie Oceny Skutków Regulacji Kancelarii Prezesa Rady Ministrów.
ORCID: 0000-0002-8598-0591

Alan Kosecki – student prawa na Wydziale Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie. Autor publikacji naukowych, organizator oraz prelegent ogólnopolskich i międzynarodowych konferencji naukowych. Jego główne zainteresowania skupiają się wokół prawa i procesu karnego, prawa międzynarodowego, prawa Unii Europejskiej oraz ochrony praw człowieka. Doświadczenie zawodowe zdobywał w Sądzie Rejonowym dla Warszawy Mokotowa w Warszawie, kancelariach adwokackich, Instytucie Wymiaru Sprawiedliwości oraz Kancelarii Prezesa Rady Ministrów. Obecnie zawodowo związany z legislacją.
ORCID: 0000-0002-9544-9905

Mgr Klaudia Łuniewska – doktorantka i absolwentka studiów prawniczych na Wydziale Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie. Specjalistka naukowo-badawcza w Instytucie Wymiaru

Sprawiedliwości. Autorka opracowań z zakresu nauk prawnych. Kierowniczka i członkini krajowych oraz międzynarodowych projektów badawczych, a także prelegentka oraz organizatorka krajowych i międzynarodowych konferencji naukowych. Wielokrotna stypendystka stypendium rektora UKSW dla najlepszych studentów. Główne zainteresowania badawcze: prawo i procedura karna, prawo nowych technologii, prawo administracyjne, ochrona praw człowieka, prawo międzynarodowe, prawo Unii Europejskiej, bezpieczeństwo wewnętrzne.
ORCID: 0000-0002-3546-3414

Dr Agnieszka Mikos-Sitek – doktor nauk prawnych, absolwentka studiów prawniczych na Wydziale Prawa, Prawa Kanonicznego i Administracji Katolickiego Uniwersytetu Lubelskiego Jana Pawła II. Adiunkt w Katedrze Prawa Finansowego Wydziału Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego, pełni funkcję kierownika kierunku prawo. W swojej pracy naukowej zajmuje się przede wszystkim problematyką prawa bankowego, bankowości centralnej, prawa budżetowego (w zakresie gospodarki finansowej państwa oraz jednostek samorządu terytorialnego), finansowaniem ochrony zdrowia. Autorka publikacji we wskazanym zakresie specjalizacji. W latach 2001–2003 redaktor dwutygodnika „Monitor Prawniczy", w latach 2003–2011 redaktor, a następnie wydawca w Dziale Literatury Prawniczej Wydawnictwa C.H. Beck sp. z o.o., redaktor prowadzący serii „System Prawa Prywatnego" pod redakcją naukową prof. dr Zbigniewa Radwańskiego wydawanej we współpracy z INP PAN, w latach 2006–2011 redaktor kwartalnika Studia Prawa Prywatnego (do 2021 r. członek Kolegium Redakcyjnego). Od 2021 r. pełni funkcję kierownika Wydawnictwa Instytutu Wymiaru Sprawiedliwości.
ORCID 0000-0002-9288-7651

Dr Bartłomiej Oręziak – koordynator Centrum Analiz Strategicznych Instytutu Wymiaru Sprawiedliwości, badacz w Central European Professors' Network 2021 (grupa badawcza „The Impact of Digital Platforms and Social Media on Freedom of Expression and Pluralism") oraz w Central European Professors' Network 2022 (grupa badawcza „The right to privacy"), współpracownik Wydziału Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie,

laureat Stypendium Ministra Nauki i Szkolnictwa Wyższego za wybitne osiągnięcia w nauce na rok akademicki 2017/2018, laureat konkursu DOCUP 2020, reprezentant IWS w Grupie Roboczej ds. Sztucznej Inteligencji działającej przy Kancelarii Prezesa Rady Ministrów.
ORCID: 0000-0001-8705-6880

Dr hab. Szymon Pawelec, prof. UW – kierownik Katedry Międzynarodowego Postępowania Karnego na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego.
ORCID: 0000-0001-7166-9180

Prof. dr hab. Łukasz Pohl – profesor nauk prawnych, pracownik Uniwersytetu Szczecińskiego, w którym kieruje Zespołem Badawczym Prawa Karnego, oraz Instytutu Wymiaru Sprawiedliwości w Warszawie, w którym przewodniczy Sekcji Prawa i Procesu Karnego. Autor ponad 100 prac naukowych z zakresu prawa karnego, w tym kilku monografii, licznych artykułów w wiodących polskich czasopismach prawniczych oraz podręcznika *Prawo karne. Wykład części ogólnej*.
ORCID: 0000–0003–0530–1569

MA Víctor Serrano Suárez – doktorant w ramach Międzyuczelnianego Programu Doktoranckiego w dziedzinie komunikacji uniwersytetów w Sewilli, Maladze, Huelvie i Kadyksie. Posiada ponad 20-letnie doświadczenie w dziedzinie prawa, komunikacji i HR, zdobyte w trakcie pracy w kancelariach prawnych, takich jak Martínez-Echevarría, lub jako dyrektor firm konsultingowych, takich jak m.in. Adecco. Magister zarządzania strategicznego i innowacji w komunikacji oraz ekspert w zakresie bezpieczeństwa informacji. Pełni funkcję Visiting International Researcher na Uniwersytecie Kolumbii Brytyjskiej. Członek Sekcji Prawa Cyfrowego ICAMÁLAGA oraz, okazjonalnie, wykładowca wizytujący na Uniwersytecie w Maladze.

Dr Jerzy Słyk – adiunkt w Katedrze Prawa Rodzinnego i Prawa Nieletnich na Wydziale Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie, kierownik Sekcji Prawa Rodzinnego w Instytucie Wymiaru Sprawiedliwości. Autor publikacji z zakresu prawa rodzinnego i prawa medycznego. ORCID: 0000-0002-3067-1986

Dr Emilia Smolak-Lozano – doktor nauk o komunikowaniu (2017), profesor Advertising and Public Relations na Uniwersytecie w Maladze. Magister socjologii (Uniwersytet Jagielloński) i studiów europejskich (University of Exeter). Ekspertka w zakresie strategicznego zarządzania komunikacją korporacyjną w mediach cyfrowych. Członkini Rady Redakcyjnej International Journal of Public Relations oraz ECREA. Autorka ponad 70 publikacji, w tym artykułów w Scopus i JCR, rozdziałów w monografiach prestiżowych redakcji i czterech książek. Prelegentka na ponad 60 międzynarodowych kongresach poświęconych komunikacji. Profesor wizytująca i badaczka na wielu renomowanych europejskich uczelniach.

Dr hab. Joanna Taczkowska-Olszewska, prof. KPSW – adwokat, od 2001 r. nauczyciel akademicki i wykładowca, prorektor ds. nauki w Kujawsko-Pomorskiej Szkole Wyższej w Bydgoszczy, pełni funkcję kierownika Sekcji Prawa i Procesu Cywilnego w Instytucie Wymiaru Sprawiedliwości, wcześniej profesor w Akademii Sztuki Wojennej w Warszawie, gdzie kierowała Katedrą Administracji i Prawa Administracyjnego na Wydziale Bezpieczeństwa Narodowego ASzWoj. Biegła sądowa w zakresie dziennikarstwa. Członkini organów konsultacyjnych i stowarzyszeń naukowych oraz ekspertka w dziedzinie prawa prasowego, a także w zakresie mediów elektronicznych i usług audiowizualnych, świadczenia usług drogą elektroniczną, w tym w zakresie odpowiedzialności dostawców usług internetowych z tytułu dostarczania treści cyfrowych i handlu elektronicznego. Autorka ekspertyz oraz publikacji naukowych z zakresu ochrony informacji, a w szczególności ochrony prywatności oraz tajemnic ustawowo chronionych w tym z zakresu ochrony danych osobowych.
ORCID: 0000-0003-1566-5884

Dr hab. Marcin Wielec, prof. UKSW – doktor habilitowany nauk prawnych, profesor Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie. Absolwent Wydziału Prawa i Administracji UKSW. Obecnie na tym Wydziale pełni funkcje: prodziekana ds. studenckich na kierunku prawo i kierunku człowiek w cyberprzestrzeni oraz kierownika Katedry Postępowania Karnego WPiA UKSW. Absolwent programu typu MBA – Top Public Executive w IESE Business School University of Navarra w Barcelonie oraz Krajowej Szkoły Administracji Publicznej im. Lecha Kaczyńskiego w Warszawie. Dyrektor Instytutu Wymiaru Sprawiedliwości w Warszawie.
ORCID: 0000-0001-6716-3224

Dr hab. Łukasz Wojcieszak, prof. PŚk – doktor habilitowany nauk społecznych oraz doktor nauk prawnych. Zatrudniony na stanowisku profesora na Politechnice Świętokrzyskiej w Kielcach. Autor około stu publikacji naukowych, w tym kilku książek. Główne zainteresowania badawcze: bezpieczeństwo energetyczne, prawo energetyczne, polityka wschodnia Polski i Unii Europejskiej.
ORCID: 0000-0002-9166-4464

Agata Wróbel – studentka prawa na Wydziale Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie. Wielokrotna stypendystka stypendium rektora UKSW, autorka publikacji naukowych, członkini międzynarodowych i krajowych projektów badawczych, organizatorka międzynarodowych oraz krajowych konferencji naukowych. Główne zainteresowania rozciągają się na tematykę cyberbezpieczeństwa, prawa karnego procesowego, prawa międzynarodowego i prawa Unii Europejskiej.
ORCID: 0000-0003-1809-0334

Oddawana do rąk Czytelników praca zbiorowa jest pokłosiem międzynarodowego projektu badawczego pt. *Cyberbezpieczeństwo Grupy Wyszehradzkiej na rzecz zapobiegania przyczynom przestępczości*, realizowanego przez Instytut Wymiaru Sprawiedliwości.

Cyberprzestępczość jest jednym z największych zagrożeń i wyzwań XXI wieku, stąd istnieje potrzeba wielopłaszczyznowego badania tego zjawiska. Jest to pole badawcze dla prawników teoretyków i praktyków, a także kryminologów, zwłaszcza zajmujących się profilaktyką kryminologiczną. Publikacja zawiera odpowiedź na wiele istotnych pytań, pojawiających się w aktualnym dyskursie naukowo-badawczym. Oprócz perspektywy krajowej ciekawie zarysowano rozwiązania przyjęte w innych krajach.

Z RECENZJI PROF. ZW. DR HAB. EWY M. GUZIK-MAKARUK

Monografia *Cyber security to prevent crime causes* dotyczy problematyki cyberbezpieczeństwa i zapobiegania cyberprzestępczości, co jest istotnym tematem, o dużej doniosłości teoretycznej i coraz większym znaczeniu praktycznym, a także wymagającym szerszej eksploracji naukowej.

Obecnie obserwujemy zjawisko przenoszenia coraz większego zakresu ludzkiej aktywności do przestrzeni wirtualnej. Mowa tutaj o takich obszarach, jak edukacja, zdrowie, biznes, finanse, a także powszechność funkcjonowania użytkowników w mediach społecznościowych, a cały ten proces dodatkowo przyspieszyła pandemia COVID-19. Wraz za tymi tendencjami podąża przestępczość, która także przenosi się do cyberprzestrzeni i jako taka wymaga podjęcia rozważań na płaszczyźnie prawnej, dlatego też wybór tematu należy uznać za trafny i niezwykle aktualny.

Z RECENZJI DR KLARY DYGASZEWICZ

ISBN 978-83-67149-30-3