

ALEKSANDRA PANEK
Studentka prawa
Uniwersytet Rzeszowski
ORCID: 0009-0006-2875-6362
e-mail: aleksandrapanek419@gmail.com
DOI: 10.5281/zenodo.22960512



CYBERPRZESTĘPSTWA NA GRUNCIE PRAWA MIĘDZYNARODOWEGO I KRAJOWEGO

Cybercrimes under international and domestic law

Abstrakt

Celem niniejszej pracy jest omówienie istoty cyberprzestępstw jako jednego z najpilniejszych wyzwań XXI wieku. Omówione zostały akty prawne, zarówno międzynarodowe, jak i krajowe, a w szczególności wybrane przepisy Kodeksu karnego. Co do tych ostatnich, najbardziej skupiam uwagę na tych, które dotyczą danych przetwarzanych za pomocą wszelkiego rodzaju systemów informatycznych. Jednak zwróciłam swoją uwagę na te przestępstwa, które nie są *stricte* cyberprzestępstwami, ale użycie odpowiednich narzędzi (np. Internetu), pozwala zaliczyć je na poczet cyberprzestępstw *sensu largo*.

Słowa kluczowe: cyberprzestępczość, cyberbezpieczeństwo, cyberprzestrzeń, przestępstwa komputerowe, ochrona danych, dane wrażliwe, systemy informatyczne, systemy informatyczno-komunikacyjne

Abstract

The aim of this paper is to discuss the nature of cybercrimes as one of the most significant challenges of the 21st century. The study examines relevant legal acts – international and domestic – with a particular Focus on selected issues of the Polish Penal Code (1997). Regarding the latter, the analysis centers primarily on regulations concerning data processed via various types of IT systems. Attention is also given to offenses that, while not strictly cybercrimes, may be classified as cybercrimes *sensu largo* due to the use of specific tools (such as the Internet) in their commission.

Keywords: cybercrimes, cybersecurity, computer crimes, data security, sensitive personal information (SPI), information system, IT and communication systems

1. Wprowadzenie

Istotą artykułu jest przede wszystkim analiza pojęć związanych z cyberprzestępstwami oraz samych przepisów regulujących ten rodzaj przestępstw. Zwrócę również uwagi na pewne nieścisłości w ustawodawstwie krajowym, a także przedstawię przepisy prawa międzynarodowego związane z omawianą tematyką. Cyberprzestępstwa stanowią jedno z najważniejszych i największych wyzwań prawa karnego XXI wieku. Wystarczy spojrzeć na rozwój Internetu i sztucznej inteligencji, dzięki którym, przestępstwa te, stały się dużo bardziej powszechne. Coraz więcej danych, w tym danych wrażliwych, jest przetwarzanych i gromadzonych przez systemy informatyczne. Przykład mogą stanowić: ePUAP; systemy teleinformatyczne, dzięki którym wiele spraw sądowych jest załatwianych tą drogą; Portal Informacyjny, poprzez który można wносить pisma do sądu, zarówno w sprawach karnych, jak i cywilnych; aplikacja mObywatel, która również jest narażona na ataki cyberprzestępców. To są tylko przykłady, nie mówiąc już o danych przetwarzanych przez wiele instytucji rządowych czy też pozarządowych. Poza tymi danymi, które są narażone na różnorakie zagrożenia, są również treści, które sami zamieszczamy w Internecie (w szczególności na portalach społecznościowych). Istnieje również tzw. Dark web (inaczej: Dark net), gdzie można znaleźć wiele nielegalnych rzeczy, jednak nie będzie to stanowiło przedmiotu niniejszego artykułu, gdyż jest to dość złożona kwestia.

Z punktu widzenia tematu niniejszej pracy, ważne są trzy podstawowe pojęcia: cyberprzestrzeń, cyberbezpieczeństwo oraz cyberprzestępstwa. Cyberprzestrzeń to pewna kategoria zbiorcza, charakteryzująca domenę funkcjonującą w oparciu o wcześniej jasno zdefiniowane elementy infrastruktury teleinformatycznej, w tym m.in. komputery, składające się z nich sieci oprogramowanie itp.¹. Patrząc na definicję cyberbezpieczeństwa to odnosi się ona do pewnego poczucia bezpieczeństwa użytkowników sieci teleinformatycznych. A zatem odnosi się do ściśle określonego obszaru działań związanych z bezpieczeństwem informacji, bezpieczeństwem komunikacji (przekazu) oraz bezpieczeństwem samej sieci². Zdefiniowanie samych cyberprzestępstw jest dość trudne i problematyczne. W żadnym akcie prawnym - zarówno na poziomie krajowym, jak i międzynarodowym – nie ma definicji legalnej tego rodzaju przestępstw. Również w samej nauce prawa karnego, czy też naukach pomocniczych, wypracowanie jednolitej definicji jest dość problematyczną kwestią. Samo pojęcie przestępczości komputerowej pojawiło się ok. 1940 roku. Natomiast jedną z pierwszych definicji sformułował D.B. Parker (1978), w której to stwierdzono, że przestępstwo komputerowe to „każdy nielegalny czyn, do którego popełnienia i ścigania niezbędna jest specjalistyczna wiedza o technice komputerowej”³. Jednak patrząc na dzisiejszy rozwój technologii, definicja ta wydaje się być nie do końca aktualna. Uzasadniam to tym, że dzisiaj specjalistyczna wiedza nie do końca jest jedynym potrzebnym składnikiem to popełnienia tego rodzaju przestępstw. Późniejsze próby zdefiniowania tego zjawiska również były częściowo trafne, lecz i tak pojawiały się kwestie problematyczne. Na gruncie prawa polskiego i międzynarodowego, nie ma definicji legalnej cyberprzestępstwa. Jednak trafna wydaje się być

¹ M. M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice 2015, s. 75.

² K. Chałubińska – Jentkiewicz, *Cyberbezpieczeństwo – zagadnienia definicyjne*, „Cybersecurity and Law” 2025, nr 1(13), s. 5.

³ B. Hołyst, *Kryminalistyka*, Warszawa 2023, s. 944.

definicja pochodząca z komunikatu Komisji Europejskiej z 7 lutego 2013 r.⁴. A zatem pojęcie cyberprzestępczości „odnosi się do szerokiego wachlarza różnych rodzajów działalności przestępczej, w przypadku której komputery i systemy informatyczne stanowią podstawowe narzędzie przestępcze lub są głównym celem działania przestępczego”⁵. A zatem można stwierdzić, że cyberprzestępstwa stanowią wszelkie naruszenia dobra chronionego prawem karnym, które zostały popełnione za pomocą komputerów i wszelkiego rodzaju sieci informatycznych.

2. Cyberprzestępstwa a prawo międzynarodowe

Jeśli chodzi o prawo międzynarodowe, pierwszym aktem prawnym, który również obowiązuje Polskę, jest Konwencja budapesztańska o cyberprzestępczości⁶, uchwalona przez Radę Europy. Nakłada ona na państwa – strony obowiązek tworzenia prawa wewnętrznego w taki sposób, aby uwzględniła one wymienione w niej przestępstwa i dotyczące ich kwestie. Konwencja wymienia następujące przestępstwa: nielegalny dostęp (art. 2), nielegalne przechwytywanie danych (art. 3), naruszenie integralności danych (art. 4), naruszenie integralności systemu (art. 5), niewłaściwe użycie urządzeń (art. 6), fałszerstwo komputerowe (art. 7), oszustwo komputerowe (art. 8), przestępstwa związane z pornografią dziecięcą (art. 9), przestępstwa związane z naruszeniem praw autorskich (art. 10), a także inne formy odpowiedzialności, tj. usiłowanie i pomocnictwo lub podżeganie (art. 11). Powyższe przepisy mają odzwierciedlenie w polskim prawie karnym, o czym będzie mowa dalej. Aczkolwiek warto zwrócić uwagę, że prawo krajowe powinno implementować treść Konwencji w całości, czego nie do końca dokonano, ponieważ Konwencja stosuje termin „system komputerowy”, natomiast w jej polskim tłumaczeniu figuruje termin „system informatyczny” (na co szczególną uwagę zwraca F. Radoniewicz⁷). Co do pozostałych elementów, polski ustawodawca w większym stopniu wziął pod uwagę treść Konwencji. Konwencja reguluje również prawo karne procesowe oraz odpowiedzialność za wymienione przestępstwa, jednak celem niniejszego artykułu jest przedstawienie kwestii materialnych. Istotny jest również protokół dodatkowy do Konwencji Rady Europy⁸, który reguluje przestępstwa na tle rasistowskim i ksenofobicznym, popełnione za pomocą systemów komputerowych. A zatem, cyberprzestępstwa na gruncie prawa europejskiego obejmują nie tylko przestępstwa dotyczące systemów informatycznych, ale również popełnione z wykorzystaniem Internetu, inne przestępstwa np. mowę nienawiści, propagowanie treści rasistowskich czy też obrazę uczuć religijnych.

⁴ Wspólny komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno – Społecznego i Komitetu Regionów; Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń /*JOIN/2013/01 final*/; EUR – Lex 52013JC0001.

⁵ K. Witek, *Przestępczość komputerowa – aspekty prawne*, „Edukacja – Technika – Informatyka” 2018, t. 24, nr 2, s. 41.

⁶ Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz. U. z 2015 r., poz. 728).

⁷ F. Radoniewicz, *Cyberprzestępstwa przeciwko danym komputerowym i systemom informatycznym w Kodeksie karnym – propozycje zmian*, Warszawa 2024, s. 30.

⁸ Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems; Strasbourg, 28.01.2003; European Treaty Series – No. 189.

Drugim aktem prawnym międzynarodowym jest, oczekująca na wejście w życie, Konwencja ONZ⁹ dotycząca cyberprzestępstw. Mimo, że nie jest to akt, który jest obowiązujący, warto o nim wspomnieć ze względu na to, że ma zasięg globalny. Jej celem będzie wzmocnienie współpracy międzynarodowej w zakresie zwalczania określonych przestępstw popełnianych za pomocą systemów technologii informacyjno – komunikacyjnych oraz wymiany materiału dowodowego w formie elektronicznej w odniesieniu do poważnych przestępstw. Konwencja ta będzie uwzględniać te same przestępstwa co konwencja Rady Europy, np. nielegalny dostęp, naruszenie integralności systemu. Dodatkowo wylicza jeszcze następujące przestępstwa: nagabywanie lub uwodzenie dziecka przez Internet w celu popełnienia wobec niego przestępstwa seksualnego; rozpowszechnianie intymnych obrazów bez zgody osoby, której dotyczą; pranie dochodów z przestępstwa. Obie konwencje pozostawiają w gestii państw – sygnatariuszy kwestie dotyczące oskarżenia, ścigania, sankcji oraz przedawnienia.

3. Istotne pojęcia z punktu widzenia omawianych cyberprzestępstw

Przechodząc do polskiego prawa karnego, omówię najważniejsze cyberprzestępstwa, które zostały określone w Kodeksie karnym z 1997 r.¹⁰, w rozdziale XXXIII „Przestępstwa przeciwko ochronie informacji”. W k.k. nie ma legalnej definicji cyberprzestępstwa, jednakże w nauce prawa karnego, termin ten występuje właśnie do wybranych przestępstw. Zanim jednak przejdę do omówienia poszczególnych przestępstw, warto zwrócić uwagę na terminologię. W polskiej ustawie karnej, brak jest definicji legalnych, które w pewien sposób precyzowałyby terminologię związaną z cyberbezpieczeństwem i cyberprzestępcami. Nastręcza to trudności interpretacyjnych poniżej omawianych przepisów, ponieważ za każdym razem trzeba odwoływać się do terminologii fachowej zamiast do definicji legalnych, które mogłyby zostać umiejscowione w art. 115 k.k.. W związku z tym, konieczne jest odwoływanie się do innych ustaw oraz do definicji słownikowych poszczególnych pojęć.

Sieć telekomunikacyjna, według ustawy z dnia 12 lipca 2024 r. Prawo komunikacji elektronicznej¹¹, to – zgodnie z art. 2 pkt 58 ustawy – „systemy transmisyjne, a także urządzenia telekomunikacyjne, oprócz urządzeń telekomunikacyjnych urządzeń końcowych, oraz inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają przekazywanie sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od przekazywanej informacji”. Z kolei systemy transmisyjne to zestaw wzajemnie powiązanych ze sobą połączeń związany z przesyłaniem na odległość określonych treści, np. dźwięków, obrazów, tekstów, czy w przypadku cyberprzestrzeni – programów bądź oprogramowani. Natomiast urządzenie telekomunikacyjne to urządzenie elektryczne lub elektroniczne przeznaczone do telekomunikacji (art. 2 pkt 74 ustawy Prawo

⁹ United Nations Convention against Cybercrime; Strengthening International Cooperation for combating Certain Crimes Committed by Means of Informations Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes; konwencja ta nie weszła w życie; <https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html> (dostęp: 22.09.2026 r.).

¹⁰ Dz. U. z 1997 r., nr 88, poz. 553 ze zm.

¹¹ Dz. U. z 2024 r., poz. 1221.

telekomunikacji elektronicznej). Jednak na potrzeby Kodeksu karnego, należałoby albo dokonać superfluum z ustawy Prawo telekomunikacji elektronicznej, ewentualnie stworzyć podobną definicję, która mogłaby brzmieć „Sieć telekomunikacyjna to system powiązanych ze sobą urządzeń transmisyjnych, takich jak urządzenia elektryczne lub elektroniczne, za pomocą których następuje przesyłanie danych”. Taka definicja, która jest również niepełna i nieprecyzyjna, byłaby bardziej stosowna niż jej brak, ponieważ dla popełnienia cyberprzestępstwa nie ma znaczenia nazwa konkretnego urządzenia, ale jego rodzaj (gatunek), natomiast znaczenie ma sam fakt dokonania i przeciwko jakiemu dobru chronionemu prawem jest ono popełnione.

Kolejnym problematycznym pojęciem jest „system komputerowy”. Polski ustawodawca stosuje pojęcie zamienne „system informatyczny”, jednak jest to błędne, ponieważ te dwa pojęcia mają inne znaczenia. System informatyczny, według art. 1 ust. a Konwencji o cyberprzestępczości, „oznacza każde urządzenie lub grupę wzajemnie połączonych lub związanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, wykonuje automatyczne przetwarzanie danych”. Natomiast system komputerowy, według art. 1(a) raportu wyjaśniającego do Konwencji o cyberprzestępczości to „urządzenie składające się ze sprzętu i oprogramowania, oprogramowane w celu automatycznego przetwarzania danych cyfrowych. Może ono obejmować elementy służące do wprowadzania i wyprowadzania danych oraz ich przechowywania. Może funkcjonować samodzielnie lub być połączone w sieć z innymi podobnymi urządzeniami”¹². A zatem system informatyczny odnosi się do grupy powiązanych ze sobą urządzeń, natomiast system komputerowy do tylko jednego urządzenia. Słowo „automatycznie” oznacza tyle, co bez ingerencji człowieka.

Od systemu informatycznego należy rozróżnić system teleinformatyczny oraz sieć teleinformatyczną. System teleinformatyczny, według art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, to „zespoł współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniających przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 12 lipca 2004 r. – Prawo komunikacji elektronicznej”. Natomiast obecnie w żadnej z obowiązujących ustaw nie ma definicji sieci teleinformatycznych. Jednak, jak wskazuje F. Radoniewicz, sieć ta „jest zespołem systemów teleinformatycznych, czyli systemów informatycznych, w których przetwarzane są dane, powiązane ze sobą sieciami telekomunikacyjnymi, służącymi przesyłaniu danych między tymi systemami”. Przede wszystkim system teleinformatyczny opiera się na urządzeniach, które w określony sposób, współpracują ze sobą. Z kolei sieć teleinformatyczna jest zespołem systemów informatycznych, które z kolei są ze sobą powiązane za pomocą sieci telekomunikacyjnych. Te systemy i urządzenia współpracują ze sobą również za pomocą transmisji danych. Transmisja to „przesyłanie danych, sygnałów na odległość przy użyciu odpowiednich urządzeń”¹³. Pojęcie to jest istotne z tego względu, że popełnienie przestępstw komputerowych może wiązać się z przesłaniem treści czy też np. oprogramowania infekującego

¹² Explanatory Report to the Convention on Cybercrime, Budapest, 23.11.2001.

¹³ Wielki Słownik Języka Polskiego PAN, hasło: *transmisja sygnałów*, <https://wsjp.pl/haslo/podglad/36151/transmisja/3946505/sygnaLOW> (dostęp: 14.09.2026 r.).

inne narzędzia. Transmisja wiąże się również z funkcjonowaniem podsłuchu czy też urządzeń wizualnych lub audiowizualnych, których użycie bez zgody osoby nagrywanej, jest nielegalne. W przestępstwach przeciwko ochronie informacji, na uwagę zasługuje pojęcie danych. Można wyróżnić ich trzy rodzaje: dane informatyczne, dane dotyczące ruchu oraz dane osobowe. Dane informatyczne i dotyczące ruchu są stricte powiązane z systemami komputerowymi bądź też informatycznymi. Ponownie odwołując się do Konwencji budapesztańskiej, a dokładniej do art. 1 ust. b, dane informatyczne „oznaczają dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny”, z kolei dane dotyczące ruchu (art. 1 ust. d Konwencji budapesztańskiej) to „dowolne dane informatyczne odnoszące się do komunikowania się za pomocą systemu informatycznego, wygenerowane przez system informatyczny, który utworzył część w łańcuchu komunikacyjnym, wskazujące swoje pochodzenie, przeznaczenie, ścieżkę, czas, datę, rozmiar, czas trwania lub rodzaj danej usługi”. Dane informatyczne są więc pewnym zapisem, o dowolnej treści, umiejscowione w systemie komputerowym (np. pliki, zdjęcia przechowywane na dysku), a dane dotyczące ruchu, w swoisty dla siebie sposób, opisują pewne właściwości (np. w przypadku przesłanego pliku za pośrednictwem mail’a, będzie to rozmiar pliku, czas przesłania, numery IP urządzenia, z którego wyszła wiadomość i dane odbiorcy itd.). Dane osobowe mogą być pewnym elementem ww. danych w przypadku, gdy takie dane zostaną przesłane. Ich definicję legalną można znaleźć w art. 4 pkt 1 Rozporządzenia 2016/679¹⁴ i są to dane, które „oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej”. Dane osobowe są objęte prawnokarną ochroną w tym znaczeniu, że ich udostępnienie czy naruszenie w jakikolwiek sposób przez osobę nieuprawnioną, stanowi czyn zabroniony.

4. Cyberprzestępstwa na gruncie Kodeksu karnego

Jednym z nich jest bezprawne uzyskanie informacji, które zostało określone w art. 267 § 1 k.k., który mówi, że „Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2”. W przepisie tym przewidziane są cztery równoważne sposoby uzyskania bez uprawnienia dostępu do informacji warunkujące odpowiedzialność karną: otwarcie zamkniętego pisma; podłączenie się do sieci telekomunikacyjnej; przełamanie albo ominięcie

¹⁴ Rozporządzenie 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

elektronicznego, magnetycznego, informatycznego lub innego szczególnego jej zabezpieczenia¹⁵. Dla odpowiedzialności karnej, za omawiany czyn, bez znaczenia jest czy sam sprawca zapoznał się z daną informacją czy ją zrozumiał. Przede wszystkim informacja ta, jeśli nie jest skierowana do sprawcy czynu określonego w ww. przepisie, jest zdobyta w sposób nielegalny. Inny przypadek stanowiłaby sytuacja, gdyby dana osoba uczestniczyła w rozmowie i za zgodą innych uczestników, utrwalałaby w jakikolwiek treści przekazywane podczas rozmów. Jeśli chodzi o dane, które są zawarte w danych informatycznych itp. uzyskanie takich informacji może nastąpić poprzez tzw. hacking. Polega on na usunięciu szczególnych konstrukcji, „osłon”, które służą uniemożliwieniu dostępu do informacji zgromadzonych w systemie¹⁶. W przepisie tym jest mowa o szczególnych zabezpieczeniach, co jest równoznaczne ze specjalistycznymi i zaawansowanymi zabezpieczeniami, a więc nie wystarczy tylko np. złamanie hasła, lecz „przebicie się” przez złożone zabezpieczenia. Istotnym pojęciem jest „system informatyczny”, które już wcześniej zostało szerzej omówione. A zatem jedno lub więcej urządzeń musi przetwarzać dane, których dotyczy popełnione przestępstwo. Jednak najważniejszą kwestią dotyczącą omawianego przestępstwa, jest ujawnienie informacji. Czasownik „ujawnić” to uczynić jawnym, wiadomym; wykryć, zdemaskować; ujawnianiem informacji jest każde zachowanie, w wyniku którego doszła ona do wiadomości osoby nieuprawnionej; ujawnienia nie można utożsamiać z rozpowszechnianiem, które oznacza czynienie informacji powszechnie wiadomą, udostępnianie jej szerszemu, bliżej nieokreślonemu kręgowi osób¹⁷. Czyli chodzi po prostu o podanie do wiadomości, danej informacji, osobie lub osobom nieuprawnionym. Ściganie za bezprawne ujawnienie informacji następuje na wniosek pokrzywdzonego (art. 267 § 4). Czyn zabroniony opisany w art. 267 § 2 k.k., objęty jest kontratypem działania w celu wykrycia błędów w systemach informatycznych, tzn. nie popełnia przestępstwa ten, kto działając w celu zabezpieczenia dóbr wymienionych w art. 267 k.k., wypełni znamiona czynu zabronionego, co wynika z art. 269c k.k.

Kolejnym z omawianych przestępstw jest utrudnianie zapoznania się z informacją (art. 268 k.k.)¹⁸. Sankcja za utrudnienie zapoznania się z informacją, na podstawie art. 268 § 2 wynosi 3 lata pozbawienia wolności, jeśli informacja ta jest dostępna na nośnikach informatycznych. Można to uzasadniać tym, że złamanie dostępu do tych informacji jest trudniejsze, a także obecnie jest więcej danych trzymanych na takich nośnikach, co wiąże się z większym prawdopodobieństwem utrudnienia dostępu do większej ilości takich informacji. Niszczenie i uszkodzanie nie odnosi się tylko i wyłącznie do samego nośnika, ale również do informacji w nim umieszczonych. Usunięcie polega na całkowitej likwidacji danych z nośnika. Istotna jest różnica pomiędzy „udaremnieniem”, a „utrudnieniem” dostępu do informacji. Udaremnienie polega na całkowitym uniemożliwieniu dostępu do informacji osobie uprawnionej (tzn. sytuacja, w której uprawniona osoba zostaje całkowicie pozbawiona możliwości zapoznania się z określoną informacją¹⁹), natomiast utrudnienie wiąże się z

¹⁵ A. Behan, *Komentarz do art. 267*, [w:] *Kodeks karny. Komentarz*, red. J. Kulesza, Warszawa 2025, teza 3.

¹⁶ P. Kozłowska – Kalisz, *Komentarz do art. 267* [w:] *Kodeks karny. Komentarz*, red. M. Mozgawa, Warszawa 2026, LEX/el., teza 6.

¹⁷ *Ibidem*, teza 5.

¹⁸ „Kto, nie będąc do tego uprawnionym, niszczy, uszkodza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2” (art. 268 § 1 k.k.).

¹⁹ A. Behan, *op. cit.*, teza 2.

wprowadzeniem przeszkód, dla osoby uprawnionej, do dostępu do informacji. Samo utrudnienie musi być znaczne i musi w istotny sposób utrudniać zapoznanie się z informacją przez osobę uprawnioną. Wykorzystanie uzyskanych informacji znaczy tyle, co uczynienie z nich pożytku dla siebie. Informatyczny nośnik danych, zgodnie z definicją legalną z art. 3 pkt 1 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, to materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej²⁰. Znamiona czynów zabronionych z §1 - §3 mogą zostać popełnione tylko i wyłącznie umyślnie. Ściganie tego przestępstwa również następuje na wniosek pokrzywdzonego, co wynika z art. 268 § 4 k.k.

Art. 268a k.k. dotyczy niszczenia danych informatycznych i jest to przestępstwo powszechne, tzn. każdy może je popełnić. W przepisie tym penalizowanych jest kilka rodzajów zachowania się sprawcy, „Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3” (art. 268a § 1 k.k.). Zniszczenie danych odnosi się tylko do treści, a nie do samego *corpus mechanicum*. A więc nie odnosi się to przestępstwo do zniszczenia nośnika, np. dysku, tylko danych, które były na nim przechowywane. Jeśli dane są zapisane w chmurze lub istnieje kopia danych to dochodzi do zniszczenia tylko i wyłącznie wyżej wspomnianego *corpus mechanicum*. Jednak w przypadku zniszczenia dysku lub płyty CD lub pendrive’a, gdy nie zapisano żadnej ich kopii – czy to w chmurze, czy też w innym miejscu – dochodzi do wypełnienia znamion przestępstwa z art. 268a § 1. Przestępstwa określone w nim mają charakter skutkowy oraz mogą zostać popełnione umyślnie. W § 2 jest kwalifikowana postać niszczenia danych informatycznych, która wiąże się z wyrządzeniem znacznej szkody majątkowej (tj. mienie przekraczające 200 000 złotych²¹). Nie ma tutaj znaczenia rodzaj przetwarzanych informacji, lecz tylko i wyłącznie sam fakt zakłócania dostępu czy też zniszczenie danych informatycznych lub ich gromadzenie. Również za przeszkadzanie w przekazywaniu danych informatycznych, sprawca będzie podlegał odpowiedzialności karnej na podstawie omawianego przepisu. Przekazanie polega na transmisji danych lub udostępnieniu nośnika danych innej, nieuprawnionej osobie.

Uszkodzenie danych informatycznych (art. 269 k.k.) obejmuje zniszczenie danych przechowywanych na nośniku, a nie samego *corpus mechanicum*. A zatem nie zostają wypełnione znamiona czynu zabronionego, jeśli np. dojdzie do fizycznego uszkodzenia dysku, a dane w nim zawarte pozostaną nienaruszone. Nie należy mylić uszkodzenia ze zniszczeniem, gdyż zniszczenie wiąże się z całkowitym unicestwieniem rzeczy²². Przedmiotem ochrony są zatem systemy ich integralność oraz informacje zawarte na danym nośniku, które mają szczególne znaczenie dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego (art. 269 § 1 k.k.). Natomiast wymiana, opisana w art. 269 § 2 k.k., polega na zastąpieniu właściwego nośnika innym nośnikiem. Omawiane przestępstwo jest przestępstwem

²⁰ Dz. U. z 2025 r., poz. 1703.

²¹ Art. 115 § 5 k.k.

²² G. Łabuda, *Komentarz do art. 288 Kodeksu karnego* [w:] *Kodeks karny. Część szczególna. Komentarz*, red. J. Giezek, Warszawa 2021, teza 10.

skutkowym oraz może być popełnione z zamiarem bezpośrednim (*dolus directus*) i ewentualnym (*dolus eventualis*). Za to przestępstwo grozi sankcja pozbawienia wolności od 6 miesięcy do ośmiu lat. Z kolei art. 269a k.k. normuje kwestie dotyczące zakłóceń systemów komputerowych. Są to podobne przepisy z tym, że art. 269 k.k. dotyczy m.in. obronności i bezpieczeństwa państwa, natomiast w omawiany przepis jest bardziej ogólny, bo dotyczy wszelkich systemów komputerowych. Poza tym przestępstwo to może być popełnione tylko i wyłącznie poprzez działanie oraz umyślnie. Za zakłócenie systemów komputerowych grozi kara od 3 miesięcy do 5 lat pozbawienia wolności. Art. 269a k.k. jest objęty kontratypem, który polega na działaniu w celu wykrycia błędów w zabezpieczeniach systemów teleinformatycznych (art. 296c k.k.). Przykładowo gdyby ktoś próbował wykryć błędy i doszłoby do zniszczenia czy naruszenia danych, sprawca ten nie ponosi odpowiedzialności karnej.

Istotnym przestępstwem, z punktu widzenia niektórych wyżej wymienionych (tj. art. 267 § 3, art. 268a §1 albo §2 w zw. z §1, art. 269 §1 lub §2, art. 269a), jest wytwarzanie, pozyskiwanie, zbywanie lub udostępnianie narzędzi hakerskich (art. 269b k.k.). Jednak dotyczy to wybranych przestępstw (katalog zamknięty), a są to: sprowadzenie stanów powszechnie niebezpiecznych dla życia lub zdrowia poprzez zakłócanie, uniemożliwianie lub wpływanie w inny sposób na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych, (art. 165 § 1 pkt 4 k.k.); niszczenie danych informatycznych (art. 268a §1 albo §2 w zw. z §1 k.k.); uszkodzenie danych informatycznych (art. 269 §1 lub §2 k.k.); zakłócenie systemu komputerowego (art. 269a k.k.); fałszerstwo materialne (art. 270 §1 k.k.); fałszerstwo materialne faktur (art. 270a §1 k.k.). Art. 269b §1a k.k. przewiduje kontratyp, który nie zakłada kary dla sprawcy omawianego przestępstwa, jeśli działa w celu zabezpieczenia dóbr chronionych przez przepis z §1. Przestępstwo to może być popełnione zarówno przez działanie jak i zaniechanie, z wyjątkiem wytwarzania narzędzi hakerskich, ponieważ może być ono tylko i wyłącznie popełnione poprzez działanie. Przykładami takich programów są: malware, ransomware, malware FakeUpdates, Qbot. Przepis ten uwzględnia nie tylko urządzenia lub programy komputerowe, za pomocą których można popełnić ww. przestępstwa, ale również hasła komputerowe, kody dostępu oraz inne dane umożliwiające nieuprawniony dostęp. Ustawodawca posługuje się w tym przepisie liczbą mnogą, jednak warto zwrócić uwagę, że do popełnienia tego przestępstwa wystarczy jedno hasło czy też jedno oprogramowanie. Warunkiem jest to, aby były one przystosowane do popełnienia przestępstw wymienionych w omawianym przepisie. Przestępstwo to jest powszechne oraz można je popełnić tylko umyślnie. Przewidzianą sankcją jest kara pozbawienia wolności od 3 miesięcy do 5 lat. Dodatkowo sąd orzeka przepadek określonych w nim przedmiotów, a może orzec ich przepadek, jeżeli nie stanowiły własności sprawcy (§2).

Poza powyżej omówionymi przestępstwami, w polskim Kodeksie karnym można znaleźć inne czyny zabronione, które należy zaliczyć do grupy cyberprzestępstw. Jednym z nich jest elektroniczna korupcja seksualna małoletniego (art. 200a § 1 k.k.). Polega ono na doprowadzenia do zgwałcenia małoletniego poniżej 15 roku życia lub seksualnego wykorzystania małoletniego, jak i również produkowaniu lub utrwalaniu treści pornograficznych, za pośrednictwem systemu teleinformatycznego lub sieci telekomunikacyjnej nawiązuje kontakt z małoletnim poniżej lat 15. Do wypełnienia znamion

czynu zabronionego, w omawianym przepisie, jest zmierzanie, za pomocą wprowadzenia go w błąd, wyzyskania błędu lub niezdolności do należytego pojmowania sytuacji albo przy użyciu groźby bezprawnej, do spotkania z nim. Wprowadzenie w błąd może polegać zarówno na działaniu (np. podanie nieprawdziwych informacji, posługiwanie się podrobionymi zdjęciami), jak i na zaniechaniu (np. przemilczenie istotnych informacji, z punktu widzenia omawianego przestępstwa). Czyn ten musi być popełniony za pomocą systemu teleinformatycznego lub sieci telekomunikacyjnej, dlatego też bezpośrednie nawiązanie kontaktu z małoletnim nie wypełnia znamion czynu zabronionego z art. 200a k.k. (w przeciwnym razie jest to usiłowanie przestępstwa z art. 200 § 1 k.k.). Czyn opisany w art. 200a § 2 k.k. polega na bezpośrednim złożeniu propozycji małoletniemu, a nie tak jak we wcześniejszym paragrafie, poprzez wprowadzenie w błąd. Jest możliwe popełnienie obu przestępstw z art. 200a k.k., poprzez samo złożenie propozycji za pośrednictwem odpowiednich środków przekazu. Przestępstwa te mają charakter powszechny i formalny oraz mogą być popełnione z zamiarem bezpośrednim (*dolus directus*) oraz ewentualnym (*dolus eventualis*).

Kolejnym istotnym przestępstwem, z punktu widzenia cyberbezpieczeństwa oraz obyczajności, jest propagowanie publicznie zachowań o charakterze pedofilskim (art. 200b k.k.). Publiczne propagowanie ww. zachowań oznacza to, że treści te muszą być dostępne dla większej (nieokreślonej) lub nieograniczonej liczby osób, które mogłyby się zapoznać z przekazywanymi przez sprawcę treściami²³. Jeśli propagowanie następuje poprzez Internet, jako środek masowego przekazu, możemy mówić o cyberprzestępstwie. Również propagowanie pedofilii poprzez sieci takie jak np. Darknet, stanowią cyberprzestępstwo. Przestępstwo ma charakter powszechny (czyli może je popełnić każdy) oraz formalny. Może ono zostać popełnione jedynie z zamiarem bezpośrednim (*dolus directus*). Do kolejnego cyberprzestępstwa, związanego z obyczajnością, jest prezentowanie treści pornograficznych publicznie (art. 202 k.k.). Katalog zachowań, które wypełniają czyn zabroniony z art. 202 k.k., jest bardzo szeroki. Dotyczy on bowiem samego prezentowania treści pornograficznych publicznie osobom, które sobie tego nie życzą (§ 1), jak i również treści pornograficznych związanych z pedofilią oraz zoofilią (§3 – §4c). Prezentacja polega na udostępnieniu większemu gronu odbiorców (adresatami prezentowanych treści jest kilka osób – brak ustawowego wskazania ile konkretnie osób – które są bliżej nieokreślone, tzn. prezentowane treści nie są skierowane do konkretnych osób tylko do przypadkowej grupy odbiorców) wskazanych treści za pomocą Internetu, banerów, plakatów czy innych form. Istotne jest pojęcie „publicznie”, które nie sprowadza się do samego miejsca publicznego, ale takiego, gdzie ww. treści trafią do nieograniczonej liczby osób. Natomiast przechowywanie nie jest równoznaczne z chwilowym przetrzymywaniem materiału pornograficznego, lecz sam fakt świadomego przetrzymywania tych treści czy też ich posiadania. Wszystkie te przestępstwa mają charakter powszechny i mogą być popełnione umyślnie.

Novum w prawie karnym stanowi patostreaming (art. 255b k.k.). Co ciekawe, patostreaming jest polskim „wynałazkiem”, a na Zachodzie takie zjawisko jest niemal nieznane²⁴. Jest to rozpowszechnianie publicznie transmisji internetowych zawierających

²³ T. Lipiński, *Komentarz do art. 200b [w:] Kodeks karny. Część szczególna. Komentarz*, red. J. Giezek, Warszawa 2021, teza 8.

²⁴ D. Ołownia, *Patostreaming jako zjawisko patologiczne i dewiacyjne*, „iNFOTEZY” 2021, nr 2(11), s. 64.

patologiczne społecznie treści, np. libacje alkoholowe, przemoc fizyczną i słowną, molestowanie seksualne²⁵. Twórcy tych treści otrzymują najczęściej profity, które są udzielane przez oglądających, ale nie muszą to być korzyści majątkowe (mogą to być również korzyści osobiste). W Kodeksie karnym wymienione są następujące treści: popełnienie czynu zabronionego zagrożonego karą pozbawienia wolności, jeżeli przedmiotem zamachu jest dobro osobiste; przemoc wobec zwierzęcia z naruszeniem przepisów ustawy; poniżające traktowanie innej osoby, nawet za jej zgodą. Znamiona tego czynu zabronionego, opisane w art. 255b § 1 k.k., wypełnia również publiczne rozpowszechnianie treści mogących wywołać przekonanie, że przedstawiają ww. zachowania (art. 255b § 2 k.k.). Powyższe przestępstwa są zagrożone karą pozbawienia wolności do lat 3. Wyższa sankcja, tj. pozbawienie wolności od 3 miesięcy do 5 lat, jest przewidziana za treści, które przedstawiają małoletniego (art. 255b § 3 k.k.). Zamachem na dobro osobiste jest sytuacja, w której to dobro osobiste jest chronione przez Kodeks karny lub inną ustawę (z odwołaniem do niniejszego przepisu). W § 4 opisany jest kontratyp, zgodnie z którym nie stanowi przestępstwa działanie w ramach działalności artystycznej, edukacyjnej, informacyjnej, prasowej lub naukowej albo w celu ochrony interesu publicznego.

Przestępstwami, które mogą być popełnione za pomocą środków masowego przekazu, w tym Internetu (szczególnie za pomocą mediów społecznościowych), są zniesławienie (art. 212 k.k.) oraz zniewaga (art. 216 k.k.). Ważna jest różnica pomiędzy tymi przestępstwami. Zniesławienie (inaczej: pomówienie) to przestępstwo, sprowadzające się do zachowania, przez które sprawca przypisuje innemu podmiotowi negatywnie oceniane właściwości lub postępowanie, co może spowodować do poniżenia tego ostatniego²⁶. Typ kwalifikowany tego przestępstwa, sprowadza się właśnie do popełnienia jego za pomocą środków masowego przekazu, w tym Internetu (art. 212 § 2 k.k.). Jeśli chodzi o zniewagę to nie ma definicji legalnej tego pojęcia, ani też nie zostało sprecyzowane jak należy interpretować to pojęcie. Jednak w doktrynie i orzecznictwie możemy znaleźć pogląd, że są to wszelkie zachowania sprawcy, które w sposób demonstracyjny wyrażają pogardę dla innej osoby, a w szczególności mają poniżyć jej godność osobistą i sprawić, by poczuła się dotknięta lub obrażona²⁷. Dla ustawodawcy obojętne jest to, czy ten czyn został popełniony pod obecność tej osoby czy też nie, ale ważne jest to, aby dotarło to do tej osoby. W § 2 omawianego przepisu opisana została postać kwalifikowana czynu, tj. popełnienie go za pomocą środków masowego komunikowania. Oba przestępstwa mogą być popełnione tylko i wyłącznie poprzez działanie oraz są ścigane z oskarżenia prywatnego.

Poza powyżej wskazanymi przestępstwami, są również inne, które można popełnić za pomocą Internetu, a tym samym zaliczyć je jako cyberprzestępstwa. Są to: publiczne nawoływanie do popełnienia przestępstw z rozdziału XVI lub ich publiczne pochwalanie (art. 126a k.k.), np. nawoływanie lub pochwalanie ludobójstwa czy też dyskryminacji; znieważenie narodu lub państwa polskiego (art. 133 k.k.); znieważenie prezydenta RP (art. 135 § 2 k.k.); publiczne znieważenie znaku lub symbolu państwowego (art. 137 k.k.); propagowanie

²⁵ <https://obserwatoriumjezykowe.uw.edu.pl/hasla/patostreaming/> (dostęp: 28.08.2026).

²⁶ J. Raglewski, *Komentarz do art. 212 [w:] Kodeks karny. Część szczególna. Komentarz. Tom II. Część II.*, red. W. Wróbel, A. Zoll, Warszawa 2017, teza 1.

²⁷ M. Marek, *Komentarz do art. 216 [w:] Kodeks karny. Komentarz*, red. M. Mozgawa, Warszawa 2026, LEX/el. teza 3.

nazizmu, komunizmu, faszyzmu lub innego ustroju totalitarnego (art. 256 k.k.); napaść z powodu ksenofobii, rasizmu lub nietolerancji religijnej (art. 257 k.k.). Są to wybrane przestępstwa z Kodeksu karnego, jednak istotne nie tylko z punktu widzenia samego faktu, że są one przestępstwami, jednak również z tego względu, że ich popełnienie może mieć miejsce w Internecie. Część społeczeństwa podnosi zarzut, że przepisy te stanowią ograniczenie wolności słowa, jednak patrząc na to, że Internet jest narzędziem powszechnie używanym, przepisy te mają sens, a ich obecność zapewnia również bezpieczeństwo w państwie (zarówno wewnętrzne jak i zewnętrzne).

5. Podsumowanie

Cyberprzestępstwa są coraz bardziej powszechne, a ich znaczenie i częstotliwość rośnie wraz z rozwojem nowych technologii. Kwestia ta nabiera szczególnego znaczenia w związku z wojną na Ukrainie, gdyż wszelkie próby destabilizacji bezpieczeństwa przez Rosję, mają i będą mieć miejsce również w cyberprzestrzeni. Tak jak już wspomniałam na wstępie, wiele naszych danych wrażliwych, jest przechowywane w różnych sieciach informatycznych, które są narażone bezpośrednio na wszelakie ataki, zarówno w sferze wewnętrznej (krajowej), jak i zewnętrznej (międzynarodowej). Również ze względu na wszelkie próby dezinformacji, cyberprzestrzeń powinna być jak najlepiej chroniona. Szczególną ochroną powinni zostać objęci małoletni, ze względu na ich prawidłowy rozwój psychiczny. W tym zakresie państwo powinno zwracać szczególną uwagę na to, jakie treści docierają do dzieci i młodzieży. Takie działanie powinno być podejmowane nie tylko poprzez wprowadzanie nowych przepisów, ale również poprzez zapewnienie rzetelnej edukacji w zakresie korzystania z Internetu, w tym ze sztucznej inteligencji. Istotna jest także współpraca ze służbami oraz instytucjami (krajowymi i międzynarodowymi), które za swój cel biorą ochronę cyberbezpieczeństwa.

Bibliografia

Akty prawne:

Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems; Strasbourg, 28.01.2003.

Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz. U. z 2015 r., poz. 728).

United Nations Convention against Cybercrime; Strengthening International Cooperation for combating Certain Crimes Committed by Means of Informations Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes; konwencja ta nie weszła w życie; <https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html>, (dostęp: 22.09.2026 r.).

Ustawa z dnia 6 czerwca 1997 r., Kodeks karny (Dz. U. z 1997 r., nr 88, poz. 553).

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2005 r., nr 64, poz. 565).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r., poz. 1560).

Ustawa z dnia 12 lipca 2024 r. Prawo komunikacji elektronicznej (Dz. U. z 2024 r., poz. 1221).
Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 7 listopada 2025 r. w sprawie ogłoszenia jednolitego tekstu ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2025 r., poz. 1703).

Literatura:

Behan A., *Komentarz do art. 267*, [w:] *Kodeks karny. Komentarz*, red. J. Kulesza, Warszawa 2025.

Bielski M., *Koncepcja kontratypów jako okoliczności wyłączających karalność*, „Czasopismo Prawa Karnego i Nauk Penalnych” 2010, rok XIV, z. 2.

Chałubińska – Jentkiewicz K., „Cyberbezpieczeństwo – zagadnienia definicyjne”, „Cybersecurity and Law” 2025, nr 1(13).

Czerski Wojciech M., *Rola mediów w przeciwdziałaniu przestępczości komputerowej wśród osób (nie)kompetentnych cyfrowo*, „Dydaktyka Informatyki” 2024, nr 19.

Hołyst B., *Kryminalistyka*, Warszawa 2023.

Karpiuk M., *Computer fraud*, „Cybersecurity and Law” 2023, nr 2(10).

Kozłowska – Kalisz P., *Komentarz do art. 267* [w:] *Kodeks karny. Komentarz*, red. M. Mozgawa, Warszawa 2026.

Lakomy M. M., *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice 2015.

Lipiński T., *Komentarz do art. 200b*, [w:] *Kodeks karny. Część szczególna. Komentarz*, red. J. Giezek, Warszawa 2021.

Łabuda G., *Komentarz do art. 288 Kodeksu karnego.*, [w:] *Kodeks karny. Część szczególna. Komentarz*, red. J. Giezek, Warszawa 2021.

Marek M., *Komentarz do art. 216* [w:] *Kodeks karny. Komentarz*, red. M. Mozgawa, Warszawa 2026, LEX/el. teza 3.

Ołownia D., *Patostreaming jako zjawisko patologiczne i dewiacyjne*, „iNFOTEZY” 2021, nr 2(11).

Radoniewicz F., *Cyberprzestępstwa przeciwko danym komputerowym i systemom informatycznym w Kodeksie karnym – propozycje zmian*, Warszawa 2024.

Radoniewicz F., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016.

Raglewski J., *Komentarz do art. 212 [w:] Kodeks karny. Część szczególna. Komentarz. Tom II. Część II.*, red. W. Wróbel, A. Zoll, Warszawa 2017, teza 1.

Rosiak Ł., *Patostreaming – istota projektowanego art. 255b kodeksu karnego*, „Prokuratura i Prawo” 2024, nr 3.

Skoczylas D., *The act on the national cybersecurity system and other legal regulations in the context of ensuring state cybersecurity. Selected issues*, „Roczniki Nauk Prawnych” 2020, t. XXX, nr 2.

Witek K., *Przestępczość komputerowa – aspekty prawne*, „Edukacja – Technika – Informatyka” 2018, t. 24, nr 2.

Pozostałe źródła:

https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/cybersecurity-service-union-institutions-bodies-offices-and-agencies-cert-eu_pl (dostęp: 01.09.2026 r.).

<https://obserwatoriumjezykowe.uw.edu.pl/hasla/patostreaming/> (dostęp: 28.08.2026 r.).

Proposal for a regulation of the European Parliament and of the Council on the European Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2); Strasbourg, 20.01.2026, COM (2026) 11 final, 2026/0011 (COD).

<https://wsjp.pl/haslo/podglad/36151/transmisja/3946505/sygnalow> (dostęp: 14.09.2026 r.).

Wspólny komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno – Społecznego i Komitetu Regionów; *Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń* /*JOIN/2013/01 final*/; EUR – Lex 52013JC0001.