Sprawca a ofiara przestępstwa w internecie

Justyna Gręda, Jan Ściga, Marcin Wolak, Maciej Kornaus

Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie

Wraz z zapoczątkowaniem dynamicznego rozwoju sieci internet w latach dziewięćdziesiątych dwudziestego wieku światowe firmy technologiczne bardzo mocno inwestują w rozwój globalnej sieci oraz usług w niej oferowanych. Jednym z największych obszarów ich zainteresowań są platformy społecznościowe, które oferują interakcję oraz dostęp do wymiany treści multimedialnych pomiędzy milionami użytkowników na całym świecie. Pomimo niewątpliwych olbrzymich szans kreowanych przez rozwój technologiczny, w tym obszarze powstaje również gigantyczna przestrzeń do nadużyć, która może być spożytkowana do wielu rodzajów przestępstw zwanych cyberprzestępstwami. Mamy zatem wspólny, zupełnie nowy obszar, na którym znajdują się zarówno potencjalni sprawcy jak i ofiary. W tej pracy koncentrujemy się na wielodomenowym spojrzeniu na sylwetkę ofiary, sprawcy oraz przedmiotu ich relacji czyli cyberprzestępstwa dokonywanego w świecie internetu.

cyberbezpieczeństwo | przestępczość internetowa | ofiara | sprawca | teleinformatyka | internet | stalking | prawo | kryminalistyka | socjologia | hacking

Wstęp

Zanim zagłębimy się w temacie cyberprzestępstw, warto na moment pochylić się nad aspektem szeroko pojętego bezpieczeństwa w różnych dziedzinach życia człowieka. Według Słownika Języka Polskiego, bezpieczeństwo definiowane jest jako *stan niezagrożenia* (1). Politycy i historycy od wieków analizują pojęcie bezpieczeństwa narodowego, czyli sytuacji, w której państwo i jego mieszkańcy mają poczucie pewności, że nie stoją przed zagrożeniem gospodarczym, kulturowym, politycznym czy ekologicznym (2). Coraz częściej mówi się także o bezpieczeństwie społecznym - ochronie praw człowieka, zaspokojeniu jego potrzeb i umożliwieniu rozwoju (3). Możemy więc wnioskować, że cyberbezpieczeństwo to sytuacja, w której nie czujemy się zagrożeni podczas przebywania w tzw. cyberprzestrzeni. Stan ten mogą zakłócać cyberprzestępcy - osoby fizyczne lub grupy zorganizowane, które za pośrednictwem metod teleinformatycznych prowadzą nastawioną na cudzą szkodę nielegalną działalność (4). Ich ofiarami padają nie tylko jednostki, ale także instytucje. Według serwisu Statista, w 2022 roku straty wynikające z cyberataków sięgnęły kwoty 7,1 biliona dolarów, co stanowi niemal 600% wzrost w stosunku do kwoty 1,2 biliona zarejestrowanej w 2019 roku (5). W ramach projektu chcemy ukazać sprawców i ofiary cyberprzestępstw w aspekcie prawnym, kryminalistycznym oraz społecznym, przyjrzeć się dokładniej samej definicji cyberprzestępstwa, a także przedstawić wyniki badania dotyczącego cyberbezpieczeństwa przeprowadzonego w naszym bliskim otoczeniu.

Spojrzenie prawne

Jak zostało wskazane w (6) cyberprzestrzeń to obszar stworzony przy użyciu najnowszych technologii informatycznych, a określenie jej jest zadaniem, które wymaga współpracy różnych dziedzin nauki. Wobec tego rozumiana jest ona jako logiczna domena ludzkiej działalności, jako środowisko wirtualne, oderwane od elementu fizycznego. Tym samym popularną definicją cyberprzestępstwa jest czyn zabroniony w rozumieniu dowolnego przepisu prawnego gdzie miejscem popełnienia czynu musi być cyberprzestrzeń. Zawężając definicję moglibyśmy zamienić miejsce popełnienia czynu na internet. Niestety częścią płynną definicji pozostaje czy całość, a jeśli nie, to jak duża część przestępstwa musi mieć miejsce w świecie wirtualnym. Opierając się o tą definicje możemy wskazać ogólną definicję ofiary cytując ją z "Polskiej Karty Praw Ofiary"(7): ”Ofiarą w rozumieniu Karty jest osoba fizyczna, której dobro prawem chronione zostało bezpośrednio naruszone lub zagrożone przez przestępstwo, a także jej najbliżsi”. Aby zdefiniować sprawcę możemy posłużyć się ”Kodeksem Karnym” albowiem zgodnie z art. 1 par. 1 k.k., ”Odpowiedzialności karnej podlega ten tylko, kto popełnia czyn zabroniony pod groźbą kary przez ustawę obowiązującą w czasie jego popełnienia.” oraz art. 18 par. 1 k.k., ”Odpowiada za sprawstwo nie tylko ten, kto wykonuje czyn zabroniony sam albo wspólnie i w porozumieniu z inną osobą, ale także ten, kto kieruje wykonaniem czynu zabronionego przez inną osobę lub wykorzystując uzależnienie innej osoby od siebie, poleca jej wykonanie takiego czynu.”. Możemy podsumować, że sprawcą jest osoba, która popełnia czyn zabroniony lub też ten kto kieruję taką osobą.

Spojrzenie kryminalistyczne

Aby dobrze zdefiniować ofiarę czy przestępcę, należałoby najpierw określić czym dokładnie jest przestępstwo komputerowe. Wdług. rozprawy (8) M. Sowy przestępstwo takie możemy podzielić na 4 grupy :

- propagowania zakazanych treści
- naruszania praw autorskich
- działalności hakerów (przestępstw hakerskich)
- przestępstw przeciwko mieniu

Pierwsza grupa to zachowania związane z propagowaniem treści zakazanych, druga obejmuje naruszenia praw autorskich oraz nieuprawnione kopiowanie programów komputerowych. Trzecia grupa to działania bezpośrednio związane z wykorzystaniem komputerów do manipulacji i dostępu do danych, takie jak niszczenie danych, podsłuch komputerowy

czy oszustwo komputerowe. Czwarta grupa to przestępstwa komputerowe które wykorzystują komputery do popełnienia tradycyjnych przestępstw przeciwko mieniu, takich jak działalność nierzetelnych sklepów internetowych.
Jeśli chodzi o odpowiedzialność, to obejmuje ona autora treści umieszczonych w Internecie, a także osobę, która decyduje się na publikację tych treści na swojej stronie internetowej i jednocześnie wyraża zgodę na ich treść. Jednakże, przypomnienie czyjegoś tekstu w celu podjęcia polemiki nie podlega karze. Zatem sprawcą wykonawczym jest użytkownik końcowy, który popełnia czyn nielegalny poprzez sieć. Natomiast osoba, która jedynie zapoznała się z nielegalnymi treściami zamieszczonymi przez inne osoby, nie jest uważana za sprawcę wykonawczego.(9)
Z uwagi na to, że cyberprzestępczość jest bardzo rozległa, trudno jednoznacznie wskazać ofiarę. Z najnowszego raportu Centralnego Biura Zwalczania Cyberprzestępczości, biorąc pod uwagę tylko czynności życia i zdrowia ludzkiego, prawie 70% ofiar to były dzieci. Raport Symantec Corporation z 2019r. zwraca uwagę na rosnący procent ataków na strony internetowe polegający głównie na kradzieży informacji bankowych (10). Wzrost o ponad 50% w porównaniu do roku poprzedniego. Inny raport z 2022r. podaje, że ponad połowa użytkowników doświadczyła cyberprzestępstwa z czego 37% z nich w ciągu ostatniego roku(11). Ofiarą może stać się każdy, niezależnie od wieku, urządzenia czy płci.

Spojrzenie społeczne

W swojej publikacji (12), Jerzy Kosiński przedstawia pentagonalny model bezpieczeństwa, obejmujący następujące obszary: militarny, polityczny, gospodarczy, ekonomiczny i społeczny. Należy zatem spojrzeć na cyberprzestępstwo także jako na naruszenie (cyber)bezpieczeństwa w zakresie piątego sektora niniejszego modelu.
Jednymi z głównych celów cyberprzestępców są osoby o ubogiej wiedzy dotyczącej funkcjonowania w wirtualnym świecie - osoby starsze oraz dzieci. Przestępcy wykorzystują swoją technologiczną przewagę, a ich ofiary darzą ich nadmiernym zaufaniem lub boją się przeciwstawić ich działaniu (13).
Zachowania, które można nazwać cyberprzestępstwami zachodzące pomiędzy dziećmi i nastolatkami zasługują na szersze omówienie w kontekście tej pracy. Mogłoby się wydawać, że trudno mówić o przestępczości, kiedy dwoje dziewięciolatków wysyła niemiłe SMSy koleżance z klasy. Nic bardziej mylnego - odmianami cyberprzemocy, która jak przedstawiono w poprzednich akapitach jest karalna są takie zachowania jak: *hejt* (działanie w sieci przejawiające agresję, złość i nienawiść), *trolling* (osobiste prowokowanie uczestników dyskusji w sieci) czy *cyberstalking* (wykorzystywanie technologii do nękania) czyli formy tzw. *cyberbullyingu* (14). Zostanie ofiarą takich praktyk często wiąże się dla młodej osoby z poczuciem wykluczenia, braku przynależności do grupy i akceptacji. Dziecko izoluje się, jego poczucie własnej wartości się obniża, pojawiają się także objawy somatyczne związane ze stresem (bóle brzucha, bezsenność) a w wielu przypadkach także myśli samobójcze (15). Niestety, cyberprzemoc w szkole jest bardzo popularnym zjawiskiem - doświadczyło jej w stosunku do siebie lub swoich znajomych niemal 80% młodzieży.

Kim w tym kontekście jest ofiara, a kim sprawca przestępstwa? Zwykle, chociaż nie zawsze, ofiarami stają się dzieci, które osiągają gorsze wyniki w nauce, pochodzą z biedniejszych rodzin lub są bardziej zamknięte w sobie. Młodzi cyberprzestępcy wykorzystują ich słabości, działają pod wpływem zazdrości lub agresji. Chcą poczuć się lepiej i udowodnić rówieśnikom swoją wyższość. Często są to młode osoby z zaburzeniami emocjonalnymi, nieumiejące poradzić sobie z własnymi problemami lub wyrządzonymi im krzywdami. W tej sytuacji niezwykle istotne jest, aby środowisko, czyli głównie szkoły reagowały jak najszybciej na wszelkie formy cyberprzemocy, ponieważ pozostawienie takich zachowań bez konsekwencji może mieć ogromny wpływ na młodzież.

Nieco inaczej sytuacja wygląda w drugiej grupie - osób mniej zaawansowanych technologicznie, narażonych na nadużycia. Padają one najczęściej ofiarami wyłudzeń danych lub majątkowych. Z badania przeprowadzonego na zlecenie Biura Informacji Kredytowej wynika, że co trzeci polak padł ofiarą wyłudzenia pieniędzy, a 38% rodaków spotkało się z podszywaniem się fałszywych firm pod rzeczywiste instytucje (16). Aż 87% Polaków odczuwa niepokój związany z możliwością utraty kontroli nad swoimi danymi osobistymi. Zagrożenie jest jak najbardziej realne - wiele dziedzin życia społecznego przeniosło się do świata wirtualnego, na co znaczący wpływ miała pandemia COVID-19. Według raportu CBOS z 2022 roku, na skutek pandemii odsetek internautów wzrósł aż o 9 punktów procentowych (17). 84% respondentów dokonało w życiu chociaż jednego zakupu przez Internet, a 80% regularnie rozmawia ze swoimi bliskimi za pośrednictwem komunikatorów.

Wraz z szybkim rozwojem metod handlu czy komunikacji *online* rozwijają się także nowe sposoby na wykorzystanie zaufania czy nieuwagi internautów. Ofiarą tego rodzaju cyberprzestępstwa może stać się każdy. Nawet osoby obeznane z technologią mogą zadziałać pod wpływem emocji i utracić środki finansowe. Co wynika z badania przeprowadzonego przez Kaspersky Lab, ponad połowa osób, które padły ofiarami wyłudzenia pieniędzy nie odzyskała lub odzyskała tylko częściowo swoje środki (18). Może to wzbudzać niechęć do dalszych zakupów za pośrednictwem stron internetowych, wpłynąć negatywnie na jakość życia, a w skrajnym przypadku doprowadzić do utraty wszystkich oszczędności i ubóstwa. Sprawcy takich przestępstw to z reguły zorganizowane grupy, czasami działające także poza krajem. Wykorzystują jednostki jako tzw. słupy lub funkcjonują pod pretekstem call center aby wzbudzić zaufanie swoich ofiar (19). Działają świadomie, z premedytacją i nastawieniem na zysk. Niezbędnym zatem jest, aby organy bezpieczeństwa zdawały sobie sprawę ze skali zagrożeń i ich wpływu na funkcjonowanie Polaków nie tylko w cyberprzetrzeni, a także społeczeństwie.

Cyberprzestępstwo a inne przestępstwa

Spojrzenie prawne, społeczne oraz kryminalistyczne na problematykę pojęcia ofiary oraz sprawcy nie wyczerpują w pełni zagadnień związanych z cyberprzestępczością. Potrzebny jest jeszcze dodatkowy element czyli relacja łącząca te dwa podmioty jakim jest fakt dokonania cyberprzestępstwa. W tym rozdziale postaramy się nieco bliżej przyjrzeć się definicji cyberprzestępstwa pod kątem cech wyróżniających go na tle innych rodzajów naruszeń prawa.

Komisja Wspólnot Europejskich pod pojęciem cyberprzestępstwa (*ang. cybercrime*) rozumie "czyny przestępcze dokonane przy użyciu sieci łączności elektronicznej i systemów informatycznych lub skierowane przeciwko takim sieciom i systemom" (20). Powyższa definicja cyberprzestępstwa dosyć sugestywnie wskazuje na obszar będący typową i unikalną dla tego rodzaju naruszeń prawa domeną – sieci komputerowych. Cyberprzestępstwo łączy zatem pojęcie tradycyjnego przestępstwa ze światem cyfrowym, osadzając definicję tego rodzaju naruszeń w trzech obszarach:

- Oszustwo i fałszerstwo z wykorzystaniem sieci
- Publikacja nielegalnych treści w mediach
- Ataki przeciwko systemom teleinformatycznym

Po wtóre, powyższa definicja, która eksponuje pojęcie systemów komputerowych sugeruje, iż w związku z dużym poziomem skomplikowania ich budowy, trudne może okazać się określenie i porównanie skutków cyberprzestępstw(21) dla przeciętnego użytkownika internetu. Niska świadomość trudnych zagadnień technicznych z tego obszaru została podkreślona również w obszarze praktyki orzeczniczej polskich sądów, która wyszła przy okazji dyskusji medialnej nad zastosowaniem systemu Pegasus, czyli oprogramowania szpiegowskiego pozwalającego podsłuchiwać rozmowy oraz wiadomości tekstowe telefonów ofiar. Sędzia Igor Tuelya nakreślił ten problem w wywiadzie z Rzeczpospolitą (22).

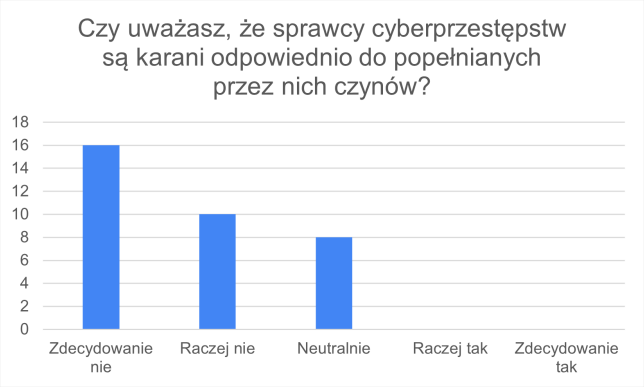
Po trzecie, to samo czasopismo "Rzeczpospolita" w artykule opublikowanym w (23) wskazuje na niezwykle trudny problem ustalenia danych sprawcy ewentualnego przestępstwa w sieciach teleinformatycznych, co również wyróżnia ten rodzaj przestępstw na tle pozostałych. Z uwagi na zastosowanie zaawansowanych technik komputerowych w kryminalistyce np. monitoringu wizyjnego udaje się zwiększyć stosunek tradycyjnych przestępstw wykrytych do stwierdzonych co potwierdzają policyjne statystyki dostępne w (24). Wydaje się, że odwrotny trend panuje w przypadku właśnie cyberprzestępstw gdzie rozwój technologi wpływa na coraz bardziej zaawansowane metody kamuflażu sprawcy, unikania odpowiedzialności za swoje czyny, a co za tym idzie, również trudności w udowodnieniu zarzucanych przestępstw.

Końcowym przykładem w tej sekcji będzie bardzo szybki wzrost przepisów prawnych obejmujących swym zakresem problematykę cyberprzestępczości. O ile tradycyjne rodzaje przestępstw nie wykazują zbytniej konieczności modyfikacji czy rozbudowywania prawa, o tyle sfera kodyfikacji zagrożeń w cyberprzestrzeni cechuje się dynamicznym wzrostem, także na poziomie europejskim gdzie instytucje unijne wydają dyrektywy państwom członkowskim, które zobligowane są do ich implementacji we wskazanych obszarach. Przykładem dyrektywy unijnej odnoszącej się do cyberbezpieczeństwa jest dyrektywa NIS2 (25), która nakłada na przedsiębiorstwa sektorów usług kluczowych zobowiązania do podjęcia odpowiednich środków bezpieczeństwa i powiadamiania organów krajowych o poważnych incydentach. Świadczy to o powszechnej konieczności edukacji w zakresie cyberbezpieczeństwa oraz monitorowania zmian prawnych w tej domenie, co z pewnością wyróżnia ten obszar na tle innych rodzajów prawa.

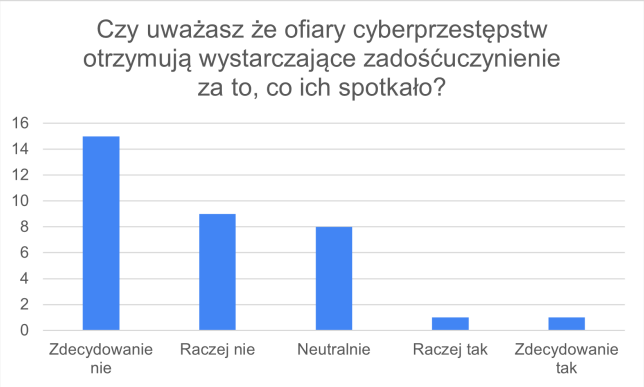
Doświadczenia związane z cyberprzestępczością - badanie

W celu sprawdzenia jak postrzegane są cyberprzestępstwa przez młode osoby postanowiliśmy przeprowadzić krótkie badanie w formie ankiety. Wzięły w nim udział 34 osoby z naszego bezpośredniego otoczenia - młodzi dorośli na etapie studiów lub na początku kariery zawodowej, którzy od wczesnego dzieciństwa mają styczność z cyfryzacją w ich życiu. Według odpowiedzi, 58,8% z nich zostało kiedyś ofiarą cyberprzestępstwa, a dla 25% wiązało się to z utratą środków finansowych.

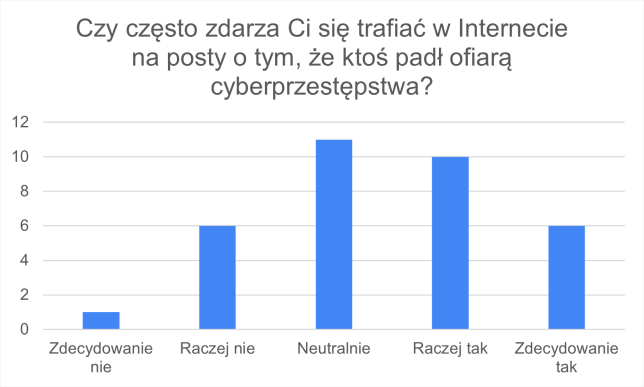
Zapytaliśmy ich także o postrzeganie samych cyberprzestępców i ich ofiar, a dokładniej stosunku wymierzonych kar i przyznanych zadośćuczynień do popełnionych przestępstw. Aż 76,5% ankietowanych uważa, że sprawcy nie są wystarczająco karani. Co więcej, żaden ankietowany nie wskazał odpowiedzi „Tak” ani „Zdecydowanie tak”.



Podobnie rozkładały się odpowiedzi w przypadku kolejnego pytania - 70,6% badanych uważa, że ofiary cyberprzestępstw nie otrzymują odpowiednich odszkodowań za to, co je spotkało. Prawie połowa ankietowanych odpowiedziała „Zdecydowanie nie”.



Ostatnim poruszonym problemem była popularność wiadomości o cyberprzestępstwach w przestrzeni internetowej. 47% badanych przyznało, że często spotyka się z informacjami o tego typu działalności w cyberprzestrzeni.



Wyniki badań pokazują, że nawet ludzie wychowani w erze Internetu mogą spotkać się z cyberprzestępczością w każdej formie. Dla jednych z nich będą to wyzwiska w komentarzach pod zdjęciem na portalu społecznościowym, drudzy stracą pieniądze na fałszywej ofercie w serwisie aukcyjnym. Cyberprzestępczość jest obecna wśród nas, a jej sprawcy nie ponoszą odpowiednich konsekwencji.

Podsumowanie

Tematyka sprawcy i ofiary przestępstwa w internecie do tej pory wydawała się dosyć oczywista ponieważ w tradycyjnym rozumieniu tych pojęć bardzo wyraziście rysuje się podział na winnego oraz poszkodowanego w wyniku określonego przestępstwa. Ta praca przyniosła nam zupełnie nową perspektywę dzięki wieloaspektowemu przyjrzeniu się temu problemowi oraz analizie porównawczej cyberprzestępstw z tradycyjnymi przestępstwami.

W naszej pracy staraliśmy się opierać na artykułach oraz literaturze przytaczającej opinie ekspertów przedmiotu badania, a dla potwierdzenia wniosków przeprowadziliśmy również samodzielnie ankietę na temat zagrożeń cyberprzestępczości w naszym najbliższym otoczeniu.

Bibliografia

1. PWN. Słownik języka polskiego, 1996.
2. Zintegrowana platforma edukacyjna. Bezpieczeństwo narodowe.
3. Janusz Gierszewski. Bezpieczeństwo społeczne jako dziedzina bezpieczeństwa narodowego. *Historia i Polityka*, 23(30):21–38, 2018. ISSN 1899-5160. doi: http://dx.doi.org/10.12775/HiP.2018.002.
4. ComCERT. Cyberprzestępca. kim jest i jaki jest cel jego działań?, 2023.
5. Tomasz Lipczyński. Każdy może paść ofiarą cyberprzestępców. oto najczęstsze formy ataków, 2023.
6. Janusz Wasilewski. Cyberprzestępczość – wybrane aspekty prawnokarne oraz kryminalistyczne, Jan 2018.
7. Polska karta praw ofiary, Oct 1999.
8. Michał Sowa. PrzestĘpczoŚĆ komputerowa – - badanie celowoŚci i skutecznoŚci kryminalizacji, 2005.
9. Iga A. Jaroszewska. Wybrane aspekty przestępczości w cyberprzestrzeni. 2017.
10. Internet security threat report, Feb 2019.
11. 2022 cyber safety insights report, 2022.
12. Jerzy Kosiński. Paradygmaty cyberprzestępczości, 2015.
13. Raj Sinha and Niraj Vedpuria. Social impact of cyber crime: A sociological analysis. 2018. doi: 10.13140/RG.2.2.20922.93126.
14. Aleksander Zawadzki Katarzyna Król. Zjawisko cyberprzemocy w kontekście bezpieczeństwa dzieci w sieci. *Edukacja. Terapia. Opieka – Tom 02. Teoretyczne aspekty i praktyczne konteksty przemocy w różnych środowiskach społecznych*, pages 179–197, 2019. ISSN 2658-0071.
15. Anna Borkowska. Cyberprzemoc w szkole - poradnik dla nauczycieli. 2021.
16. Forsal. Co trzeci polak doświadczył zagrożeń związanych z cyberprzestępczością [badanie].
17. Centrum Badania Opinii Społecznej. Korzystanie z internetu w 2022 roku. *Komunikat z badań*, 2022. ISSN 2353-5822.
18. Interia biznes. Ofiary cyberprzestępczości finansowej mają problemy z odzyskaniem wszystkich utraconych środków.
19. Regina Skibińska. Plaga cyberprzestepstw. trudna droga do ustalenia sprawcy, 2021.
20. Maciej Siwicki. Podział i definicja cyberprzestępstw.
21. Dave Russell. Cyberprzestępstwo jest przestępstwem jak każde inne. https://www.rp.pl/prawo-karne/art19113041-cyberprzestepczosc-trudno-ustalic-dane-sprawcy-w-sieci, 2021.
22. Rzeczpospolita. Sędzia igor tuleya: Możliwe, że zgodziłem się na pegasusa. https://www.rp.pl/sady-i-trybunaly/art39874451-sedzia-igor-tuleya-mozliwe-ze-zgodzilem-sie-na-pegasusa, 2024.
23. Rzeczpospolita. Cyberprzestępczość: trudno ustalić dane sprawcy w sieci. https://www.rp.pl/prawo-karne/art19113041-cyberprzestepczosc-trudno-ustalic-dane-sprawcy-w-sieci, 2021.
24. statystyki.policja.pl. Statystyki policyjne. https://statystyka.policja.pl/st/przestepstwa-ogolem/przestepstwa-kryminalne/7-wybranych-kategorii-p/122289,Przestepstwa-z-7-wybranych-kategorii.html, 2021.
25. EUR-Lex. Dyrektywa nis2. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX