RUCH PRAWNICZY, EKONOMICZNY I SOCJOLOGICZNY
Rok LXXXVIII – zeszyt 2 – 2026
https://doi.org/10.14746/rpeis.2026.88.2.08

ANNA GOLONKA[a]

CYBEROSZUSTWO Z WYKORZYSTANIEM NOWOCZESNYCH TECHNOLOGII: ZAGROŻENIA I PRAWNE ASPEKTY PRZECIWDZIAŁANIA

CYBER FRAUD USING MODERN TECHNOLOGIES: THREATS AND LEGAL ASPECTS OF COUNTERACTING

The paper addresses the issue of cyber fraud as a type of fraud committed in cyberspace. The primary objective is to draw attention to the threats entailed by the use of modern technologies, in particular artificial intelligence, machine learning, and blockchain technology, to commit this crime. This subject is presented from a criminological and criminal-law perspective. In the former respect, the trends and scale of the phenomenon are analysed, with reference to the dynamics of progress in the IT field and specific examples of cyber fraud, following an analysis of the etymological issues relating to the terms *cyberspace* and *cyber fraud*. Regarding the criminal law aspects, specific EU and national regulations related to counteracting the discussed practices were analysed in detail, such as the Artificial Intelligence Act (AI Act), the Polish Penal Code, and the Act on Combating Abuse in Electronic Communication. Thus, the research was based on the formal-dogmatic method with empirical elements. On this basis, final conclusions are drawn. Cyber fraud constitutes a serious, rapidly growing threat in which perpetrators increasingly utilize modern technologies. A key problem remains the victims' lack of familiarity with these tools. Effective counteraction against these phenomena requires continuous adaptation of criminal provisions to technical progress, strengthening international cooperation between law enforcement agencies, and implementing systemic educational programs to raise public digital awareness.

Keywords: fraud; cybercrime; modern technologies

W opracowaniu podjęto problematykę cyberoszustwa jako rodzaju oszustwa popełnionego w cyberprzestrzeni. Nadrzędnym celem jest zwrócenie uwagi na zagrożenia, jakie niesie za sobą wykorzystanie nowoczesnych technologii, w szczególności sztucznej inteligencji, uczenia maszynowego oraz technologii *blockchain* do popełnienia tego przestępstwa. Tematykę tę ukazano z perspektywy kryminologicznej oraz prawnokarnej. W tym pierwszym względzie przeanalizowano tendencje i skalę zjawiska, odnosząc się do dynamiki postępu w dziedzinie IT oraz konkretnych przykładów cyberoszustw, poprzedzając to analizą kwestii etymologicznych terminów *cyberprzestrzeń* i *cyberoszustwo*. W odniesieniu do aspektów prawnokarnych, szczegółowej analizie poddano wybrane regulacje unijne i krajowe związane z przeciwdziałaniem omawianym procederom, takie jak Akt o sztucznej inteligencji (AI Act), polski Kodeks karny oraz ustawa o zwalczaniu nadużyć w komunikacji elektronicznej. Tym samym w badaniach bazowano na metodzie formalno-dogmatycznej

[a] University of Rzeszów, Poland / Uniwersytet Rzeszowski, Polska
agolonka@ur.edu.pl, https://orcid.org/0000-0002-0199-2203

RPEiS 88(2), 2026: 127–145. *ISSN (Online) 2543-9170 ISSN (Print) 0035-9629*

z elementami empirycznymi. Rozważania prowadzą do wniosków, że cyberoszustwo stanowi poważne, wykazujące silną tendencję wzrostową zagrożenie, w którym sprawcy coraz częściej wykorzystują nowoczesne technologie. Kluczowym problemem pozostaje nieznajomość tych narzędzi przez ofiary przestępstw. Skuteczne przeciwdziałanie tym zjawiskom wymaga stałego dostosowywania przepisów karnych do postępu technicznego, zacieśniania międzynarodowej współpracy organów ścigania oraz realizacji systemowych programów edukacyjnych podnoszących cyfrową świadomość społeczeństwa.

Słowa kluczowe: oszustwo; cyberprzestępstwo; nowoczesne technologie

I. WSTĘP

Postęp w rozwoju technologicznym stał się nieunikniony. Przez wielu jest on wręcz pożądany i oczekiwany. Życie we współczesnym świecie, w dobie technologii informatycznych, bez dostępu do Internetu, „podręcznego" smartfonu czy nieodzownego w pracy laptopa, tabletu czy chociaż PC-ta wydaje się trudne do wyobrażenia. Postępująca digitalizacja życia społecznego i gospodarczego, jaka cechuje obecne czasy, niesie za sobą wiele korzyści, w szczególności takie, jak: szybki i łatwy dostęp do dóbr i usług, kreowanie realistycznych wizji, komunikacja w czasie rzeczywistym, poprawa jakości życia czy wyręczanie człowieka w codziennych obowiązkach. Wszystkich atutów rozwoju technologicznego nie sposób, rzecz jasna, wyliczyć. Przewrotnie rzec by można nawet, że docenianych nie tylko przez tych, którzy czerpią z tego legalne profity. Nie pozostawia bowiem złudzeń to, iż drugą stroną medalu są zagrożenia, na jakie narażeni jesteśmy, sięgając po zdobycze technologiczne. Ich źródłem są w szczególności cyberprzestępstwa. W tej kategorii mieszczą się zaś nie tylko cyberataki *sensu stricto*, lecz także przestępstwa popełnione przy wykorzystaniu nowoczesnych technologii. Do takich należy m.in. *cyberoszustwo*, czyli oszustwo popełnione w cyberprzestrzeni. Pojęcie to nie funkcjonuje wprawdzie w języku prawnym, niemniej bywa używane[1]. Zasadność posługiwania się nim wynika z faktu, iż sprawcy, dostosowując *modus operandi* do postępu technologicznego, sięgają coraz częściej po rozwiązania, urządzenia i narzędzia bazujące na najnowszych osiągnięciach nauki i techniki. Tym samym pojawiają się nowe tendencje związane z oszustwem popełnionym przy wykorzystaniu wschodzących technologii (*emerging technologies* [ET]). Warto je przeanalizować, w szczególności z perspektywy możliwości ich wykorzystania do celu oszustwa. W tym zakresie zaś prym wiedzie sztuczna inteligencja (*artificial intelligence* [AI]), chociaż w czołówce plasuje się także technologia *blockchain* (Howarth, 2024). Trzeba też dodać, że zagadnienia poruszone w tym artykule, ograniczonym objętościowo, nie wyczerpią tej problematyki. Nie byłoby bowiem możliwe kompleksowe jej omówienie ani z perspektywy technologicznej, ani nawet kryminologicznej. Równie istotna wydaje się przy

[1] Zob. np. portal GS24.pl, https://gs24.pl/tag/cyber-oszustwo, czy Głos Wielkopolski, https://gloswielkopolski.pl/tag/cyber-oszustwo

tym kwestia regulacji dotyczących zapobiegania cyberoszustwu popełnionemu z wykorzystaniem nowoczesnych technologii. Tymczasem, jak potwierdzają badania przeprowadzone w 2023 r. przez Global Anti-Scam Alliance (GASA) we współpracy ze ScamAdvisor, żaden kraj nie wdrożył dotychczas takich rozwiązań prawnych i technicznych, które pozwalałyby na uczynienie go wzorem w walce z tym procederem (Abraham, 2022; Consumers International Congress, 2023; Greening, 2022)[2]. Wobec tego należy też poddać analizie poczynania krajowego ustawodawcy, skoro w 2023 r. została uchwalona ustawa dedykowana walce z nadużyciami w komunikacji elektronicznej. Nabiera ona znaczenia zwłaszcza w odniesieniu do zapobiegania cyberszustwom. Mając na względzie aspekt prewencyjny, poza zakresem analizy pozostaje pozostawić przepisy karnomaterialne, szczególnie że określone w nich typy czynów zabronionych zasługują na poświecenie im miejsca w odrębnym opracowaniu. Tym samym w artykule omówiono aspekty związane z tendencjami w zakresie oszustwa popełnionego w cyberprzestrzeni przy wykorzystaniu ET tudzież wątpliwości prawne, jakie mogą one wywoływać z perspektywy zapobiegania takim czynom.

II. ETYMOLOGIA POJĘCIA CYBEROSZUSTWA

W pierwszej kolejności należałoby wyjaśnić pojęcie *cyberoszustwa*. W tym względzie kluczowe jest stwierdzenie, iż stanowi ono rodzaj cyberprzestępstwa (Opitek, 2023, s. 202–223), a zatem do jego popełnienia dochodzi w specyficznej przestrzeni, jaką jest cyberprzestrzeń. Z kolei ten termin jest stosunkowo powszechnie stosowany, i to nie tylko przez specjalistów z branży IT. Poza informatykami (Dela, 2020, s. 35) posługują się nim m.in. socjolodzy i prawnicy (Aleksandrowicz, 2016, s. 11–12; Lakomy, 2015, s. 93–102; Worona, 2020, s. 29–31). Ci pierwsi uznają, że *cyberprzestrzeń* to ludzka, zbiorowa zdolność do artykułowania możliwości, w których artefakty technologiczne są projektowane, używane i konceptualizowane (Mbanaso i Dandaura, 2015, s. 18). Cyberprzestrzeń jest obecnie również pojęciem prawnym. Jej definicje legalne zawarto w kilku aktach prawnych. Bazując na nich, można uznać, iż jest to przestrzeń przetwarzania i wymiany informacji, tworzona przez systemy teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami[3]. Podejście, w którym akcentuje się specyfikę cyberprzestrzeni jako obszaru działalności człowieka, uzasadnia nomenklaturę odnoszącą się do cy-

[2] Badania przeprowadzone przez Global Anti-Scam Alliance (GASA) dotyczyły oszustwa w cyberprzestrzeni i uczestniczyło w nich ponad 200 ekspertów zajmujących się tą problematyką oraz 4430 konsumentów z całego świata.

[3] Ustawa z 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) wprowadziła definicję legalną cyberprzestrzeni do art. 2 ust. 1b ustawy z 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (t.jedn.: Dz. U. 2022, poz. 2091), art. 2 ust. 1a ustawy

berprzestępstwa jako czynu, do którego dochodzi w obszarze cyberprzestrzeni (Zych, 2019, s. 116). W literaturze wskazuje się przy tym również na wykorzystanie technologii informatycznych i Internetu do podejmowania działalności przestępczej (Mehan, 2014, s. 67; Siwicki, 2012, s. 249–251). Warto dodać, że niekiedy rozróżnia się wąskie oraz szerokie ujęcie cyberprzestępstwa. W pierwszym mianem tym zwykło się określać to, co stanowi synonim cyberataku (przy uwzględnieniu wielu jego form). Natomiast w szerokim rozumieniu (stanowiącym odpowiednik *cyber-enabled crimes*), obejmuje ono „tradycyjne" przestępstwa, które są „ułatwiane albo wzmacniane przez Internet" (Interpol, 2020, s. 12). Innymi słowy, chodzi o te przestępstwa, w których Internet odgrywa kluczową rolę przy ich popełnieniu, będąc narzędziem (środkiem) umożliwiającym w ogóle realizację znamion albo to ułatwiający. W tej kategorii pojęciowej najczęściej wymienia się: *scamming* (Golonka, 2022, s. 291–295)[4], *phishing*[5], wyłudzenia związane z bankowością elektroniczną, piramidy finansowe, a także nielegalny handel ludźmi lub narządami i organami ludzkimi (Bertrand, 2000, s. 39–47; Hoffmann, 2018, s. 14–28; Interpol-Raport, 2020, s. 20–32; Kumar, 2020, s. 79–179; McQuade, 2021, s. 34–35; Rahman, 2020, s. 67–71). Tym samym ta kategoria pojęciowa (*cyber-enabled crimes*) obejmuje szeroką gamę czynów.

Należałoby też dodać, że w wypadku cyberoszustw ich cechą wspólną będzie również wprowadzenie w błąd (w formie czynnej lub biernej), jako immanentna cecha oszustwa (Abagnale, 2020; Oczkowski, 2004; Siwicki, 2018). Należy zauważyć, że cyberprzestępstwa nie należy traktować jako synonimu przestępstwa komputerowego. To drugie pojęcie jest znaczeniowo szersze, ponieważ obejmuje również czyny z wykorzystaniem komputera bez połączenia z siecią teleinformatyczną (Lewulis, 2021, s. 24).

Mając na uwadze powyższe, wolno uznać, że cyberoszustwo oznacza oszustwo popełnione w cyberprzestrzeni i jako takie stanowiące jedno z cyberprzestępstw. Problematyka poruszana w tym opracowaniu przemawia dodatkowo za uwzględnieniem cyberprzestępstwa w jego szerokim rozumieniu (*cyber-enabled crime*). Taka optyka pozwala na podjęcie analizy wykorzystania ET przez cyberoszustów. Tym bardziej że statystyki wskazują na stałą tendencję wzrostową w tym zakresie (Hodges, 2024).

---

z 21 czerwca 2002 r. o stanie wyjątkowym (t.jedn.: Dz. U. 2017, poz. 1928) oraz art. 3 ust. 1 pkt 4) ustawy z 18 kwietnia 2002 r. o stanie klęski żywiołowej, t.jedn.: Dz. U. 2017, poz. 1897.

[4] *Scamming* to forma oszustwa, w której sprawcy za pomocą manipulacji polegającej na zastosowaniu sztuczek perswazyjnych składają wprowadzające w błąd obietnice osiągnięcia korzyści majątkowej lub osobistej.

[5] *Phishing* polega: „na masowym wysyłaniu e-maili kierujących na fałszywą stronę, łudząco przypominającą oryginalną, która w rzeczywistości przechwytuje informacje wpisywane przez użytkownika", a celem jest: „uzyskanie poufnych danych poprzez podszywanie się pod podmioty i instytucje, zwykle znane i zaufane (takie jak banki, sklepy internetowe, serwisy aukcyjne, serwisy pocztowe" (Radoniewicz, 2016, s. 95–96, 107). W innym ujęciu *phishing* (od *password harvesting fishing* – łowienie haseł) to rodzaj oszukańczego pozyskania poufnych informacji osobistych przez podszywanie się pod osobę lub instytucję godną zaufania (Murszewski, 2023, s. 642).

III. CYBEROSZUSTWO Z WYKORZYSTANIEM NOWOCZESNYCH TECHNOLOGII – TENDENCJE ZJAWISKA

Rozważania wypada rozpocząć od ukazania tendencji, zwanych „trendami" kryminologicznymi (Focal Team, 2025), dotyczących cyberoszustwa. Pozwolą one na ukazanie zagrożeń wynikających z coraz powszechniejszego wykorzystania ET przez sprawców oszustwa popełnionego w cyberprzestrzeni, a w dalszej kolejności na odniesienie się do problematyki prawnej. W tym względzie preferowane są przez nich te sposoby, które prowadzą do nawiązania bezpośredniego kontaktu z potencjalnym pokrzywdzonym. Odnosi się to – być może paradoksalnie – również do cyberoszustwa. Wówczas sprawcy korzystają z urządzeń lub technologii pozwalających na imitowanie połączenia z konkretną, faktycznie istniejącą osobą. W tym celu sięgają po różne metody i techniki. Należą do nich w szczególności takie, które umożliwiają im stworzenie pozorów połączenia przychodzącego z konkretnego numeru telefonicznego, np. od osoby najbliższej; na zniekształcenie połączenia głosowego w taki sposób, aby stworzyć pozory, że pochodzi ono od konkretnego abonenta. Sprawcy wykorzystują przekierowanie (precyzyjniej – stosują tzw. SIM *swapping*), dzięki czemu omijają operatora rejestrującego połączenie. Aktualnie korzystają nawet ze sztucznej inteligencji do przeprowadzenia rozmowy telefonicznej służącej oszustwu, bazując na stosownych algorytmach (*audio-deepfake*), o czym poniżej.

Gdy chodzi o wprowadzenie w błąd co do numeru, z którego jest realizowane połączenie telefoniczne (*caller ID spoofing*), zwane CLI *spoofingiem*, to opiera się ono na użyciu bramek VoIP (*Voice over Internet Protocol*). Są to urządzenia (technologie), które konwertują głos na sygnał cyfrowy, umożliwiając wykonywanie połączeń bezpośrednio z komputera, telefonu VoIP lub innych urządzeń obsługujących dane. CLI *spoofing,* sam w sobie, z całą pewnością nie należy ani do zjawiska nowego, ani mało znanego, tudzież rzadko spotykanego (Gryszczyńska, 2023). Natomiast zaawansowane rozwiązania technologiczne pozwalają na coraz bardziej wyrafinowane sposoby nadawania pozorów rzeczywistego kontaktu telefonicznego dzięki wykorzystaniu sztucznej inteligencji. Przykładem może być *voice scamming*[6], stanowiący specyficzną formę cyberoszustwa, w której *scamming* jest połączony z klonowaniem tembru brzmienia głosu – tzw. *voice cloning-scam* (Skipper, 2025). Proceder ten jest coraz częściej obserwowany w praktyce (Saeidi i in., 2024). Jego sprawcy – w sposób właściwy dla scammingu, stosują zarówno socjotechniki wprowadzające w błąd (najczęściej związane z wywołaniem presji czasowej na spełnienie ich żądania przekazania pieniędzy lub wywołaniem panicznego strachu o – rzekomo dzwoniącą – osobę najbliższą znajdującą się w krytycznej sytuacji), jak i korzystają przy tym z zaawansowanych algorytmów. Te ostatnie, przy wykorzystaniu uczenia maszynowego

[6] Eksperyment, który wykazał, jak trudno rozpoznać oszustwo w formie AI Scam został przeprowadzony przez specjalistę w dziedzinie Cybersecurity – prof. O. Buckleya z University of East England i zaprezentowany przez BBC (2023).

(*machine learning* [ML]), nawet na podstawie kilku słów nagranych w trakcie krótkiej rozmowy odbytej z osobą, której głos będzie stanowił wzór do wykreowania sklonowanego połączenia głosowego, są w stanie imitować go następnie w trakcie odbytego już „na żywo" połączenia telefonicznego – naturalnie po odpowiedniej modyfikacji, zgodnej z oczekiwaniami scammerów. Algorytmy są tworzone najczęściej przy wykorzystaniu technologii *deep learning* (DL), czyli rodzaju ML, w którym uczenie odbywa się przez doświadczanie i rozumienie świata w kategoriach hierarchii pojęć. Wspomniane systemy sztucznie wykreowanych sieci neuronowych pozwalają na symulowanie mechanizmu działania zbliżonego do ludzkiego mózgu, dzięki czemu są one w stanie odpowiednio odbierać i przetwarzać zasób dostarczonych informacji (Kaplan, 2025, s. 47–52; Wang, 2021). Precyzyjniej zaś, jak dowodzą badania, w przypadku voice-scammingu zazwyczaj bazuje się (poza sieciami typu Koder-Dekoder, *encoder-decoder networks* [ED]), na generatywnych sieciach przeciwstawnych – jako architekturze DL (*Generative Adversarial Network* [GAN]), splotowych sieciach neuronowych (*Convolutional Neural Network* [CNN]), a także głębokich sieciach neuronowych (*Deep Neural Network* [DNN]; Khanjani i in., 2023). Innym sposobem zdobycia wzorca wokalnego jest również „kradzież" głosu na potrzeby ich późniejszego wykorzystania do planowanego oszustwa, co może mieć miejsce np. w trakcie połączenia z przedstawicielem banku, nagranego mikrofonem z dalekiego pola ofiary, następnie odtworzonego na słuchawce telefonu z głośnikiem (w atakach typu *far field detection*; Prenger i in., 2019, s. 3617–3621). Warto dodać, że specjaliści w dziedzinie rozwiązań technologicznych zwykli zaliczać *voice cloning-scam* do *audio-deepfake*, czyli dźwięków (treści wokalnych), które są syntetycznie wygenerowane lub manipulowane za pomocą sztucznej inteligencji (AI) w taki sposób, aby wiernie odzwierciedlały prawdziwe (Khanjani i in., 2023).

Analizując problematykę tendencji w zakresie spoofingu, warto zwrócić także uwagę na rosnące w gwałtownym tempie incydenty związane z podszywaniem się pod Automatyczne Systemy Identyfikacji (AIS)[7], tzw. AIS *spoofing*. Systemy takie, początkowo używane do unikania kolizji w transporcie morskim, obecnie pełnią nie tylko funkcje związane z lokalizacją (nadawaniem pozycji statku), ale też zawierają szereg danych, takich jak tożsamość dostawców. *Spoofing* w tym przypadku polega na fałszowaniu komunikatów w systemie AIS i przez to wprowadzanie w błąd statków, operatorów żeglugi morskiej, a nawet władz odpowiedzialnych za transport morski (Androjna i in., 2021). W rezultacie manipulacji sprawcy mogą np. tworzyć „statki widma", zaciemniać prawdziwy ruch w żegludze lub symulować ruchy floty. Konsekwencje tego mają zaś wymiar nie tylko jednostkowy – szkoda pojedynczego przedsiębiorcy, czy więcej – zagrożenia dla życia i zdrowia załogi, ale nawet mogą wpływać na wyniki ekonomiczne regionu, czy wręcz całego państwa lub godzić w jego bezpieczeństwo narodowe (Ampatzidis, 2024).

[7] Statystyki potwierdzają wzrost o 400% w skali globalnej (październik 2022 – kwiecień 2023) i wskazują jako podatne na zagrożenie żeglugi: Rosji, Grecji, ZEA, Kuwejtu, Iranu, Arabii Saudyjskiej, Wietnamu i Norwegii (Ampatzidis, 2024).

Coraz częściej notowanym procederem staje się również SIM *swapping* (zwany także SIM hijackingiem). Jest to oszustwo polegające na skopiowaniu karty SIM w celu przejęcia subskrypcji usługi mobilnej, a przez to uzyskania dostępu do poufnych danych osobowych i finansowych. Badania prowadzone pod kątem zagrożeń, jakie stwarza ten rodzaj procederu, potwierdziły nie tylko wagę zagrożenia i możliwe skutki wykorzystania uzyskania nieautoryzowanego dostępu do sieci teleinformatycznych, ale także to, co m.in. przesądza o specyfice SIM *swap*, czyli jego powiązaniu z kradzieżą danych osobowych i wykorzystaniu fałszywie uzyskanej usługi mobilnej do popełnienia przestępstwa (Kim i in., 2022). O przypadki SIM swappingu nietrudno także w polskich realiach. Tytułem przykładu można wskazać na ten, jaki był objęty śledztwem prowadzonym pod nadzorem Prokuratury Regionalnej w Poznaniu przez Zarząd w Poznaniu Centralnego Biura Zwalczania Cyberprzestępczości, dotyczącym sprawców przestępstw internetowych działających w ramach zorganizowanej grupy przestępczej. Jak podaje policja, w tej sprawie 12 lipca 2024 r. skierowano do SO w Warszawie akt oskarżenia, którym objęto łącznie 12 osób oskarżonych m.in. o przeprowadzanie w latach 2018–2021 czynów polegających na przełamywaniu zabezpieczeń systemów bankowości elektronicznej oraz bezprawnym pozyskiwaniu loginów i haseł dostępowych do rachunków rozliczeniowych osób fizycznych i prawnych, przy wykorzystaniu metody tzw. SIM *swap*, oraz kradzieży tożsamości, przy wykorzystaniu podrobionych dokumentów tożsamości[8]. Szkody wynikające z popełnionych przestępstw szacuje się na kwotę ponad 18 mln zł, z tym że sprawcy – jak podaje policja, usiłowali przejąć środki pieniężne w łącznej kwocie 26 mln zł. Jeżeli mieć zaś na względzie aspekt SIM swappingu związany z samą doniosłością zagrożenia, to wypada wskazać, że jest on zaliczany do zaawansowanych trwałych zagrożeń (*advanced persistent threat* [APT])[9]. Chodzi o ten rodzaj cyberzagrożeń, w których ataki są przeprowadzane przy udziale władz państwowych lub zorganizowanych grup działających na ich zlecenie. Mają one charakter zmasowanych ataków przy wykorzystaniu danych dostępnych na kartach SIM (Che Mat i in., 2024, s. 3–16), a celem działania sprawców jest uzyskanie nieautoryzowanego dostępu do kont rozliczeniowych, jak również do danych ich posiadaczy. Nie powinno budzić wątpliwości, że proceder ten staje się wyzwaniem, zwłaszcza w dobie coraz powszechniejszego użycia e-SIM. W kontekście nowoczesnych technologii, przede wszystkim technologii *blockchain* (*blockchain technology* [BT]), proceder SIM swappingu jest wiązany z transakcjami kryptowalutowymi (Kim i in., 2022, s. 240). Wiele giełd kryptowalut wykorzystuje uwierzytelnianie dwuskładnikowe SMS (SMS 2FA) lub inne metody uwierzytelniania (*MFA authentication*) wieloskładnikowego, które opierają się na karcie SIM

[8] Akt oskarżenia w sprawie kradzieży przy wykorzystaniu SIM swappingu Policja.pl (2024).

[9] Przykładem APT są ataki przeprowadzane przez powiązaną z Rosją grupę hakerów Gamaredon (znaną jako: Aqua Blizzard, Armageddon, Shuckworm, UAC-0010) na ukraińską infrastrukturę. Polegały na uzyskaniu dostępu do kont elektronicznych celem eksfiltracji danych, wektorem ataku były głównie e-maile na konta służbowe pracowników lub wiadomości w komunikatorach: Telegram, WhatsApp, Signal, wysyłane przy użyciu wcześniej przejętych kont (Kapitan Hack, 2023; Palczewski, 2023).

użytkownika, a po uprzednim sklonowaniu lub podmianie karty SIM sprawca cyberoszustwa zyskuje pełny dostęp do dowolnej usługi, dla której zastosowano kartę SIM celem uwierzytelnienia dostępu do niej (Hallman, 2023, s. 4). Przy okazji warto zwrócić uwagę na możliwości ich wykorzystania nie tylko do popełnienia oszustwa (Opitek, 2024, s. 224–229), ale również (na jego bazie jako czynu pierwotnego) do prania pieniędzy (Golonka, 2024, s. 213–216). Wykorzystuje się przy tym miksery kryptoaktywów, głównie kryptowalut. Proceder zazwyczaj polega na wykorzystaniu „tradycyjnych" metod (Trozze i in., 2022, s. 12), jak np. *spoofing,* połączony z wykorzystaniem bramek FCT (*fixed-cellular terminals*), tzw. simboxów, pozwalających na wykonanie połączenia telefonicznego przy podszywaniu się pod inną osobę lub firmę. Jej numer jest także wykazywany jako inicjujący połączenie. Następnie, po nawiązaniu kontaktu z potencjalnym klientem, sprawcy polecają zainstalować oprogramowanie do obsługi transakcji kryptowalutowych. W istocie służy ono jednak wyłącznie do uzyskania danych poufnych (np. umożliwiających dostęp do konta bankowego). Jest to więc program typu *backdoor*. Na dalszym etapie, po uzyskaniu dostępu do konta ofiary, przeprowadzane są transakcje na walucie fiducjarnej, prowadzące do jej zamiany na walutę wirtualną. Na takim *modus operandi* opierali się zresztą sprawcy stosunkowo głośnego medialnie przypadku oszustwa. Chodzi o osoby działające w zorganizowanej grupie przestępczej na obszarze Polski i Ukrainy, które za pośrednictwem fałszywych inwestycyjnych platform internetowych: aspenholding.com, olympusmarkets.com, lvgrowmarkets.com oraz gorisemarkets.com oferowały zakup kryptowaluty – bitcoina, finalnie doprowadzając ponad 600 osób do niekorzystnego rozporządzenia mieniem, którego straty oszacowano na ponad 40 mln zł (Prokuratura Krajowa, 2024).

Niemniej, poza „inwestycyjnymi" formami cyberoszustwa kryptowalutowego (włączając te typu *pig butchering*, czyli oparte na wykorzystaniu relacji z osobą oszukaną budowanej po to, by zaangażowała się ona na dłuży czas lub na większe sumy w inwestycję), obecnie stosowane jego formy bazują także na sztucznej inteligencji. W tym zakresie proceder może przybrać różne oblicza. Sztuczna inteligencja jest wykorzystywana zarówno w schemacie: *pump-and--dump,* gdzie algorytmy służą do manipulacji związanych ze sztucznym pompowaniem i „zrzucaniem" wartości rynkowej kryptowaluty (Sabry i in., 2020, s. 175855), jak i do generowania fałszywych treści (*deepfake*). W tym drugim przypadku sztuczna inteligencja, uwzględniając chat GPT, jest wykorzystywana do celu reklamy kryptowalutowego projektu inwestycyjnego. Klienci są zachęcania do udziału za pomocą fałszywie wygenerowanych wizerunków znanych osób, a nawet wytworzonych hologramów dyrektorów firm inwestycyjnych, z którymi można „omówić" w bezpośredniej rozmowie udział w „intratnym" projekcie. Ponadto AI służy do generowania fałszywych tokenów (*initial coin offering* [ICO]), a ściślej – promowania rzekomo istniejących (Akartuna, 2024, s. 11, 13, 16–18).

W odniesieniu do tendencji w zakresie cyberoszustwa nie sposób wreszcie pominąć problemu generowania syntetycznej tożsamości (*synthetic identity theft* [SIT]). Proceder ten jest zazwyczaj połączony z kradzieżą (autentycznej)

tożsamości. Jego istota sprowadza się do wykreowania nowej – syntetycznej – tożsamości za pomocą AI (Mungai, 2024, s. 3). „Dane osobowe" powstają przez odpowiednie połączenie danych osobowych autentycznej osoby (zazwyczaj uzyskane w nielegalny sposób) oraz zbioru danych wygenerowanych dzięki zastosowaniu nowoczesnych technologii. Przykładowo, opierając się na badaniach empirycznych, syntetyczne rekordy danych osobowych zostają wygenerowane przy użyciu biblioteki Faker Pythona (Faker Python Library), a bazą są autentyczne dane, takie jak: adresy e-mail, hasła, nazwy użytkowników, adresy IP, numery telefonów i informacje o kartach kredytowych, uzyskane w nielegalny sposób. Hasła są zaczerpnięte z listy haseł „rockyou.txt". Miasto, stan i kod pocztowy zostały przypisane losowo do rekordów za pomocą biblioteki Python „pyzipcode". Kody kierunkowe (dla USA) są pobierane z North American Numbering Plan Administrator (NANPA; Sharma i Bantan, 2025). Sama biblioteka Faker Pytona (m.in. dzięki obsłudze algebry liniowej oraz transformacji Fouriera) korzysta z algorytmów – uczenia maszynowego i sztucznej inteligencji (Chelliah, 2025), co z kolei ma służyć ułatwieniu i szybszemu korzystaniu z jej biblioteki – NumPy. W praktyce jednak służy także do kreowania syntetycznego zestawu danych (czy wręcz nowej tożsamości), nierzadko w przestępnym celu. Taka syntetyczna tożsamość może być bowiem wykorzystana w obrocie gospodarczym do różnych celów, w szczególności zaś może ona udawać reprezentanta inwestora, przedstawiciela firmy itd. Oczywiście w omawianym kontekście każda z tych „ról" będzie ukierunkowana na wprowadzenie w błąd innej osoby.

Wspomniany proceder – kreowania SIT – wydaje się tylko jednym z aspektów dotyczących możliwości wykorzystania zaawansowanych technologii do cyberoszustwa. Coraz chętniej wykorzystywane dane biometryczne człowieka do personalizacji ustawień i, *nomen omen*, zapewnienia bezpieczeństwa, mogą bowiem także podlegać zarówno kradzieży (Roberts, 2007, s. 14–25), jak i „wytworzeniu" danych biometrycznych. Innymi słowy, wzorem SIT, za pomocą AI mogą zostać wygenerowane syntetyczne dane biometryczne. Stosowanie danych biometrycznych w obrocie gospodarczym staje się coraz powszechniejsze w obszarze technologii *cybersecurity*. Paradoksalnie jednak, jak dowodzą badania naukowe, dane biometryczne mogą zostać również skradzione, przerobione lub podrobione (Jain i Kant, 2015, s. 284–288), a biorąc pod uwagę tendencje w zakresie przestępczości związanej z możliwościami wykorzystania sztucznej inteligencji – mogą zostać wykorzystane do wytworzenia syntetycznych danych, a następnie służyć do popełnienia cyberoszustwa[10].

[10] Akt o sztucznej inteligencji przewiduje, że systemy AI służące „identyfikacji biometrycznej osób zaangażowanych w działalność przestępczą lub objętych dochodzeniami muszą spełniać rygorystyczne wymogi i obowiązki, aby mogły uzyskać dostęp do rynku UE", a „stosowanie systemów zdalnej identyfikacji biometrycznej w czasie rzeczywistym, takich jak rozpoznawanie twarzy w przestrzeni publicznej przez organy ścigania" jest w ogóle zakazane (jako stwarzające ryzyko nieakceptowalne – w czteropoziomowej skali ryzyka związanego z wykorzystaniem AI). Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE)

IV. PRAWNE ASPEKTY PRZECIWDZIAŁANIA OPISANYM PROCEDEROM

Opisane wyżej procedery stanowią wyzwanie nie tylko dla specjalistów w dziedzinie IT. Ich działania koncentrują się bowiem przede wszystkim na opracowaniu narzędzi, które wykorzystując możliwości ET, pozwalają zapobiegać atakom – głównie na systemy finansowe (Sharma, 2024). W ślad za tymi działaniami powinny podążać także inne, w szczególności związane z budowaniem świadomości społecznej w zakresie zagrożeń, jakie stwarza rozwój nowoczesnych technologii, tudzież socjotechnik, jakie pozostają immanentną cechą wielu procederów oszustwa. Poza tym jednak nie sposób byłoby zapobiegać cyberoszustwom bez stworzenia należytych ram prawnych. W tym względzie działania ustawodawcy podążają w dwóch kierunkach: po pierwsze, są one nastawione na prewencję; po wtóre, na zwalczanie cyberoszustwa. Poniżej zostaną zaprezentowane uwagi odnoszące się do pierwszego aspektu.

W tej mierze, co wypada zauważyć, asumptem do opracowania unormowań krajowych były regulacje Unii Europejskiej. W omawianym względzie dotyczy to ustawy o zwalczaniu nadużyć w komunikacji elektronicznej[11], której uchwalenie stanowi wyraz implementacji do krajowego porządku prawnego postanowień dyrektywy UE 2018/1972 ustanawiającej Europejski kodeks łączności elektronicznej[12]. Unijny akt prawny nakłada na dostawców publicznych sieci łączności elektronicznej lub publicznie dostępnych usług łączności elektronicznej m.in. obowiązki dotyczące wprowadzenia środków w celu ochrony bezpieczeństwa sieci lub usług, a także zapobiegania skutkom incydentów związanych z bezpieczeństwem lub ich minimalizacją. Dyrektywa 2018/1972 przewiduje raczej ogólne postanowienia, z których wynika, że środki te powinny zapewniać poziom bezpieczeństwa (sieci i usług) „proporcjonalny do istniejącego ryzyka z uwzględnieniem aktualnego stanu wiedzy i technologii". Przy tym przy ich opracowywaniu należy brać pod uwagę „co najmniej wszystkie stosowne aspekty następujących kwestii: w odniesieniu do bezpieczeństwa sieci i urządzeń – bezpieczeństwo fizyczne i bezpieczeństwo środowiska, bezpieczeństwo dostaw, kontrola dostępu do sieci i integralność sieci; w odniesieniu do postępowania w przypadku incydentów związanych z bezpieczeństwem – procedury postępowania w przypadku incydentu związanego z bezpieczeństwem, zdolności wykrywania incydentów, zgłaszanie incydentów związanych z bezpieczeństwem i informowanie o nich; […] w odniesieniu zaś do monitorowania, kontroli i testowania – strategie monitorowania i rejestrowania, ćwiczenia w zakresie planów awaryjnych, testowanie sieci i usług, oceny bezpieczeństwa i monitorowanie zgodności" (pkt 94).

2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji). Tekst mający znaczenie dla EOG (Dz. Urz. UE L 1689, 13.06.2024, s. 1–112).

[11] Ustawa z 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej, t.jedn.: Dz. U. 2024, poz. 1803 (dalej jako: u.z.n.k.e.).

[12] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z 11 grudnia 2018 r. – Europejski kodeks łączności elektronicznej (wersja przekształcona), Dz. Urz. UE L 2018, nr 321, s. 36, ze zm. (dalej jako: dyrektywa 2018/1972).

Ustawa o zwalczaniu nadużyć w komunikacji, czyniąc zadość regulacjom zawartym w dyrektywie 2018/1972, wprowadza rozwiązania prawne mające na celu zapobieganie i zwalczanie nadużyć w komunikacji elektronicznej, polegających m.in. na: wysłaniu krótkiej wiadomości tekstowej (SMS), w której nadawca podszywa się pod inny podmiot w celu nakłonienia odbiorcy tej wiadomości do określonego zachowania, w szczególności przekazania danych osobowych, niekorzystnego rozporządzenia mieniem, otwarcia strony internetowej, inicjowania połączenia głosowego lub instalacji oprogramowania – *smishing* (art. 3 pkt 2 u.z.n.k.e.) oraz na nieuprawnionym posłużeniu się lub korzystaniu przez użytkownika lub przedsiębiorcę telekomunikacyjnego wywołującego połączenie głosowe, informacją adresową wskazującą na osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej inną niż ten użytkownik lub przedsiębiorca telekomunikacyjny, służące podszyciu się pod inny podmiot, w szczególności w celu wywołania strachu, poczucia zagrożenia lub nakłonienia odbiorcy tego połączenia do określonego zachowania, zwłaszcza do przekazania danych osobowych, niekorzystnego rozporządzenia mieniem lub instalacji oprogramowania CLI *spoofing* (art. 3 pkt 3 u.z.n.k.e.). Ustawodawca uznał, że środkami do tego są, w szczególności: monitorowanie występowania smishingu przez Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT NASK) na podstawie informacji otrzymanych od odbiorców SMSów, tworzenie wzorów wiadomości stanowiących przejawy tego procederu, obowiązek przedsiębiorców telekomunikacyjnych blokowania wiadomości odpowiadających takiemu wzorowi za pomocą systemu teleinformatycznego pozwalającego na automatyczną identyfikację takich wiadomości oraz nadpisu SMS (czyli identyfikatora SMS, używanego przez podmioty publiczne, np. urzędy skarbowe). Niezależnie od tego u.z.n.k.e. przyznaje przedsiębiorcom telekomunikacyjnym uprawnienie (a więc fakultatywnie) do blokowania wiadomości MMS, „w których nadawca podszywa się pod inny podmiot w celu nakłonienia odbiorcy tej wiadomości do określonego zachowania" (art. 9 u.z.n.k.e.). Poza tym: „W celu zapobiegania i zwalczania CLI spoofing przedsiębiorca telekomunikacyjny blokuje połączenie głosowe albo ukrywa identyfikację numeru wywołującego dla użytkownika końcowego" (art. 16 u.z.n.k.e.). Przedsiębiorca taki, realizując nałożone na niego obowiązki, „stosuje środki organizacyjne i techniczne służące monitorowaniu, wykrywaniu oraz wymianie informacji o CLI spoofing, a także blokowaniu połączenia głosowego albo ukrywaniu identyfikacji numeru wywołującego dla użytkownika końcowego" (art. 19 ust. 1u.z.n.k.e.). Ustęp 2 tego artykułu przewiduje jednak, że „dostawca publicznie dostępnych usług telekomunikacyjnych", który: a) jest jednocześnie operatorem usług telekomunikacyjnych, b) świadczy usługi telekomunikacyjne dla co najmniej 50 000 abonentów, może zawrzeć z Prezesem UKE porozumienie określające szczegółowo owe środki.

Przytoczone regulacje u.z.n.k.e. pozwalają na stwierdzenie, że poza chwalebnym dostrzeżeniem rangi zagrożenia, tudzież potrzeby zapobiegania przejawom smishingu i CLI spoofingu, ustawa ta nie przewiduje unormowań przystosowanych do wyzwań, jakie stwarza i wykorzystanie ET w tych procederach. Przede wszystkim nakłada ona obowiązki na przedsiębiorcę teleko-

munikacyjnego. Wobec tego wyklucza zagrożenia (kolokwialnie rzecz ujmując) typu: maszyna–maszyna. Należy zauważyć, że nadużycia w komunikacji elektronicznej (np. *smishing*) przy wykorzystaniu sztucznej inteligencji mogą stosunkowo łatwo i szybko omijać „wzory" opracowane na podstawie informacji dostarczonych przez przedsiębiorców telekomunikacyjnych do CSIRT NASK. Z kolei redakcja przepisów nie przewiduje faktu blokowania („blokuje się"), a wymaga uprzednio pewnych ustaleń, w tym tego, że „nadawca podszywa się pod inny podmiot" (*arg. ex* art. 3 pkt 2 u.z.n.k.e.). Pewien niedosyt może budzić nałożenie powinności zapobiegania zjawiskom w całości na przedsiębiorców telekomunikacyjnych, chociaż docelowo – jak wolno uznać – znacznie lepszym rozwiązaniem byłoby przekazanie zadań związanych w szczególności z monitorowaniem oraz monitowaniem o zagrożeniu organowi centralnemu, z możliwością chociażby wstępnego zablokowania przez niego określonych treści, obrazów lub dźwięków. Podejście to opiera się na założeniu, co oczywiste, że jego działania byłyby wspierane przez narzędzia umożliwiające bieżący monitoring, analizę, przetwarzanie w czasie rzeczywistym. Chodzi o stosowne algorytmy (bazujące na AI i ML), chociażby takie, jak te „wzorowane" na detektorach sztucznej inteligencji (co do celu ich działania). Natomiast bardziej zaawansowane technologie uczyniłyby realnym zapobieganie nie tylko obecnie znanym i ujawnianym nadużyciom w komunikacji elektronicznej, ale również takim, które dopiero mogą wystąpić – stosownie do dynamiki cechującej postęp w rozwoju nowoczesnych technologii i równie „postępowych" działań sprawców z nich korzystających.

Pozostając przy podniesionych wyżej przykładach wykorzystania nowoczesnych technologii do celu cyberoszustwa, wypada również zauważyć, że regulacje przewidziane w u.z.n.k.e. nie obejmują tych przypadków, w których doszłoby do użycia sztucznie wytworzonych danych – zwłaszcza syntetycznej tożsamości. Nie wydaje się bowiem, aby w takiej sytuacji doszło do podszycia się pod „inną osobę", skoro takiej osoby w rzeczywistości nie ma. Wobec tego jedynymi regulacjami, jakie mogłyby wówczas znaleźć zastosowanie, byłyby te, które odnoszą się *stricte* do odpowiedzialności cywilnej lub karnej – nie zaś do przeciwdziałania zjawisku, a i one, co wypada zaznaczyć, *de lege lata* nasuwają zastrzeżenia. Część z nich, m.in. kradzież tożsamości, doczekała się nawet stosownych opracowań (Radoniewicz, 2024). O innych sygnalizowano w piśmiennictwie – jak chociażby o możliwościach wykorzystania AI do celu zwalczania zjawiska (Adebola i in., 2024, s. 290) lub o dylematach związanych z odpowiedzialnością karną za *deepfake* (Garcia-Vera, 2024; Harris, 2019; Ziobroń, 2021, 2024). W nawiązaniu do zaprezentowanych w niniejszym artykule możliwości wykorzystania w tej mierze sztucznej inteligencji, warto jedynie dodać, że dotyczy to także procederu *voice cloning* (modyfikacji głosu za pomocą AI, w tym jego kradzieży). Gdy zaś chodzi o uprawnienia „dostawcy publicznie dostępnych usług telekomunikacyjnych" (do zawarcia porozumienia z Prezesem UKE – art. 19 ust. 2 u.n.n.k.e.), nie wydaje się ono właściwe. Wynika to z tego, że – po pierwsze, wiąże się z realizacją obowiązku nałożonego na przedsiębiorcę telekomunikacyjnego, o którym mowa w ust. 1 (a pojęcia te nie są zakresowo identyczne), a po drugie, nie przewidziano nawet definicji

legalnej takiego dostawcy (w u.z.n.k.e. jest mowa jedynie o dostawcy poczty elektronicznej, co z pewnością nie jest tożsame). Z kolei uprawnienie przedsiębiorcy telekomunikacyjnego do blokowania MMS-ów może budzić obiekcje związane z koniecznością wykazania celu podszywania się (MMS-y można blokować tylko wówczas, gdy dochodzi do podszywania się oraz gdy służy to konkretnemu celowi). Nie ma tam miejsca np. na uzasadnione podejrzenie przedsiębiorcy, że *in concreto* mogło dojść do takiego podszywania się.

Analizując problematykę związaną z prewencją przed cyberoszustwem, nie sposób byłoby pominąć jeszcze jednej kwestii, a mianowicie tego, że postęp technologiczny prowadzi do specyficznego zacierania się granicy pomiędzy fikcją a rzeczywistością. W niektórych przypadkach prezentowania dóbr i usług w obrocie gospodarczym bywa ona wręcz trudna do wychwycenia przez odbiorcę, zwłaszcza gdy wykorzystuje się przy tym takie technologie, jak rzeczywistość rozszerzona czy wirtualna (Rampolla i Kipper, 2012). Uzasadnia to wątpliwości dotyczące samej możliwości wprowadzenia w błąd lub wyzyskania błędnego przekonania o pewnym stanie rzeczy. Jak bowiem podniesiono w judykaturze: „[s]posób działania sprawcy oszustwa względem innej osoby może zatem polegać na: wprowadzeniu jej w błąd poprzez wywołanie u niej wyobrażenia o istniejącej (nie przyszłej) rzeczywistości, która jest w istocie inna niż przedstawia jej sprawca”[13]. Tak postawiona teza nasuwa oczywiste pytanie o świadomość odbiorcy, dotyczącą prezentowanej usługi czy towaru, co z kolei stanowi sedno oszustwa. Tym bardziej że – jak przekonywano – dla bytu oszustwa obojętne jest, czy odbiorca zapoznał się ze stanem faktycznym, a nawet czy mógł on lub powinien był to uczynić (Siwicki, 2018, s. 170). Gdyby brać pod uwagę kryteria oceny dotyczącej wprowadzenia w błąd lub wyzyskania błędnego przekonania o stanie rzeczy (Oczkowski, 2004, s. 37–43), teoretycznie powinno być wykluczone oszustwo w przypadku, gdy odbiorca komunikatu zostaje poinformowany o zastosowaniu technologii i fakcie nierzeczywistej reprezentacji. Podejście takie wydaje się optymalne, niemniej postęp technologiczny uzmysławia, że pewne formy reprezentacji rzeczywistości – choć wysoce wiarygodne, mogą wprowadzać w błąd, nawet jeśli są opatrzone odpowiednią informacją dotyczącą tego, kto się nimi posługuje, co do ich wirtualnego charakteru. Przykładów nie trzeba daleko szukać, skoro „rozmowy” z chatbotem albo asystentem AI są już powszechnie wykorzystywane w obrocie gospodarczym (choć obecnie jeszcze w różnym zakresie). Możliwość wprowadzenia przez nie w błąd co do przekazanej informacji staje się zatem nowym wyzwaniem. Abstrahując od problematyki związanej z odpowiedzialnością za takie czyny, która nadaje się na odrębne opracowania (por. np. Kaplan, 2025), w tym miejscu wypada stwierdzić, że w polskich regulacjach prawnych nie przewidziano adekwatnych środków zapobiegania nielegalnemu wykorzystaniu nowoczesnych technologii, w szczególności do celu oszustwa w cyberprzestrzeni. W odniesieniu do wykorzystania sztucznej inteligencji regulacją, która normuje m.in. zakazane praktyki w zakresie AI oraz zasady funkcjonowania w obrocie (dozwolonych) systemów wysokiego ryzyka, jest rozporządzenie UE

[13] Wyrok SN z 19 lipca 2007 r., V KK 384/06, Lex nr 299205.

2024/1689, zwane Aktem o sztucznej inteligencji[14] (Akt o AI; por. odpowiednio: art. 5, obowiązujący od 2 lutego 2025 r., oraz rozdział III, art. 6–49 powołanego Aktu). Rozporządzenie to uwzględnia fakt, że AI: „może być wykorzystywana niewłaściwie i może dostarczać nowych i potężnych narzędzi do praktyk manipulacji, wyzyskiwania i kontroli społecznej" (Preambuła, motyw 28), jak również, że techniki manipulacyjne oparte na AI mogą być wykorzystywane w celu wprowadzania w błąd poprzez skłanianie innych osób do podejmowania decyzji w sposób, który podważa i ogranicza ich autonomię, decyzyjność i swobodę wyboru, a nawet wykorzystywać słabości danej osoby lub określonej grupy osób ze względu np. na ich wiek, niepełnosprawność, szczególną sytuację społeczną lub ekonomiczną. Wskazuje, że takie systemy AI „powinny być zakazane" (por. pkt 28 i 29 Preambuły Aktu). Ponadto Akt o AI przewiduje potrzebę budowania świadomości dotyczącej AI (art. 62 ust. 3 – Urząd ds. AI, art. 66 – Rada ds. AI), co stanowi niewątpliwie krok w dobrym kierunku. Można jednak przypuszczać, że będzie wymagało czasu osiągnięcie zadowalających rezultatów takich kampanii informacyjnych, czyli świadomości dotyczącej działania systemów AI i ich zrozumienie, przynajmniej w takim stopniu, jakiego należałoby oczekiwać, aby z poziomu użytkownika/adresata wprowadzających w błąd informacji realnie zapobiegać cyberoszustwom z ich wykorzystaniem. Inną sprawą pozostaje zaś to, że w zakresie m.in. obowiązków podmiotów (szeroko rzecz ujmując) wprowadzających do obrotu systemy AI należy się spodziewać bardziej szczegółowych regulacji krajowych.

Na koniec rozważań prawnych w zakresie zapobiegania cyberoszustwom trzeba wspomnieć także o dylematach związanych z wielomiejscowością czynów popełnionych w cyberprzestrzeni (Chałubińska-Jętkiewicz, 2019, s. 65–79; Golonka, 2024b, s. 105–118), a także o anonimizacji, utrudniającej wykrycie sprawcy (a niekiedy nawet ujawnienie procederu). W odniesieniu do popełnienia oszustwa w cyberprzestrzeni trudności wynikają przede wszystkim ze specyfiki tego rodzaju przestrzeni, niedającej się w prosty sposób zaliczyć do żadnej znanej prawu międzynarodowemu kategorii. Poza tym wątpliwości budzi ustalenie determinantów miejsca popełnienia czynu (czy za takowe uznać np. miejsce przebywania sprawcy, lokalizacji serwera, urządzenia lub urządzeń służących do popełnienia czynu, czy miejsca pobytu osoby pokrzywdzonej, względnie należącego do niej urządzenia). Stąd w literaturze wysunięto propozycje rozwiązań w zakresie jurysdykcji w cyberprzestrzeni (Worona, 2020, s. 417–424), w tym koncepcję *czwartej przestrzeni* „na kształt aterytorialnego tworu" (Czekalska, 2004, s. 75). Gdy zaś chodzi o anonimizację, właściwą działaniom bazującym chociażby na technologii *blockchain*, na której opierają się m.in. transakcje walutą wirtualną, to – jak potwierdzają badania – staje się ona sporym wyzwaniem (Krysiński, 2020; Rakha, 2024). Dotyczy to nie tylko ustalenia, że doszło do popełnienia przestępstwa,

[14] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, Dz. Urz. UE L, 2024/1689, opubl. 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj

ale także wykrycia jego sprawcy lub sprawców, np. kradzieży, oszustwa kryptowalutowego czy czynów podejmowanych na dalszym etapie, a zmierzających do wprowadzenia do obrotu nielegalnie pozyskanej kryptowaluty, czyli prania pieniędzy (Golonka, 2024a, s. 216–217).

V. PODSUMOWANIE

Reasumując, zaprezentowane rozważania nasuwają zasadniczy wniosek, że cyberoszustwo, a ściślej różne jego formy, stanowią współcześnie poważne zagrożenie. Jak wynika z zaprezentowanych tendencji zjawiska, coraz częściej wykorzystywane są do tego celu także nowoczesne technologie, w tym przede wszystkim sztuczna inteligencja. Potwierdzają to także przytoczone na wstępie badania przeprowadzone w 2023 r. przez GASA we współpracy ze ScamAdvisor. Budowanie świadomości społecznej w tym zakresie ogranicza się jednak zazwyczaj do aktualnie panujących tendencji. Raczej sporadycznie, o ile w ogóle, zwraca się uwagę na możliwości, jakie stwarza rozwój technologiczny i popiera to stosownymi przykładami cyberoszustw. Tymczasem zagrożenia z tym związane nie są incydentalne. Co więcej, powszechnie są już dostępne narzędzia, takie jak Faker Python, oraz środki, jak bramki VoIP wspierane przez AI, które otwierają drogę do bardziej wyrafinowanych sposobów na wprowadzenie w błąd lub wyzyskanie błędu celem osiągnięcia korzyści majątkowej.

Pozytywnie należy zatem ocenić fakt, że polski legislator – wprowadzając stosowne unormowania w dziedzinie bezpieczeństwa sieci i usług telekomunikacyjnych – przychodzi w sukurs działaniom przedsiębiorców i dostawców usług telekomunikacyjnych. Odnosi się to przede wszystkim do uchwalenia ustawy o zwalczaniu nadużyć w komunikacji elektronicznej. Niemniej w obowiązującym brzmieniu jej przepisy mogą nasuwać pewne obiekcje. W zakresie podyktowanym omawianą problematyką, czyli prawnych środków zwalczania nadużyć w komunikacji elektronicznej, jakimi są *smishing* oraz CLI *spoofing,* zastrzeżenia może budzić zarówno definicja legalna smishingu, jak i zakres obowiązków spoczywających na podmiotach wskazanych w tej ustawie. Podobna uwaga odnosi się do niedostosowania przepisów do potrzeb podyktowanych rozwojem technologicznym. Nawet jeżeli ustawodawca uznaje, że aktualnie nie jest (jeszcze) zasadne uwzględnianie tego w przepisach mających na celu zapobieganie przestępstwom w cyberprzestrzeni (czemu zaprezentowane wyżej rozważania, nierzadko poparte także statystykami, zdają się jednak przeczyć), to z całą pewnością pożądane byłoby rozważenie możliwości wykorzystania sztucznej inteligencji w zakresie samego zapobiegania i/lub zwalczania oszustw w cyberprzestrzeni. Być może stanowiłoby to krok na drodze do bardziej perspektywicznego opracowywania regulacji krajowych, zwłaszcza w tych obszarach, które tego wymagają ze swej natury (sprawy karne i wymiaru sprawiedliwości) bądź też dla których Akt o sztucznej inteligencji może okazać się niewystarczający (jak np. obowiązki dostawców i podmiotów korzystających z systemów AI ograniczonego ryzyka).

Author contributions / Indywidualny wkład autora (CRediT): **Anna Golonka** – 100% (Conceptualization / Konceptualizacja; Investigation / Przeprowadzenie badań; Writing – original draft / Pisanie – pierwszy szkic; Writing – review & editing / Pisanie – recenzja i edycja).

Conflict of interest / Konflikt interesów: The author declares no conflict of interest. / Autorka nie zgłosiła konfliktu interesów.

Funding / Finansowanie: The author declares no institutional funding. / Autorka oświadczyła, że nie korzystała z finansowania instytucjonalnego.

The use of AI tools / Wykorzystanie narzędzi AI: The author declares no use of AI tools. / Autorka oświadczyła, że nie korzystała z narzędzi AI.

Data availability / Dostępność danych: Not applicable. / Nie dotyczy.

References / Bibliografia

Abagnale, F. W. (2020). *Oszukaj mnie, jeśli potrafisz. Proste sposoby przechytrzenia współczesnych kanciarzy*. Helion.

Abraham, J. (2022, 8 December). Consumer and expert survey reveals: No country is good at fighting online scams [Blog]. GASA. Pobrane 2 marca 2025, z: https://www.gasa.org/post/consumer-and-expert-survey-reveals-no-country-is-good-at-fighting-online-scams

Adebola, O. O., Ogungbe, O., Adegboye, N., i Adetuyi, T. E. (2024). Strategies for combating synthetic identity fraud: The role of machine learning and behavioral analysis in enhancing financial ecosystem security. *International Journal of Research in Engineering and Science, 12*(4), 280–292. https://doi.org/10.13140/RG.2.2.15459.36643

Akartuna, E. A. (2024). *AI-enabled crime in the cryptoasset ecosystem. Exploring emerging risks and trends in crypto and artificial intelligence. Elliptic Report*. Elliptic. Pobrane 27 stycznia 2025, z: https://www.hkdca.com/wp-content/uploads/2024/08/enabled-crime-crytoasset-ecosystem-elliptic-1.pdf

Aleksandrowicz, T. R. (2016). Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego. *Przegląd Bezpieczeństwa Wewnętrznego, 8*(15), 11–28.

Ampatzidis, D. (2024). AIS spoofing in the maritime industry: A growing risk and compliance challenge. Pobrane 10 grudnia 2024, z: https://www.kpler.com/blog/ais-spoofing-in-the-maritime-industry-a-growing-risk-and-compliance-challenge

Androjna, A., Perkovič, M., Pavic, I., i Mišković, J. (2021). AIS data vulnerability indicated by a spoofing case-study. *Applied Sciences*, *11*(5015). https://doi.org/10.3390/app11115015

BBC. (2023, 23 października). BBC One-Watchdog. AI Voice Scams. Pobrane 1 czerwca 2026, z: https://www.bbc.co.uk/programmes/p0gnrtnz

Bertrand, M. (2000). The old and the new. W: M. Bertrand (red.), *Fraud! How to protect yourself from schemes, scams, and swindles* (s. 37–59). Amacom.

Chałubińska-Jętkiewicz, K. (2019). *Cyberodpowiedzialność*. Marszałek.

Che Mat, N. I., Jamil, N., Yusoff, Y., i Mat Kiah, M. L. (2024). A systematic literature review on advanced persistent threat behaviors and its detection strategy. *Journal of Cybersecurity, 10*(1), 1–18. https://doi.org/10.1093/cybsec/tyad023

Chelliah I. (2025). Beginner's guide to NumPy for data science – All about AI-ML. Pobrane 20 lutego 2025, z: https://indhumathychelliah.com/2021/01/24/beginners-guide-to-numpy-for-data-science/

Czekalska, J. (2004). Jurysdykcja w cyberprzestrzeni a teoria przestrzeni międzynarodowych. *Państwo i Prawo, 59(11)*, 73–81.

Dela, P. (2020). *Teoria walki w cyberprzestrzeni*. Wydawnictwo Akademii Sztuki Wojennej.

Focal Team. (2025, 1 stycznia). Top 11 fraud trends & how to prevent them in 2025. Pobrane 1 czerwca 2026, z: https://www.getfocal.ai/blog/top-fraud-trends

Garcia-Vera, G. (2024). Deep fake- postęp technologiczny a prawo karne. *Acta Iuridica Resoviensis, 1*(44), 39–52. https://doi.org/10.15584/actaires.2024.1.3

Consumers International Congress. (2023). *Global statement: Stopping online scams*. Pobrane 1 czerwca 2026, z: https://www.consumersinternational.org/media/513807/anti-scams-global-statement-6-12-23.pdf

Golonka, A. (2022). Scamming. W: P. Łabuz, I. Malinowska i M. Michalski (red.), *Przestępczość zorganizowana. Aspekty prawne kryminalno-kryminalistyczn*e (s. 290–303). Difin.

Golonka, A. (2024a). Cyberlaundering in the era of modern technologies. *Przegląd Policyjny*, *154*(2), 205–224. https://doi.org/10.5604/01.3001.0054.8516

Golonka, A. (2024b). Cyberpranie pieniędzy jako przestępstwo „bez granic" – refleksje na tle zasad międzynarodowego prawa karnego i koncepcji jurysdykcji karnej w cyberprzestrzeni. W: L. Brodowski i D. Kuźniar (red.), *Wokół problematyki państwa jako podmiotu prawa międzynarodowego. Księga jubileuszowa Profesor Elżbiety Dyni* (s. 105–118). Wydawnictwo UR.

Greening, J. (2022). Consumer and expert survey reveals: No country is good at fighting online scams. GASA. Pobrane 2 marca 2025, z: https://www.gasa.org/post/consumer-and-expert-survey-reveals-no-country-is-good-at-fighting-online-scams

Gryszczyńska A. (2023). Criminal liability for CLI spoofing. *GIS Odyssey Journal*, *3*(2), 37–49. https://doi.org/10.57599/gisoj.2023.3.2.37

Hallman, R. A. (2023, grudzień). SIM Swapping attacks for digital identity Theft: A threat to financial services and beyond [Preprint]. Pobrane 22 grudnia 2024, z: https://www.researchgate.net/publication/376612643_SIM_Swapping_Attacks_for_Digital_Identity_Theft_A_threat_to_financial_services_and_beyond

Harris, D. (2019). Deepfakes – False pornography is here and the law cannot protect you. *Duke & Law Technology Review*, *17*(1), 99–128. https://scholarship.law.duke.edu/dltr/vol17/iss1/4/

Hodges, K. (2024, 16 czerwca). Value of e-commerce losses to online payment fraud worldwide from 2020 to 2023 – Raport. *Statista*. Pobrane 16 lutego 2025, z: https://www.statista.com/statistics/1273177/ecommerce-payment-fraud-losses-globally/

Hoffmann, T. (2018). *Główni aktorzy cyberprzestrzeni i ich działalność*. W: T. R. Dębowski (red.), *Cyberbezpieczeństwo wyzwaniem XXI wieku* (s. 11–30). ArchaeGraph.

Howarth, J. (2024, 15 listopada). 13 top technology trends (2024 & 2025). *Exploding Topics*. Pobrane 5 grudnia 2024, z: https://explodingtopics.com/blog/technology-trends

Interpol. (2020, July). *Analytical report: Online African organized crime from surface to dark web*. https://www.interpol.int

Jain, R., i Kant, Ch. (2015). Attacks on biometric systems: An overview. *International Journal of Advances in Scientific Research*, *1*(7), 283–288. https://doi.org/10.7439/ijasr.v1i7.1975

Kapitan Hack. (2023, 18 lipca). CERT-UA pokazuje kulisy ataku z błyskawiczną eksfiltracją danych. *Kapitan Hack.pl*. Pobrane 2 stycznia 2025, z: https://kapitanhack.pl/2023/07/18/nieskategoryzowane/cert-ua-pokazuje-kulisy-ataku-z-blyskawiczna-eksfiltracja-danych/

Kaplan, J. (2025). *Generatywna AI. Wszystko, co warto wiedzieć*. Państwowe Wydawnictwo Naukowe.

Khanjani, Z., Watson, G., i Janeja, V. P. (2023, 9 stycznia). Audio deepfakes: A survey. *Frontiers in Big Data, 5*, 1001063. https://doi.org/10.3389/fdata.2022.1001063

Kim, M., Suh, J., i Kwon, H. (2022). A study of the emerging trends in SIM swapping crime and effective countermeasures. W: R. Lee i G. Gim, (red.), *2022 IEEE/ACIS – 7th International Conference on Big Data, Cloud Computing, and Data Science (BCD), Aug. 4 2022 to Aug. 6 2022 Vietnam* (s. 240–245). Danang. https://doi.org/10.1109/BCD54882.2022.9900510

Konieczny, M. K. (2023). Cyberprzestępczość – krótka historia, współczesne oblicza i trudna do przewidzenia przyszłości. *Roczniki Administracji i Prawa 2023*, *1*(23), 29–50. https://doi.org/10.5604/01.3001.0016.3776

Kosiński, J. (2015). *Paradygmaty cyberprzestępczości*. Difin.

Krysiński, Ł. (2020). Identyfikacja cyberprzestępców. *Prokuratura i Prawo*, *2*, 120–134.

Kumar, R. (2020). *Kidney transplants and scams: India's troublesome legacy*. Sage.

Lakomy, M. (2015). *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*. Wydawnictwo Uniwersytetu Śląskiego.

Lewulis, P. (2021). O rozgraniczeniu definicyjnym pomiędzy przestępczością „cyber" i „komputerową" dla celów praktycznych i badawczych. *Prokuratura i Prawo*, *3,* 12–31.

Lin, H. S., Dam, K. W., i Owens, W. A. (2009). *Technology, policy, law, and ethics regarding US acquisition and use of cyberattack capabilities*. National Academies Press.

Mbanaso, U. M., i Dandaura, E. S. (2015). The cyberspace: Redefining a new world. *IOSR Journal of Computer Engineering*, *17*(3), 17–24. https://doi.org/10.9790/0661-17361724

McQuade, S. C. (2021). *Encyclopedia of cybercrime*. Greenwood Group.

Mehan, J. (2014). *Cyberwar, cyberterror, cybercrime & cyberactivism: An in-depth guide to the role of standards in the cybersecurity environment* (wyd. 2). IT Governance Publishing.

Mungai, R. (2024). Synthetic identity fraud a critical primary national security priority. *SSRN*. http://dx.doi.org/10.2139/ssrn.4770398

Murszewski, J. (2023). *Phishing w ujęciu prawnokarnym*. W: J. Bojarski, N. Daśko, J. Lachowski, T. Oczkowski i A. Ziółkowska (red.), *Współczesne oblicze prawa karnego, prawa wykroczeń, kryminologii i polityki kryminalnej. Księga jubileuszowa dedykowana Profesor Violetcie Konarskiej-Wrzosek* (s. 641–650). Wolters Kluwer Polska.

Oczkowski, T. (2004). *Oszustwo jako przestępstwo majątkowe i gospodarcze*. Zakamycze.

Opitek, P. (2015). Przestępstwo skimmingu. *Prokuratura i Prawo*, *11*, 66–81.

Opitek, P. (2023). *Kwalifikacja prawna i opis znamion przestępstw teleinformatycznych. Studium prawno-kryminalistyczne*. Krajowa Szkoła Sądownictwa i Prokuratury.

Palczewski, S. (2023, 16 sierpnia). Cyberataki na agencje rządowe Ukrainy. *CyberDefence24*. Pobrane 2 stycznia 2025, z: https://cyberdefence24.pl/cyberbezpieczenstwo/cyberataki-na-agencje-rzadowe-ukrainy

Policja.pl. (2024, 26 lipca). Akt oskarżenia w sprawie kradzieży przy wykorzystaniu metody tzw. SIM SWAP. Pobrane 1 czerwca 2026, z: https://policja.pl/pol/aktualnosci/248400,Akt-oskarzenia-w-sprawie-kradziezy-przy-wykorzystaniu-metody-tzw-SIM-SWAP.html

Prenger, R., Valle, R., i Catanzaro, B. (2019). Waveglow: A flow-based generative network for speech synthesis (s. 3617–3621). W: *Conference Paper z 18 Dec 2018. Conference: ICASSP 2019 – 2019, 12–17 May 2019*. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), arXiv: 1811.00002v1. https://doi.org/10.48550/arXiv.1811.00002

Prokuratura Krajowa. (2024, 30 października). Akt oskarżenia w sprawie oszustwa na szkodę ponad 600 osób w związku z zakupem kryptowaluty Bitcoin. Pobrane 1 czerwca 2026, z: https://www.gov.pl/web/prokuratura-krajowa/akt-oskarzenia-w-sprawie-oszustwa-na-szkode-ponad-600-osob-w-zwiazku-z-zakupem-kryptowaluty-bitcoin

Radoniewicz, F. (2016). *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*. Wolters Kluwer Polska.

Radoniewicz, F. (2024). *Cyberprzestępstwa przeciwko danym komputerowym i systemom informatycznym w kodeksie karnym – propozycje zmian*. C. H. Beck.

Rahman, M. R. A. (2020). Online scammers and their mules in Malaysia. *Journal of Law and Society*, *26*(8), 65–72. https://doi.org/10.17576/juum-2020-26-08

Rakha, N. A. (2024). Cybercrime and the legal and ethical challenges of emerging technologies. *International Journal of Law and Policy*, *2*(5), 28–35.

Rampolla, J., i Kipper, G. (2012). Augmented reality: An emerging technologies guide to AR. Syngress.

Roberts, R. Ch. (2007). Biometric attack vectors and defences. *Computers & Security*, *26*(1), 14–25. https://doi.org/10.1016/j.cose.2006.12.008

Sabry, F., Labda, W., Erbad, i Malluhi, A. (2020). Cryptocurrencies and artificial intelligence: Challenges and opportunities. *IEEE Access*, *8*, 175840–175858. https://doi.org/10.1109/ACCESS.2020.3025211

Saeidi, M. (2024, 17 maja). Voice cloning scams are a growing threat. Here's how you can protect yourself. CBS News-New York. Pobrane 23 lutego 2025, z: https://www.cbsnews.com/newyork/news/ai-voice-clone-scam/

Sharma, A., i Bantan, M. (2025). Simulating data breaches: Synthetic datasets for depicting personally identifiable information through scenario-based breaches. *Data in Brief*, *58*(111207). https://doi.org/10.1016/j.dib.2024.111207

Sharma, P. (2024). Algorithms and strategies for fraud prevention on online platforms. *World Journal of Advanced Research and Reviews, 23*(02), 2220–2225. https://doi.org/10.30574/wjarr.2024.23.2.2462

Siwicki, M. (2012). Podział i definicja cyberprzestępstw. *Prokuratura i Prawo*, *7–8*, 241–251.

Siwicki, M. (2018). *Prawo karne wobec oszustw i innych związanych z nimi przestępstw w handlu internetowym oraz bankowości elektronicznej*. Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika.

Skipper, K. J. (2025). Voice cloning AI scams are on the rise [Blog]. Pobrane 27 stycznia 2025, z: https://www.becu.org/blog/voice-cloning-ai-scams-are-on-the-rise

Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., i Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crime Sciences*, *11*(1), 1–35. https://doi.org/10.1186/s40163-021-00163-8

Wang, W. (2021, 6 grudnia). The essence of deep learning. *TechRxiv* (Preprint November, 2021). https://doi.org/10.36227/techrxiv.17078699

Worona, J. (2020). *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*. Wolters Kluwer, Lex.

Ziobroń, A. (2021). Deepfake a prawo karne. Uwagi de lege lata i de lege ferenda dotyczące fałszywej pornografii. *Studenckie Prace Prawnicze, Administratywistyczne i Ekonomiczne*, *37*, 226–236. https://doi.org/10.19195/1733-5779.37.15

Ziobroń, A. (2024). Political deepfake. Remarks de lege lata and postulates de lege ferenda. *Studia Prawnicze. Rozprawy i Materiały*, *1*(34), 79–92. https://doi.org/10.48269/2451-0807-sp-2024-1-04

Zych, J. (2019). *Teleinformatyka dla bezpieczeństwo*. Grupa Wydawnicza FNCE.