Czasopismo Prawa Karnego i Nauk Penalnych
Journal of Criminal Law and Penal Studies
ISSN: 1506-1817 e-ISSN: 2719-6569
Rok/Volume XXX: 2026 Nr/No. 1

https://doi.org/10.60677/CPKiNP2026.1.4

Maciej Siwicki[1]

https://orcid.org/0000-0002-3120-0211

Karalność oszustwa komputerowego w wybranych państwach Ameryki Łacińskiej oraz Europy

Punishability of Computer Fraud in Selected Countries in Latin America and Europe

1. Wprowadzenie

Oszustwa komputerowe są dziś jednymi z najpoważniejszych zagrożeń dla bezpieczeństwa zarówno osób, jak i instytucji na całym świecie[2]. Istotny wzrost liczby ataków, wymierzonych głównie w infrastrukturę krytyczną oraz przedsiębiorstwa, jest w szczególności zauważany w Ameryce Łacińskiej. Według raportu firmy Kasperski 92% przedsiębiorstw z tego regionu doświadczyło prób infiltracji ich sieci, podczas gdy ponad 62% przedsiębiorstw zgłosiło incydenty, w których cyberprzestępcy uruchomili złośliwy kod w ich sieci lub próbowali nawiązać łączność z przejętymi systemami i przejąć nad nimi kontrolę. Kaspersky wskazuje także na ciągły wzrost liczby ataków ransomware, zwłaszcza

[1] Maciej Siwicki – dr hab., LL.M., prof. UMK, Instytut Stosunków Międzynarodowych, Wydział Nauk o Polityce i Bezpieczeństwie, Uniwersytet Mikołaja Kopernika w Toruniu / habilitated doctor, LL.M., associate professor, Institute of International Relations, Faculty of Political Science and Security Studies, Nicolaus Copernicus University in Toruń. Wkład/Contribution: 100%.
✉ msiwicki@umk.pl

[2] Globalne straty z powodu cyberprzestępczości sięgnęły w 2024 r. 9,5 biliona USD, co odpowiadałoby trzeciej co do wielkości gospodarce świata. *Globalne*…

w Brazylii, Meksyku i Chile[3]. Szczególnie dotkliwy był atak na początku 2025 r. na Paragwaj, w wyniku którego doszło m.in. do masowego wycieku danych osobowych około 7,4 miliona obywateli, co obejmuje niemal całą populację kraju[4].

W odpowiedzi na nowe wyzwania podjęto liczne działania mające na celu dostosowanie prawa do przemian technologicznych, zwłaszcza w obszarze cyfryzacji i regulacji dotyczących gospodarki cyfrowej oraz bezpieczeństwa cyfrowego. Kraje Ameryki Łacińskiej, podejmując działania w celu dostosowania swojego prawa do przemian technologicznych, często odnoszą się do rozwiązań przyjętych w innych państwach, zwłaszcza tych w Unii Europejskiej[5]. Można jednak zaobserwować, że często przyjmowane są odmienne rozwiązania prawne, w tym pomija się penalizację niektórych zachowań lub stosuje różne definicje prawne. Szczególnie w obszarze cyberprzestępczości takie podejście nie zawsze jest korzystne, gdyż cyberprzestępczość ma charakter transgraniczny i wymaga szybkiej, skoordynowanej reakcji państw.

Celem niniejszego opracowania jest porównanie rozwiązań prawnych przyjętych w różnych systemach prawnych, co ma przede wszystkim umożliwić identyfikację dobrych praktyk oraz wskazanie luk regulacyjnych, które mogą być przeszkodą w efektywnej walce z przestępczością komputerową. W kontekście współpracy międzynarodowej takie analizy pomagają też formułować rekomendacje na rzecz harmonizacji i ujednolicania podejść prawnych i proceduralnych.

Wybór państw do analizy prawnoporównawczej w zakresie oszustw komputerowych opiera się na kilku istotnych przesłankach. Po pierwsze,

---

[3] *Aumento*… Według grupy CrowdStrike takie grupy cyberprzestępcze, jak Mispadu, Kiron czy ALPHV BlackCat odniosły sukcesy w atakach na instytucje finansowe i przedsiębiorstwa w Brazylii, Meksyku, Argentynie i Kolumbii. K. Ratto, *LatAm*…

[4] Ataki te obejmowały m.in. włamania do systemów rządowych (np. Ministerstwo Zdrowia, Najwyższy Sąd Electoralu, Ministerstwo Finansów, Policja Narodowa) oraz działania takich grup cyberprzestępczych, jak Brigada Cyber PMC i Flax Typhoon (związana z chińskim państwem).

[5] Współpraca regulacyjna między Ameryką Łacińską a UE w zakresie prawa cyfrowego i telekomunikacyjnego jest aktywnie prowadzona w ramach różnych inicjatyw, m.in. dialogów regulacyjnych pomiędzy organami regulacyjnymi. Zob. Unia Europejska. Agencja Wsparcia BEREC (Biuro BEREC), https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/agency-support-berec-berec-office_pl; Urząd Komunikacji Elektronicznej. Współpraca w ramach Unii Europejskiej, https://bip.uke.gov.pl/sprawy-miedzynarodowe/wspolpraca-w-ramach-unii-europejskiej/.

skupienie się na wybranych krajach umożliwia wnikliwsze i szczegółowe zbadanie odmiennych podejść legislacyjnych, które odzwierciedlają zróżnicowane uwarunkowania prawne, społeczne i technologiczne. W Europie wybrane państwa często charakteryzują się rozwiniętym systemem prawnym i silnym naciskiem na regulacje związane z cyfryzacją, co czyni je cennymi punktami odniesienia. Z kolei w Ameryce Łacińskiej, gdzie cyfryzacja i przepisy dotyczące cyberbezpieczeństwa są często we wczesnej fazie implementacji, wybrane kraje stanowią ważne przykłady dynamiki wprowadzania nowych regulacji oraz wyzwań w egzekwowaniu prawa. Ponadto wybór Ameryki Łacińskiej i Europy jako obszarów badawczych jest uzasadniony intensywną współpracą regulacyjną między tymi regionami, widoczną m.in. w inicjatywach takich jak eLAC czy partnerstwach między regulatorami telekomunikacji (np. Regulatel i BEREC). W efekcie podjęcie tego tematu umożliwia nie tylko ocenę stopnia zaawansowania i skuteczności regulacji w wybranych państwach, ale także wskazanie konkretnych kierunków rozwoju prawodawstwa oraz praktyk współpracy transgranicznej, co jest kluczowe w dobie rosnącej cyfryzacji i globalizacji przestępczości komputerowej.

2. Pojęcie oszustwa

W rozumieniu potocznym zazwyczaj przyjmuje się, że oszustwo to zamierzone, nieuczciwe, fałszywe, zwodnicze naruszenie istniejących zasad współżycia społecznego (np. naruszenie obowiązujących zasad postępowania w obrocie gospodarczym) podjęte w celu osiągnięcia nienależnej korzyści (dodatniej wartości) poprzez doprowadzenie innej osoby lub osób do niekorzystnego dla nich rozporządzenia. Celem manipulacji będzie najczęściej uzyskanie przez sprawcę korzyści majątkowej[6].

[6] W słowniku *Black's Law Dictionary* przy definiowaniu oszustwa zwraca się uwagę, że jest to ogólne określenie na zróżnicowane zachowania będące tworem ludzkiej pomysłowości o indywidualnym charakterze, których celem jest uzyskanie przewagi nad inną osobą poprzez stworzenie fałszywego wrażenia lub ograniczenia możliwości poznania prawdy. Oszustwo może obejmować wszelkiego rodzaju sztuczki, mistyfikacje, podstępy, pozorowanie i inne nieuczciwe sposoby, przy pomocy których wprowadza się inną osobę w błąd. *Fraud*, w: *Fraud*..., s. 2.201, https://studylib.net/doc/25856303/acfe-manual-2020-international-edition. Zob. też *Fraud*, w: *Black's*... Zob. na temat terminów „cyberprzestępstwo" i „przestępczość komputerowa" M. Siwicki, *Cyberprzestępczość*..., s. 9–21; M. Siwicki, *Podział*..., s. 246–256.

Przestępczość określana jako tzw. oszustwo komputerowe różni się od tak klasycznie rozumianego oszustwa przede wszystkim specyfiką techniczną i sposobem działania, który łączy elementy manipulacji systemami komputerowymi i ingerencji w przetwarzanie danych. Jeżeli przyjrzymy się sposobom, w jaki sprawcy dokonują oszustw z wykorzystaniem nowoczesnych technologii, można wyróżnić z jednej strony oszustwa polegające na oszukańczym oddziaływaniu na proces decyzyjny człowieka, w których „komputer" stanowi narzędzie przestępstwa, służąc sprawcy m.in. jako kanał komunikacyjny, narzędzie umożliwiające dostęp do informacji lub też narzędzie służące do rozpowszechniania komunikacji *phishingowej*. Z drugiej strony oszukańczy zamach może być skierowany nie tylko na osobę, ale również na system, dane i programy komputerowe związane z procesem przetwarzania, gromadzenia lub przesyłania np. skomputeryzowanych depozytów pieniężnych. Mając na względzie to, że istota oszustwa wiąże się z błędną oceną rzeczywistości przez osobę rozporządzającą własnym lub cudzym mieniem, posługiwanie się w tym drugim wypadku terminem „oszustwo" budzi wiele wątpliwości. Przeciwnicy używania tej nazwy w stosunku do manipulacji systemami komputerowymi wskazują, że oszustwo to podstępne nakłonienie innej osoby do działania w określony sposób. Ofiara ma „uwierzyć", że określone fakty mają miejsce, że coś, co jest fałszywe, jest prawdą. Z tego też względu jedynie człowiek może być przedmiotem oszustwa, a nie maszyna, która nie ma świadomości, a jedynie w sposób automatyczny wykonuje polecenia[7].

Pojawiające się problemy ze zdefiniowaniem zjawiska oszukańczego wykorzystania słabości i podatności technicznych elektronicznych systemów przetwarzania danych zdają się w pierwszej kolejności wynikać z pewnego zamieszania terminologicznego, które powstało wokół tego zjawiska. W literaturze przedmiotu do ich opisu używa się bowiem takich terminów, jak „oszustwo komputerowe", „oszustwo syntaktyczne", „oszustwo tożsamościowe", „niewłaściwe oszustwo informatyczne", „fałszywe nadużycie przetwarzania danych", „szkodnictwo komputerowe", „«nieuprawnione» manipulacje komputerowe", „phishing", „pharming",

[7] Nazwę oszustwo komputerowe niektórzy autorzy uznają za nieadekwatną m.in. dlatego, że w przypadku tego przestępstwa sprawca nie oddziałuje – tak jak przy klasycznym oszustwie – na osobę, lecz na działanie urządzenia technicznego. Zob. M. Kulik, *Oszustwo*..., s. 348.

„kradzież tożsamości", często bez jednoczesnego ścisłego sprecyzowania ich znaczenia[8]. Z oczywistych względów może to skomplikować wysiłki podejmowane w celu zwalczania tego zjawiska głównie ze względu na jego globalny i transgraniczny charakter. Utrudnienia mogą pojawić się m.in. na polu badań i pomiaru przestępczości, rozwoju wspólnej polityki, edukacji społeczeństwa, pomocy pokrzywdzonym czy też rozwoju wspólnych metod i technik zapobiegania.

Drugą przyczyną pojawiających się trudności jest próba budowania definicji tego zjawiska w opozycji do pojęcia oszustwa klasycznego, w oparciu na kryterium naruszenia bezpieczeństwa elektronicznie przetwarzanych informacji poprzez ingerencję w funkcjonowanie systemu komputerowego odpowiedzialnego za przetwarzanie, gromadzenie i przesyłanie danych podjęte w celu uzyskania nienależnej (bezprawnej) korzyści majątkowej. Tymczasem kwestia określenia, jakie czyny uznaje się za bezprawne, pozostaje ściśle związana z konkretnym systemem prawnym i nie może być dokonywana *in abstracto*. Dlatego też zasadność użycia terminu „oszustwo komputerowe" wymaga przede wszystkim odwołania do konkretnego systemu prawnego i zawartych w nim uregulowań normatywnych.

3. Aspekty prawnoporównawcze

Obecnie można zaobserwować, że odmienne uwarunkowania prawne i tradycje kulturowe powodują, że charakter czynów zabronionych pod groźbą kary, jakie przewiduje ustawodawstwo w zakresie przestępstw związanych z bezpieczeństwem przetwarzania informacji, wykazuje w prawie porównawczym istotne różnice. Ogólnie można wydzielić trzy podstawowe sposoby kryminalizacji oszukańczego wykorzystania słabości i podatności technicznych elektronicznych systemów przetwarzania danych po części odpowiadające wymienionym powyżej podziałom definicji oszustwa komputerowego.

Po pierwsze, wyodrębnia się nowy typ oszustwa komputerowego, który ma posłużyć przeciwdziałaniu oszustwom, które są wynikiem nieautoryzowanych modyfikacji w trakcie przetwarzania danych z zamiarem nieuprawnionego uzyskania korzyści.

---

[8] Zob. M. Siwicki, *Prawo*..., s. 55–61.

Po drugie, ustawodawca stara się precyzyjnie wypełnić luki, jakie wraz z postępem technicznym pojawiły się w definicji klasycznego oszustwa poprzez nadanie mu nowej postaci normatywnej.

W końcu, w szeregu ustawodawstw rezygnuje się z karalności oszustwa komputerowego, zauważając, że tego rodzaju zachowania wypełniają znamiona innych czynów zabronionych, takich jak przestępstwo wykorzystania „narzędzi hackerskich", przerobienia lub podrobienia dokumentu, instalacji w systemie specjalnego oprogramowania szpiegującego czy uzyskania nieuprawnionego dostępu do systemu komputerowego.

3.1. Nowy typ oszustwa

Wprowadzenie nowego typu oszustwa jest zazwyczaj uzasadniane tym, że ustawowe znamiona klasycznego oszustwa nie są spełnione w wypadku czynu polegającego na oddziaływaniu na urządzenie automatycznie przetwarzające informacje, gdy tymczasem czyn ten może przynieść sprawcy nienależną korzyść majątkową[9]. W Polsce w art. 287 k.k.[10] wymóg posłużenia się przez sprawcę typowym dla oszustwa wprowadzeniem pokrzywdzonego w błąd lub też wykorzystaniem czyjegoś błędu, został zastąpiony wymogiem ingerencji w przetwarzanie danych informatycznych. Zamiast obiektywnej oceny, czy doszło do skutku w postaci niekorzystnego rozporządzenia mieniem własnym lub cudzym przez osobę wprowadzoną w błąd lub której błąd został przez sprawcę wyzyskany, pojawiła się konieczność oceny realizacji znamion w zamiarze bezpośrednim zabarwionym jednym z dwóch wskazanych w tym przepisie motywów (*dolus directus coloratus*), tzn. osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody[11].

Od tradycyjnego w definicji oszustwa wprowadzenia w błąd odstępuje się także w ustawodawstwie Republiki Federalnej Niemiec. Ustęp

---

9 Takie uzasadnienie zostało podane w Polsce. Zob. *Uzasadnienie*…, s. 206–207.

10 Ustawa z 6 czerwca 1997 r. – Kodeks karny, Dz.U. 2025, poz. 383, tekst jedn. ze zm., dalej: Kodeks karny, k.k.

11 Wyrządzenie szkody majątkowej może być rozpatrywane jako rzeczywista strata doznana przez pokrzywdzonego (*damnum emergens*) oraz utrata spodziewanych korzyści (*lucrum cessans*), jak również szkody niemajątkowej wyrządzonej osobie. Działanie w celu wyrządzenia szkody nie musi być tożsame z działaniem w celu osiągnięcia korzyści majątkowej, jak również możliwa jest sytuacja odwrotna. R. Korczyński, R. Koszut, *Oszustwo*…, s. 17.

pierwszy artykułu 263a (§ 263a StGB – Computerbetrug) niemieckiego kodeksu karnego z 1998 r.[12] stanowi, że kto z zamiarem uzyskania dla siebie lub osoby trzeciej niezgodnej z prawem materialnym korzyści uszkadza własność innej osoby (doprowadza do powstania szkody w mieniu innej osoby) poprzez wpływanie na rezultat (wynik) przetwarzania danych dzięki błędnej konfiguracji programu, wykorzystania nieprawidłowych lub niepełnych danych, nieautoryzowanego wykorzystania danych lub innego nieuprawnionego wpływania na przebieg przetwarzania, podlega karze pozbawienia wolności do pięciu lat lub karze grzywny.

Podobne rozwiązanie przyjęto w art. 504quater § 1 belgijskiego kodeksu karnego z 1867 r.[13], na mocy którego ten, kto dąży do uzyskania dla siebie lub innej osoby, z zamiarem oszustwa, bezprawnej korzyści ekonomicznej, wprowadza dane do systemu komputerowego, modyfikuje i usuwa dane przechowywane, przetwarzane lub przesyłane przez system komputerowy lub zmienia za pomocą wszelkich innych środków technologicznych normalne użytkowanie danych w systemie komputerowym, podlega karze pozbawienia wolności od sześciu miesięcy do 5 lat i grzywny. Również chorwacki kodeks karny z 1997 r.[14] oprócz klasycznego oszustwa określonego w art. 224 zawiera oszustwo komputerowe w art. 224a. Na mocy tego przepisu karze pozbawienia wolności od sześciu miesięcy do 5 lat podlega ten, kto z zamiarem uzyskania dla siebie lub osoby trzeciej bezprawnej korzyści materialnej wchodzi, wykorzystuje, zmienia, usuwa albo w jakikolwiek inny sposób sprawia, że dane komputerowe lub programy są nieużywalne, albo wyłącza funkcjonowanie systemu lub programów komputerowych i tym samym uszkadza własność innej osoby. Przepis ten w ustępie trzecim przewiduje także karalność produkowania, nabywania, sprzedawania, posiadania oraz

---

12 Ustawa z 13 listopada 1998 r. – Kodeks karny (Strafgesetzbuch – StGB), BGBl. 1998 I, s. 3322, dalej: niemiecki kodeks karny. Sekcja dotycząca oszustwa komputerowego znajduje się w rozdziale 22 (Betrug und Untreue), Bundesministerium der Justiz, § 263a Computerbetrug, „Gesetze im Internet", https://www.gesetze-im-internet.de/stgb/__263a.html.

13 Ustawa z 8 czerwca 1867 r. – Kodeks karny (Code pénal), Moniteur belge z 1867 r. Dz.U. 09-06-1867 nr 1867060850, s. 3133, dalej: belgijski kodeks karny. Dostępny w wersji angielskiej online: https://legislationline.org/sites/default/files/documents/f4/Belgium_CC_1867_am2018_fr.pdf.

14 Ustawa z 21 października 1997 r. – Kodeks karny (Kazneni zakon), Narodne novine br. 110/1997, dalej: chorwacki kodeks karny. Dostępny w wersji angielskiej online: http://www.zakon.hr/z/98/Kazneni-zakon.

umożliwiania innym nabycia specjalistycznego sprzętu, urządzeń, danych lub programów komputerowych stworzonych lub przystosowanych do przestępstwa oszustwa komputerowego.

Taki szczególny typ oszustwa przewiduje się także w duńskim kodeksie karnym w art. 279a (§ 279a Straffeloven), w którym mowa jest o bezprawnym zmienianiu, dodawaniu lub usuwaniu informacji lub programu używanych w elektronicznym przetwarzaniu danych[15]. Kodeks karny Republiki Estonii w art. 213 przewiduje karalność oszustwa komputerowego, wymagając spowodowania szkody majątkowej u innej osoby poprzez bezprawne wprowadzenie, zmianę, wykreślenie, zniszczenie albo zablokowanie programu komputerowego lub danych, jak również innej bezprawnej ingerencji w przetwarzanie danych w celu uzyskania korzyści majątkowej[16]. Węgierski kodeks karny[17] również penalizuje oszustwo komputerowe (art. 375), którego sprawcą może być każdy, kto w celu uzyskania nienależnej korzyści finansowej wprowadza dane do systemu informacyjnego albo zmienia lub kasuje dane z takiego systemu oraz sprawia, że dane stają się niedostępne albo w inny sposób ingeruje w działanie systemu informacyjnego, powodując tym samym szkodę.

Podobne rozwiązania przyjęto także w niektórych państwach Ameryki Łacińskiej. W Chile na mocy art. 197 bis kodeksu karnego (Código Penal, Artículo 197 bis) za oszustwo komputerowe uznaje się działanie w celu wyrządzenia szkody innej osobie lub w celu uzyskania korzyści majątkowej dla siebie lub dla osoby trzeciej poprzez „manipulacje systemem informatycznym poprzez wprowadzanie, zmianę, uszkodzenie lub usunięcie danych informatycznych albo poprzez jakąkolwiek ingerencję w działanie systemu informatycznego”[18]. Podobnie w Argentynie, zgodnie z art. 173 pkt 16 kodeksu karnego, znowelizowanego ustawą

15 Ustawa z 15 kwietnia 1930 r. – Kodeks karny (Straffeloven), Lovtidende A nr 126/1930, tekst jedn. (Lovtidende A nr 1085/2022), dalej: duński kodeks karny.

16 Ustawa z 6 czerwca 2001 r. – Kodeks karny (Karistusseadustik), RT I 2001, 61, 364, dalej: estoński kodeks karny. Źródło i pełny tekst przepisów kodeksu karnego Estonii, w tym art. 213, są dostępne online w języku angielskim: https://www.riigiteataja.ee/en/eli/522012015002/consolide.

17 Ustawa z 25 lipca 2012 r. – Kodeks karny (Büntető Törvénykönyv), Magyar Közlöny 2012, poz. 100, dalej: węgierski kodeks karny.

18 Ustawa z 12 listopada 1874 r. – Kodeks karny (Código Penal), Diario Oficial de la República de Chile z 1874 r., Congreso Nacional de Chile, Código Penal, „Ley Chile – Biblioteca del Congreso Nacional”, https://www.bcn.cl/leychile/navegar?idNorma=1177743.

nr 26.388[19], karalne jest oszukiwanie innej osoby poprzez zastosowanie „jakiejkolwiek techniki manipulacji informatycznej, która zakłóca normalne funkcjonowanie systemu komputerowego lub transmisję danych".

Warto także zwrócić uwagę na Artículo 347-BIS (Fraude informático) wprowadzony do kodeksu karnego w Urugwaju na mocy ustawy Ley Nº 20.327 z 23 sierpnia 2024 r.[20] Na mocy tego przepisu wyodrębnione zostały trzy typy oszustwa komputerowego:

a) pierwsze – polegające na użyciu podstępów lub sztuczek mających na celu wprowadzenie w błąd innej osoby, aby uzyskać informacje za pomocą technologii informacyjnych i komunikacyjnych na swoją korzyść lub na korzyść osoby trzeciej, wyrządzając szkodę innej osobie,
b) drugie – polegające na dokonaniu manipulacji informatycznych lub podobnych działań w celu przeprowadzenia nieautoryzowanych operacji finansowych, przelewów lub płatności na szkodę innej osoby, niezależnie od tego, czy korzyść jest osobista, czy dla osoby trzeciej,
c) trzecie – polegające na użyciu dowolnego typu karty, czeku, kodu lub innego środka płatniczego albo powiązanych z nimi danych do przeprowadzania nieautoryzowanych przelewów, płatności lub innych operacji w celu uzyskania korzyści kosztem innej osoby.

Można zauważyć, że w tej definicji oszustwa komputerowego (*fraude informático*) nie jest karalne wykorzystanie błędu innej osoby, ale jest przy tym wyraźnie wymagane, żeby uzyskanie informacji prowadziło do wyrządzenia szkody.

Inne rozwiązanie przyjęto w Peru, gdzie – zgodnie z artykułem 8. Oszustwo komputerowe[21] z ustawy Ley Nº 30096 Peru[22] – odpowiedzial-

---

19 Ustawa z 29 października 1921 r. – Kodeks karny (Código Penal de la Nación Argentina), Boletín Oficial de la República Argentina z 1921 r., Ley 11.179 – Código Penal de la Nación Argentina (Texto actualizado), dalej: argentyński kodeks karny, „Argentina.gob.ar", https://www.argentina.gob.ar/normativa/nacional/ley-11179-16546/texto.

20 Poder Legislativo de Uruguay, Código Penal (Ley Nº 9.155), „IMPO", https://www.impo.com.uy/bases/codigo-penal/9155-1933.

21 Przepis był nowelizowany m.in. w 2014 r. (Ley N° 30171) oraz w grudniu 2023 r. (Decreto Legislativo Nº 1614), kiedy dodano m.in. karalność podszywania się pod interfejsy czy strony internetowe oraz inne szczegóły dotyczące bezprawnej manipulacji systemami komputerowymi.

22 Ustawa z 8 kwietnia 1991 r. – Kodeks karny (Código Penal), Diario Oficial El Peruano, Decreto Legislativo Nº 635, dalej: peruwiański kodeks karny. Congreso de la República del Perú, Ley Nº 30096 – Ley de delitos informáticos, „Gob.pe", https://cdn.www.gob.pe/uploads/document/file/1671764/1678028-ley-n-30096-ley-de-delitos-informticos-y-sus-modificatorias.pdf.

ność karną poniesie osoba, która za pomocą technologii informacji lub komunikacji celowo i nielegalnie dąży do uzyskania dla siebie lub innej osoby nieuczciwej korzyści kosztem osoby trzeciej poprzez zaprojektowanie, wprowadzenie, zmianę, usunięcie, skasowanie, sklonowanie danych komputerowych lub jakiekolwiek ingerowanie lub manipulowanie działaniem systemu komputerowego, będzie karana karą pozbawienia wolności nie krótszą niż trzy lata i nie dłuższą niż osiem lat oraz grzywną w wysokości od 60 do 120 dni grzywny. Kara pozbawienia wolności nie krótsza niż pięć i nie dłuższa niż dziesięć lat oraz grzywna od 80 do 140 dni będzie orzekana, jeśli szkoda dotyczy mienia państwowego przeznaczonego na cele socjalne lub programy wsparcia społecznego. Przepis ten jest dość ogólny i szeroki, co może prowadzić do trudności interpretacyjnych w praktyce, zwłaszcza przy definiowaniu granicy między legalnym a nielegalnym działaniem w systemach informatycznych. Konieczność wykazania, że działanie było „celowe i nielegalne" oraz że przyniosło „nieuczciwą korzyść kosztem osoby trzeciej" może być trudna do udowodnienia, zwłaszcza w złożonych przypadkach cyberprzestępstw, gdzie intencje i rzeczywiste skutki są często trudne do ustalenia. Choć przewidziane są wyższe kary za szkody dotyczące mienia państwowego, to poza tym przepis nie rozróżnia wyraźnie różnych stopni szkodliwości czy kontekstów czynu, co może powodować niejednolitą praktykę sądową.

W Paragwaju na mocy art. 188 paragwajskiego kodeksu karnego[23] – oszustwa komputerowe (Estafa mediante sistemas informáticos) penalizowane jest wpływanie na wynik przetwarzania danych komputerowych poprzez błędne programowanie, fałszywe dane, niewłaściwe użycie informacji lub inne niedozwolone działania podjęte w celu osiągniecia nieuczciwej korzyści majątkowej. Warunkiem karalności jest spowodowanie szkody majątkowej. W ustępie drugim przewidziano przy tym karalność przygotowania do tego przestępstwa poprzez produkcję, pozyskiwanie, sprzedaż, przechowywanie lub udostępnianie innym programów komputerowych służących do popełnienia takiego czynu.

[23] Ustawa z 26 listopada 1997 r. – Kodeks karny (Código Penal), Gaceta Oficial nr 50/1997, Ley Nº 1.160/97, dalej: paragwajski kodeks karny. Congreso de la República del Paraguay, Código Penal (Ley Nº 1.160/97), Colección Derecho Penal, „Poder Judicial de Paraguay", https://www.pj.gov.py/ebook/libros_files/coleccion-derecho-penal.pdf.

Można zauważyć, że w tej grupie państw kluczowy jest zamiar uzyskania nieuprawnionej korzyści majątkowej lub wyrządzenia szkody innej osobie. Karalne jest wprowadzanie, modyfikowanie, usuwanie danych komputerowych lub ingerencja w prawidłowe działanie systemów komputerowych (np. zmiana konfiguracji, wyłączanie programów, manipulacja danymi). Zakres penalizacji nie jest ograniczony wyłącznie do tradycyjnego „wprowadzenia w błąd", ale obejmuje szeroki zakres technik wykorzystywanych do manipulacji danymi i systemami informatycznymi. Przyjęte rozwiązania nie są oczywiście identyczne. I tak na przykład chorwacki kodeks karny (art. 224a) rozszerza ochronę także na wyłączenie funkcjonowania systemu oraz uszkodzenie cudzej własności przez działania na systemie. Niemiecki kodeks karny art. 263a kładzie nacisk na „uszkodzenie własności" poprzez wpływ na wynik przetwarzania danych, skupiając się na skutku szkody majątkowej. Polski Kodeks karny (art. 287) odchodzi od wymogu „wprowadzenia w błąd", zastępując go kryterium ingerencji w przetwarzanie danych oraz nastawieniem motywacyjnym (osiągnięcie korzyści lub wyrządzenie szkody). Można także zauważyć, że w szczególności w części państw Ameryki Łacińskiej (Brazylia, Urugwaj) widoczne są próby dostosowania prawa do międzynarodowego charakteru cyberprzestępczości oraz zaawansowanych technologii, podczas gdy inne stosują bardzo szerokie i ogólne definicje, które wymagają dalszego doprecyzowania. Co więcej, w niektórych z tych państw wymaga się wyraźnego wyrządzenia szkody, wyłączając karalność błędów czy działań prawnie uprawnionych (Paragwaj, Urugwaj).

3.2. Dostosowanie klasycznego oszustwa do nowych realiów

Odmienne podejście można zaobserwować w ustawodawstwie drugiej grupy państw, gdzie często nie tylko określa się nowy typ oszustwa, ale wyraźnie odwołuje się do konstrukcji oszustwa klasycznego. Charakterystyczne w tym względzie jest rozwiązanie przyjęte w Bułgarii[24], gdzie – zgodnie z art. 212a bułgarskiego kodeksu karnego dodanym

[24] Ustawa z 1 maja 1968 r. – Kodeks karny (Наказателен кодекс), Държавен вестник бр. 26/1968, tekst jedn. (ДВ бр. 27/2019) ze zm., dalej: bułgarski kodeks karny. Dostępny w wersji angielskiej online: https://legislationline.org/sites/default/files/documents/67/PENAL_PROCEDURE_CODE_am2011_en.pdf.

w 2002 r. (SG nr 38/2007) – oszustwo komputerowe stanowi działanie w celu uzyskania korzyści majątkowej dla siebie lub innej osoby poprzez przedstawianie lub utrzymanie fałszywego obrazu faktów u innej osoby w wyniku wprowadzania, modyfikowania, usuwania danych informatycznych lub poprzez wykorzystanie podpisu elektronicznego. Na gruncie tego kodeksu karnego nie pojawia się zatem pytanie, czy w błąd można wprowadzić maszynę, ale czy człowiek został wprowadzony w błąd za pomocą komputera.

W Szwecji, w sekcji 1 rozdziału IX szwedzkiego kodeksu karnego[25] pod tytułem „Oszustwa i inne nieuczciwości" (ang. Chapter 9 On Fraud and Other Dishonesty), definicję oszustwa klasycznego poszerzono o dokonywanie zamian w programie lub w zapisie (ang. *alterations to a programme or recording*) oraz inne, bezprawne wpływanie (ang. *unlawfully affects*) na wynik automatycznego przetwarzania danych lub którykolwiek inny podobny automatyczny (ang. *other similar automatic*) proces, w wyniku czego sprawca osiąga zysk, a stratę ponosi inna osoba.

W Hiszpanii, zgodnie z ust. 1 artykułu 248 hiszpańskiego kodeksu karnego[26], oszustwo klasyczne stanowi używanie podstępu w celach zarobkowych, aby wprowadzić inną osobę w błąd, tak aby dokonała ona rozporządzenia mieniem, zaś według ust. 2 a) za sprawcę oszustwa uważa się także osobę, która w celu osiągnięcia zysku dokonuje jakiejkolwiek manipulacji danymi lub programem komputerowym, aby doprowadzić do nieuprawnionego przeniesienia aktywów majątkowych ze szkodą dla innej osoby. Według podpunktu b) oszustwa dokonują także osoby, które produkują, przesyłają lub dostarczają programy komputerowe specjalnie przeznaczone do dokonywania oszustw komputerowych.

Podobnie definiowane jest oszustwo komputerowe w art. 177[1] łotewskiego kodeksu karnego[27], stanowiąc *lex specialis* w stosunku do art. 177

[25] Ustawa z 21 grudnia 1962 r. – Kodeks karny (Brottsbalken), Svensk författningssamling (SFS) 1962:700, tekst jedn. (SFS 2024:900) ze zm., dalej: szwedzki kodeks karny. Dostępny w wersji angielskiej online: https://legislationline.org/sites/default/files/documents/98/Sweden_CC.pdf.

[26] Ustawa Organiczna 10/1995 z 23 listopada 1995 r. – Kodeks karny (Código Penal), Boletín Oficial del Estado (BOE) nr 281 z 24 listopada 1995 r., s. 33987, tekst jedn. (BOE nr 313 z 30 grudnia 2023 r.) ze zm., dalej: hiszpański kodeks karny. Dostępny w wersji angielskiej online: https://legislationline.org/sites/default/files/2023-10/Criminal_Code_2016.pdf.

[27] Ustawa z 17 czerwca 1998 r. – Kodeks karny (Krimināl kodekss), Latvijas Vēstnesis nr 199/200 (3614/3615) z 8 lipca 1998 r., dalej: łotewski kodeks karny.

przewidującego karalność oszustwa. Według tego przepisu przewiduje się odpowiedzialność karną tego, kto świadomie wprowadza fałszywe dane do automatycznego systemu przetwarzania danych, by uzyskać cudzą własność albo prawa do takiej własności, albo uzyskać inną korzyść majątkową po to, by wywrzeć wpływ na przetwarzanie jego zasobów. Z kolei w Rumunii oszustwo komputerowe (art. 249 rumuńskiego kodeksu karnego[28]) i oszukańcze operacje finansowe (art. 250) zostały wprowadzone do rozdziału IV „Oszustwo popełnione przez użycie systemów komputerowych i elektronicznych metod płatności".

W tej drugiej grupie znajdują się także państwa z Ameryki Łacińskiej. I tak przykładowo w Argentynie na mocy art. 9 ustawy Ley 26388/2008[29], która wprowadziła pkt 16 w art. 173 argentyńskiego kodeksu karnego, za szczególne przypadki oszustwa komputerowego uznaje się oszukanie innej osoby „za pomocą dowolnej techniki manipulacji informatycznej, która zakłóca normalne działanie systemu informatycznego lub przesył danych". Karalne jest również niszczenie, zmiana, uniemożliwienie dostępu do danych, dokumentów, programów bądź systemów informatycznych albo wprowadzanie do systemu szkodliwych programów. Artykuł 153 bis penalizuje nieautoryzowany dostęp do systemów lub danych informatycznych (*hacking*). Podstawową wadą tego rozwiązania jest przede wszystkim brak precyzji definicji i zakresu penalizacji art. 173 pkt 16 argentyńskiego kodeksu karnego. Zastosowanie tego rozwiązania może powodować wiele praktycznych problemów wynikających z trudności w ocenie, czy dane działanie sprawcy faktycznie zakłóca podstawowe funkcje systemu lub transmisję danych, czy z rozgraniczeniem między zakłóceniem a błędem technicznym lub awarią wykorzystaną przez sprawcę, ze zdefiniowaniem, kiedy dana manipulacja była dokonana w celu oszukania lub uzyskania korzyści, a nie np. była przypadkowa lub korzystna dla systemu. Mogą się pojawić także problemy dowodowe będące efektem technicznych trudności w wykryciu i udowodnieniu manipulacji komputerowych, zwłaszcza przy złożonych atakach lub działaniach ukrytych.

---

[28] Ustawa nr 286/2009 z 17 lipca 2009 r. – Kodeks karny (Codul penal), Monitorul Oficial al României nr 510 z 24 lipca 2009 r., dalej rumuński kodeks karny. Zob. K. Buczkowski, M. Jankowski, P. Bachmat, *Regulacja*…

[29] Congreso de la Nación Argentina, Ley 26.388 – Modificación del Código Penal, Información Legislativa – „Argentina.gob.ar", https://www.argentina.gob.ar/normativa/nacional/ley-26388-141790/texto.

Podobne rozwiązania przyjęto także w art. 186 pkt 2 ekwadorskiego kodeksu karnego (Código Orgánico Integral Penal, COIP)[30], gdzie definicja oszustwa rozumianego jako wprowadzanie w błąd innej osoby, by ta dokonała czynu szkodzącego jej majątkowi lub majątkowi osoby trzeciej w celu uzyskania korzyści majątkowej dla siebie lub innej osoby poprzez symulację fałszywych faktów (*hechos falsos*) albo zniekształcenie lub ukrycie faktów prawdziwych (*hechos verdaderos*), rozszerzono o punkty pierwszy i drugi. Według pierwszego z nich za oszustwo uznaje się m.in. zmienianie, sklonowanie, zdublowane: kart kredytowych, debetowych, płatniczych lub podobnych, zaś według punktu drugiego za oszustwo uznaje się „użycie urządzeń elektronicznych, które zmieniają, modyfikują, klonują lub dublują oryginalne urządzenia bankomatów, w celu przechwycenia, zapisania, kopiowania lub odtworzenia informacji z kart kredytowych, debetowych, płatniczych lub podobnych".

Warto także zwrócić uwagę na rozwiązania przyjęte w Peru, gdzie obok wprowadzenia przepisu penalizującego oszustwo komputerowe, w kodeksie karnym rozszerzono definicję oszustwa także na „manipulację głosem, obrazem, dźwiękiem lub ruchami ciała osób trzecich, wykorzystując sztuczną inteligencję lub podobne technologie w sposób powodujący szkodę ekonomiczną dla ofiary" (pkt 7 art. 196-A peruwiańskiego kodeksu karnego)[31]. Również w Brazylii, na mocy ustawy zmieniającej kodeks karny (La Ley de Delitos Informáticos – Ley n.º 12.737/2012)[32], rozszerzono klasyczną definicję oszustwa, przyjmując, że oszustwo komputerowe (*El fraude informático*) to oszustwo popełnione z wykorzystaniem informacji dostarczonych przez ofiarę lub osobę trzecią wprowadzoną w błąd za pomocą mediów społecznościowych,

---

30 Ustawa Organiczna 101 z 10 sierpnia 2014 r. – Kodeks karny integralny (Código Orgánico Integral Penal), Registro Oficial Suplemento 180 z 10 lutego 2014 r., dalej: ekwadorski kodeks karny. Asamblea Nacional del Ecuador, Código Orgánico Integral Penal (COIP), „Ministerio de Defensa Nacional del Ecuador", https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf.

31 Congreso de la República del Perú, Código Penal (Decreto Legislativo Nº 635), „Diario Oficial El Peruano", https://diariooficial.elperuano.pe/Normas/obtenerDocumento?idNorma=2.

32 Ustawa Dekret nr 2.848 z 7 grudnia 1940 r. – Kodeks karny (Código Penal), Diário Oficial da União z 31 grudnia 1940 r., dalej: brazylijski kodeks karny. Presidência da República (Getúlio Vargas), Decreto-Lei Nº 2.848, de 7 de Dezembro de 1940 – Código Penal, „Portal da Legislação", https://www.planalto.gov.br/ccivil_03/decreto-lei/del-2848compilado.htm.

kontaktów telefonicznych, przesyłania fałszywych e-maili lub w inny podobny sposób oszustwa. Jednocześnie przewiduje się typ kwalifikowany, jeśli przestępstwo jest popełnione z wykorzystaniem serwera znajdującego się poza terytorium Brazylii oraz gdy przestępstwo jest popełnione na szkodę podmiotu prawa publicznego lub instytucji ekonomii społecznej, pomocy społecznej lub dobroczynności. W tym rozwiązaniu kluczowym elementem jest połączenie tradycyjnego oszustwa z wykorzystaniem środków cyfrowych i komunikacyjnych.

We wszystkich państwach znajdujących się w tej grupie kluczowym elementem jest zamiar uzyskania korzyści majątkowej lub wyrządzenia szkody innej osobie poprzez wprowadzenie w błąd – co wzoruje się na klasycznej konstrukcji oszustwa. Wprowadzenie w błąd dotyczy przede wszystkim osoby fizycznej lub prawnej, a nie samej maszyny, co oznacza, że oszustwo komputerowe jest rozpatrywane jako działanie prowadzące do wprowadzenia człowieka w błąd przy użyciu narzędzi cyfrowych. Warto przy tym zauważyć, że wśród wymienionych państw Argentyna ma najmniej precyzyjne przepisy, przez co istnieją duże trudności interpretacyjne i dowodowe, zwłaszcza przy odróżnianiu awarii od przestępstwa. Ekwador oferuje bardziej szczegółowy i techniczny opis metod oszustwa, szczególnie w obszarze finansów elektronicznych, zaś Peru i Brazylia wprowadzają nowoczesne rozwiązania, rozszerzając karalność na manipulacje wykorzystujące sztuczną inteligencję i multimedia, co wskazuje na dynamiczne podejście do postępujących zmian technologicznych. W przypadku tych dwóch ostatnich państw należy jednak zauważyć, że w świetle art. 8 Konwencji o cyberprzestępczości[33] najistotniejszy jest faktyczny wpływ na dane informatyczne lub systemy komputerowe oraz cel oszustwa, którym jest korzyść majątkowa lub wyrządzenie szkody. Oznacza to, że przypadki obejmujące np. same działania socjotechniczne czy manipulacje bezpośrednio ingerujące wyłącznie w postrzeganie ofiary, bez faktycznej ingerencji w dane lub systemy komputerowe, nie mieszczą się w ścisłej definicji oszustwa komputerowego z art. 8 konwencji. Jak zostało wskazane wyżej, ten problem został rozwiązany w Peru poprzez przyjęcie nowej definicji oszustwa komputerowego. W Brazylii użycie zwrotu „inny podobny sposób oszustwa",

[33] Konwencja o cyberprzestępczości (Convention on Cybercrime), sporządzona w Budapeszcie 23 listopada 2001 r., CETS nr 185, https://rm.coe.int/1680081561.

który jest otwarty i niedefiniowany enumeratywnie, daje możliwość objęcia przepisem nowych, rozwijających się technologicznie form oszustw cyfrowych nieopisanych konkretne w prawie, ale analogicznych pod względem sposobu działania i efektów do wymienionych przykładów. W praktyce może to dotyczyć np. nowych technik *phishingu*, oszustw prowadzonych przez aplikacje mobilne, komunikatory internetowe lub inne środki elektroniczne wykorzystywane do manipulacji ofiarami.

3.3. Rezygnacja z odrębnej karalności oszustwa komputerowego

W trzeciej, ostatniej grupie znajduje się m.in. francuski kodeks karny[34], który nie zna przestępstwa oszustwa komputerowego. W tym państwie kryminalizuje się jednak m.in. nieuprawnione wpływanie na automatyczne przetwarzanie danych, niezależnie od celu, w jakim jest ono dokonywane (art. 323–1, 2 lub 3 francuskiego kodeksu karnego)[35]. Podobnie kwestię tę reguluje rosyjski kodeks karny z 13 czerwca 1996 r. (art. 272–274)[36]. Te rozwiązania także zostały przyjęte w części państw Ameryki Łacińskiej. I tak na przykład w Meksyku, zgodnie z art. 211 bis oraz art. 212 bis Federalnego Kodeksu karnego (Código Penal Federal)[37], karalne jest nieupoważnione używanie, modyfikowanie, niszczenie lub usuwanie danych, systemów lub programów informatycznych. W tym państwie skupiono się na ochronie systemów i danych komputerowych oraz określono sankcje za nieuprawnione działania na tych systemach (modyfikacje, usuwanie, kopiowanie danych), nie wyodrębniając jednak osobnego typu przestępstwa oszustwa komputerowego. Klasyczne

---

34 Ustawa z 22 lipca 1992 r. – Kodeks karny (Code pénal), Journal Officiel de la République Française (JORF) nr 170 z 23 lipca 1992 r., s. 9874, dalej: francuski kodeks karny, „Legifrance", https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719/.

35 Dostępny w wersji angielskiej online: https://legislationline.org/sites/default/files/documents/ca/France_CPC_am2006_en.pdf.

36 Ustawa Federalna nr 63-FZ z 13 czerwca 1996 r. – Kodeks karny (Уголовный кодекс), Собрание законодательства Российской Федерации (СЗ РФ) nr 25, poz. 2954 z 17 czerwca 1996 r., dalej: rosyjski kodeks karny. Dostępny w wersji angielskiej online: https://legislationline.org/sites/default/files/documents/a6/RF_CC_1996_am03.2012_en.pdf.

37 Ustawa Federalna z 14 sierpnia 1931 r. – Kodeks karny federalny (Código Penal Federal), Diario Oficial de la Federación z 15 sierpnia 1931 r., dalej: meksykański kodeks karny. Código Penal Federal de México, Congreso General de los Estados Unidos Mexicanos, „Cámara de Diputados – LeyesBiblio", https://oig.cepal.org/sites/default/files/1931_codigopenal_eumexicanos.pdf.

oszustwo karane jest jednak na podstawie art. 386 i polega na wprowadzeniu w błąd innej osoby lub wykorzystaniu jej błędu, a następnie nielegalnym przywłaszczeniu sobie jakiejś rzeczy lub osiągnięciu nieuczciwego zysku. Podobne rozwiązanie jest przyjęte w Kolumbii, gdzie według kolumbijskiego kodeku karnego karalna jest m.in. nieuprawniona zmiana lub zniszczenie danych lub systemów (art. 269 A i kolejne), zaś klasyczne oszustwo opisane jest w art. 386 i przewiduje karalność uzyskania korzyści majątkowej przez wprowadzenie kogoś w błąd[38].

Wszystkie kraje z tej grupy nie wyodrębniają osobnego typu przestępstwa „oszustwa komputerowego". Definicje koncentrują się głównie na technicznej ochronie systemów i integralności danych, a nie na klasycznym oszustwie jako działaniu wprowadzającym w błąd osobę fizyczną lub prawną, co może być skuteczne w ochronie systemów komputerowych, ale jednocześnie narażać na przesadną penalizację i trudności interpretacyjne. Stosowanie tylko ogólnych konstrukcji karania manipulacji technicznych może nie wystarczyć w przypadku zaawansowanych cyberprzestępstw.

4. Podsumowanie

Jak zostało to wskazane wyżej, ogólnie można wymienić trzy podstawowe podejścia do kryminalizacji oszukańczego wykorzystywania słabości i podatności technicznych elektronicznych systemów przetwarzania danych, które odpowiadają różnym definicjom oszustwa komputerowego. Istniejące w prawie porównawczym różnice w definiowaniu analizowanej przestępczości z oczywistych względów mogą wydłużyć czas wykrywania i ścigania sprawców, a brak jednolitych międzynarodowych standardów i procedur utrudnia współpracę międzynarodową oraz wymianę danych, co jest kluczowe dla skutecznego zwalczania analizowanej przestępczości, tzn. oszustw komputerowych. Powyższe problemy definicyjne nie są oczywiście przeszkodą nie do pokonania. Jeżeli weźmie się pod uwagę, że na arenie międzynarodowej brak jest na przykład globalnej definicji terroryzmu, a pomimo to zostały z sukcesem

[38] Ustawa nr 599 z 24 lipca 2000 r. – Kodeks karny (Código Penal), Diario Oficial nr 44.097 z 24 lipca 2000 r., dalej: kolumbijski kodeks karny. Congreso de la República de Colombia, Ley 599 de 2000 – Código Penal, „Gestor Normativo – Función Pública", https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6388.

wypracowane międzynarodowe instrumenty prawne służące przeciwdziałaniu temu zjawisku, w tym zakresie dokonuje się także analizy statystycznej i prowadzi współpracę międzynarodową. Można także zakładać, że równie skuteczne może być przeciwdziałanie zjawisku oszustw komputerowych. Co więcej, funkcjonowanie w prawie porównawczym wielu definicji opisujących jedno zjawisko nie jest wcale czymś nowym. O ile standardowe definicje mogą posłużyć optymizacji strategii przeciwdziałania, to jednak w żadnym wypadku nie są one konieczne, aby rozwiązać jakiś problem. Istnienie na arenie międzynarodowej wielu definicji może przecież w praktyce prowadzić także do tego, że ten sam problem zostanie rozwiązany na różne sposoby, stanowiąc jednocześnie wskazówkę możliwej drogi rozwoju dla innych.

Streszczenie

Przestępczość komputerowa stanowi rosnące wyzwanie dla bezpieczeństwa osób i instytucji na całym świecie. W niniejszym artykule przeprowadzono analizę porównawczą ustawodawstwa wybranych krajów Ameryki Łacińskiej i Europy, identyfikując trzy główne podejścia do penalizacji oszukańczego wykorzystania luk w systemach elektronicznego przetwarzania danych: utworzenie odrębnego przestępstwa oszustwa komputerowego, adaptację i rozszerzenie klasycznych definicji oszustwa o formy związane z komputerami oraz brak odrębnego przestępstwa, z naciskiem na przestępstwa techniczne dotyczące ingerencji w systemy komputerowe. Podkreślone są różnice terminologiczne i regulacyjne, które wpływają na skuteczne ściganie oszustw komputerowych i współpracę międzynarodową w tej kwestii. Zwrócono uwagę na konieczność wprowadzenia dynamicznej regulacji uwzględniającej postęp technologiczny, taki jak sztuczna inteligencja i nowe techniki cyfrowej manipulacji.

Słowa kluczowe

oszustwo komputerowe, cyberprzestępczość, prawo porównawcze, ustawodawstwo, Ameryka Łacińska, Europa, regulacje technologiczne, sztuczna inteligencja, współpraca międzynarodowa

Summary

Computer fraud poses an increasing challenge to the security of individuals and institutions worldwide. This study compares the legislation of selected Latin American and European countries, identifying three main approaches to criminalizing the fraudulent exploitation of vulnerabilities in electronic data processing systems: creating a separate offense of computer fraud; adapting and extending classic fraud definitions to include

computer-related forms; andnot having a separate offense, with an emphasis on technical offenses involving interference with computer systems. The study also highlights terminological and regulatory differences that affect the effective prosecution and international cooperation in this area. The importance of dynamic regulation that incorporates technological advances, such as artificial intelligence and novel digital manipulation techniques, is emphasized.

Keywords

computer fraud, cybercrime, comparative law, legislation, Latin America, Europe, technological regulation, artificial intelligence, international cooperation

Bibliografia/Bibliography

Aumento sostenido de los ataques de ransomware en América Latina, „Kaspersky" z 12 maja 2025 r., https://latam.kaspersky.com/about/press-releases/aumento-sostenido-de-los-ataques-de-ransomware-en-america-latina-kaspersky.

Buczkowski K., Jankowski M., Bachmat P., *Regulacja przestępstwa oszustwa w wybranych systemach prawnych państw Unii Europejskiej*, Warszawa 2018, https://iws.gov.pl/wp-content/uploads/PDF/2018/PRAWA%20KARNE%20I%20KRYMINOLOGIA/IWS-K.Buczkowski-P.Bachmat-Regulacja-przest%C4%99pstwa-oszustwa.pdf.

Fraud, w: *Black's Law Dictionary Free Online Legal Dictionary (2nd Ed.)*, http://thelawdictionary.org/fraud/.

Fraud, w: *Fraud Examiners Manual (International Edition)*, Association of Certified Fraud Examiners, Austin, Texas (USA) 2020, https://studylib.net/doc/25856303/acfe-manual-2020-international-edition.

Globalne straty spowodowane cyberprzestępczością osiągnęły w 24 wartość 9,5 bln USD – raport, „PAP Biznes" z 15 kwietnia 2025 r., https://biznes.pap.pl/wiadomosci/gry-i-technologie/globalne-straty-spowodowane-cyberprzestepczoscia-osiagnely-w-24.

Korczyński R., Koszut R., *„Oszustwo" komputerowe*, „Prokuratura i Prawo" 2002, nr 2.

Kulik M., *Oszustwo komputerowe*, w: *System Prawa Karnego. Tom 9. Przestępstwa przeciwko mieniu i gospodarcze*, red. R. Zawłocki, Warszawa 2015.

Ratto K., *LatAm Ecrime Malware Evolution 2024*, „CrowdStrike" z 16 grudnia 2014 r., https://www.crowdstrike.com/en-us/blog/latam-ecrime-malware-evolution-2024.

Siwicki M., *Cyberprzestępczość*, Warszawa 2013.

Siwicki M., *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012, nr 7–8.

Siwicki M., *Prawo karne wobec oszustw i innych związanych z nimi przestępstw w handlu internetowym oraz bankowości elektronicznej*, Toruń 2018.

Uzasadnienie rządowego projektu nowego kodeksu karnego, w*: Nowe kodeksy karne z 1997 r. z uzasadnieniami*, Warszawa 1997.