DARIA ZARZYCKA
Magister prawa
Uniwersytet Warmińsko-Mazurski w Olsztynie
ORCID: 0000-0002-1408-0326
e-mail: dar.zarzycka@wp.pl
DOI: 10.5281/zenodo.20347880

# PRZESTĘPSTWA W CYBERPRZESTRZENI NA PRZYKŁADZIE WŁAMAŃ NA KONTA SPOŁECZNOŚCIOWE W INTERNECIE ORAZ PROBLEMY PRZY WYKRYWANIU SPRAWCÓW TYCH CZYNÓW

Cybercrimes, as exemplified by hacking into social media accounts on the Internet, and the problems with detecting the perpetrators of these acts

**Abstrakt**

Dynamiczny rozwój mediów społecznościowych, stworzył wiele możliwości, ale jednocześnie przyczynił się do wzrostu cyberprzestępczości. Jednym z najczęściej występujących zjawisk, są włamania na konta na portalach społecznościowych. Skutki takich włamań są wielowymiarowe i obejmują zarówno straty materialne czy utratę danych, ale też konsekwencje psychologiczne, polegające chociażby na strachu przed aktywnością w Internecie, jak i społeczne, które mogą być związane z utratą reputacji i zaufania — zarówno w życiu prywatnym, jak i zawodowym. Czyny te są penalizowane przez Kodeks karny, dzięki czemu możliwe jest ich egzekwowanie, jednak nie zawsze służby dysponują odpowiednimi środkami i metodami wykrywczymi. W nieniniejszym artykule, autorka skupia się na tym, jakie przestępstwa są najczęściej popełniane w związku z włamaniami na konta społecznościowe, a także omawia sprawy, które podlegały orzecznictwu polskich sądów po to, by wysnuć wnioski w jakich sprawach postępowania doprowadziły do skutecznego wykrycia sprawcy, w jakich zaś nie, a następnie wskazuje na konieczność usprawnienia metod wykrywania sprawców cyberprzestępstw.

**Słowa klucze:** prawo karne, cyberprzestępczość, zniesławienie, znieważenie, włamanie na konto, media społecznościowe

**Abstract**

The dynamic development of social media has created numerous opportunities, but it has also contributed to the rise in cybercrime. One of the most common phenomena is the hacking of social media accounts. The consequences of such hacks are multifaceted and include both material losses and data loss, as well as psychological consequences, such as fear of online activity, and social consequences, which can be associated with a loss of reputation and trust— both in private and professional life. These acts are penalized by the Penal Code, making them enforceable, but law enforcement agencies do not always have the appropriate means and methods of detection. In this article, the author focuses on the crimes most frequently committed in connection with social media hacking. Author also discusses cases that have been subject to

Polish court rulings to draw conclusions in which proceedings led to the successful detection of the perpetrator and in which cases the perpetrator was not and then points to the need to improve methods for detecting cybercrime perpetrators.

**Keywords:** criminal law, cybercrime, defamation, insult, account hacking, social media

## 1. Wprowadzenie

Dynamiczny rozwój technologii informacyjnych spowodował upowszechnienie dostępu do Internetu. Zgodnie z danymi Głównego Urzędu Statystycznego, w 2024 roku w Polsce, dostęp do Internetu miało niemal 96% gospodarstw domowych[1], co potwierdza fakt, że większość społeczeństwa aktywnie z niego korzysta. Powszechny dostęp do sieci niesie za sobą zarówno wielość pozytywów, jak i zagrożeń dla jego użytkowników[2]. Współczesna cyberprzestrzeń daje możliwość pozostawania w nieustannym kontakcie z bliskimi, dokonania zakupu interesujących nas przedmiotów online, załatwiania spraw urzędowych czy niemalże natychmiastowego zdobycia interesujących nas informacji — przykładowo popularnonaukowych czy edukacyjnych, jednak pomimo wymienionych korzyści, stała się również miejscem popełniania przestępstw.

Cyberprzestępczość stanowi jedno z głównych wyzwań świata cyfrowego, a wbrew temu co może się pierwotnie wydawać — nie dotyczy ona wyłącznie prawa karnego, a wykracza znacznie poza jego ramy. Analiza tego zjawiska, jak i próba jego zwalczania, wymaga podejścia interdyscyplinarnego, łączącego informatykę, kryminologię, prawo, socjologię, psychologię[3] czy nauki o bezpieczeństwie, bowiem jest to specyficzny rodzaj przestępstw, popełnianych w świecie wirtualnym, jednak wyrządzających szkodę w świecie rzeczywistym, gdzie sprawcy kierują się różnego rodzaju pobudkami.

Z perspektywy informatycznej, konieczne jest odpowiednie zabezpieczenie systemów przed nieuprawnionym dostępem, jak i opracowanie metod wykrywania sprawców tych czynów. Prawo zaś musi odpowiednio reagować na działania przestępcze i jednocześnie chronić społeczeństwo przed ich skutkami, jak i karać sprawców. Kryminologia pozwala zrozumieć mechanizmy postępowania sprawców, a psychologia i socjologia podatność społeczeństwa na te mechanizmy.

Wśród cybeprzestępstw, istotne miejsce zajmują czyny polegające na nieuprawnionym dostępie do kont w mediach społecznościowych, które prowadzą nie tylko do naruszenia prywatności, ale często również dóbr osobistych czy nawet bezpieczeństwa ofiar. W ocenie autorki niniejszej publikacji, cyberprzestępczość stanowi obecnie jedno z największych wyzwań dla prawa karnego.

Włamania na konta na portalach społecznościowych mają różne podłoże. Czasem jest to chęć wyłudzenia pieniędzy, innym razem forma zemsty czy próby ośmieszenia ofiary ze

[1] Społeczeństwo informacyjne w Polsce w 2024 roku: https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2024-roku,2,14.html (dostęp online z dnia 16 października 2025 roku).
[2] A. Wiatrowska, *(Nie)Bezpieczne korzystanie z Internetu przez młodych dorosłych — raport z badań,* „Annales Universitatis Mariae Curie-Skłodowska Lublin-Polonia" vol. XXXVII, 2024, nr 4, s. 66.
[3] P. Zegarow, *Analiza. Psychologiczne aspekty cyberbezpieczeństwa, „*NASK Cyberpolicy" 2019, s. 1.

strony włamywacza. Oczywiście są to tylko przykłady, gdyż przesłanek kierujących sprawcami jest znacznie więcej. Z uwagi na to, że czyny te mają miejsce w cyberprzestrzeni, ich sprawcy często czują się bezkarni. Jednak pozostają w błędzie, bowiem ustawodawca stypizował przestępstwa, które popełnione mogą być również w cyberprzestrzeni i są to między innymi podszywanie się pod inną osobę, bezpodstawne uzyskanie informacji, zniesławienie czy znieważenie, będące uregulowane w Kodeksie karnym[4]. Wskazać jednak należy, że samo stypizowanie wskazywanych czynów w ustawie karnej, nie jest jednoznaczne z poniesieniem przez sprawcę odpowiedzialności. Ogromną rolę w doprowadzeniu do ukarania za wymienione czyny (oraz inne, możliwe do popełnienia w cyberprzestrzeni), odgrywają organy ścigania, tj. Policja czy Prokuratura.

Celem niniejszego artykułu jest analiza wybranych aspektów prawnokarnych włamań na konta na portalach społecznościowych – ze szczególnym uwzględnieniem rodzaju i sposobu popełnienia czynu, a także problemów związanych z ustaleniem tożsamości sprawcy, aż po analizę orzeczeń sądów polskich. Celem dokonania wskazanej analizy autorka odniesie się do tekstów ustaw, opracowań doktryny oraz orzecznictwa. Niniejsze opracowanie nie jest badaniem empirycznym, a ma charakter dogmatyczno-prawny z analizą orzecznictwa, ma ono natomiast przedstawić rodzaje przestępstw popełnianych w cyberprzestrzeni oraz ukazać przykłady takich czynów wraz ze sposobem działania sprawcy, a także odnieść się do problemów związanych z wykrywaniem sprawców cyberprzestępstw.

## 2. Przestępczość w cyberprzestrzeni — definicje i problematyka

Jak wskazywano we wstępie, przestrzeń wirtualna nie jest wolna od przestępczości, a wręcz przeciwnie — kształtuje się tam przestępczość wirtualna, zwana cyberprzestępczością. Na początku, rozważyć należy pojęcie przestępczości oraz cyberprzestrzeni, bowiem stanowią one podstawę rozważań będących przedmiotem niniejszego artykułu. Przestępczość w szerokim znaczeniu tego pojęcia, definiuje się jako zbiór zdarzeń, które można określić przestępstwami[5]. Pojęcie przestępstwa zaś definiowane jest jako czyn zabroniony przez ustawę w chwili jego popełnienia, zawiniony oraz szkodliwy społecznie w stopniu wyższym niż znikomy[6]. Wobec powyższego, przestępstwami będą wszelkie czyny spełniające te warunki, przestępczością zaś ogół tych czynów.

Cyberprzestrzeń zaś jest swego rodzaju światem wirtualnym, który opiera się zarówno na systemach teleinformatycznych, jak i relacjach tworzonych przez osoby z tych systemów korzystające. Człowiek może niejako wstąpić do tego świata za pośrednictwem odpowiedniego urządzenia — np. smartfona, tabletu czy komputera[7]. Niemalże całe życie aktualnego społeczeństwa w pewien sposób przenosi się do przestrzeni wirtualnej, a w konsekwencji, pojawia się w niej przestępczość internetowa, która z uwagi na miejsce występowania, określana jest mianem cybeprzestępczości. Wskazać tutaj należy, że cyberzestępczość pomimo

[4] Ustawa z dnia 6 czerwca 1997 roku Kodeks karny (t.j. Dz. U. z 2025 r., poz. 383), dalej: k.k.
[5] A. Lisowska-Kierepka, *Przestępczość jako zjawisko geograficzne? Przegląd badań nad zjawiskiem w świetle wybranych nauk*, „Przegląd Geograficzny" 2020, nr 92, s. 268.
[6] M. Niemiec, *Przestępstwo wypadku drogowego i zasady odpowiedzialności karnej; postępowanie przygotowawcze w sprawie wypadku* [w:] *Przestępstwo wypadku drogowego w pytaniach i odpowiedziach,* M. Niemiec, Warszawa 2019, LEX/el.
[7] B. Kałdon, *Cyberprzestrzeń jako zagrożenie dla człowieka XXI wieku,* „Seminare. Poszukiwania naukowe." 2016, t. 37, nr 2, s. 88.

tego, że jest znacznym problemem w aktualnym stanie prawnym, wciąż nie posiada definicji legalnej w polskim ustawodawstwie, wobec czego definiowanie tego pojęcia oparte jest na wywodach doktryny. Przykładowo M. Stefanowicz wskazuje, iż będzie to ogół czynów skierowanych przeciwko systemom informatycznym, które polegać mogą zarówno na skierowaniu zamachu przeciwko konkretnemu komputerowi (tj. będzie on celem), jak i czyny przy użyciu komputera (tj. będzie on narzędziem)[8]. W niniejszym opracowaniu, cyberprzestępczość rozumiana będzie przede wszystkim w drugim znaczeniu, kiedy to komputer będzie służył jako narzędzie czynu zabronionego.

Na cyberprzestępczość składają się czyny niedozwolone popełnione za pośrednictwem sieci teleinformatycznych, przyjąć więc należy, że cyberprzestępczość, to ogół czynów zabronionych popełnianych z wykorzystaniem systemów komputerowych czy sieci teleinformatycznych[9], a więc cyberprzestępstw kierowanych przeciwko różnego rodzaju dobrom chronionym przez prawo karne[10]. Wskazać należy, że mogą być to zarówno przestępstwa, których dokonanie jest możliwe i w świecie realnym, i w świecie wirtualnym, jak i wyspecjalizowane typy przestępstw, które dokonywane są wyłącznie w cyberprzestrzeni[11]. Wobec powyższego, Kodeks karny nie posługuje się w żadnym przepisie pojęciem „cyberprzestępstwo", a po prostu przestępstwo. Do wybranych przestępstw dokonywanych w cyberprzestrzeni autorka odniesie się w dalszej części niniejszego opracowania.

Podkreślić należy, że problematyka związana z cyberprzestępczością ma charakter nasilający się. Potwierdza to chociażby porównanie statystyk za lata 2023-2024 Centralnego Biura Zwalczania Cyberprzestępczości, będącego jednostką organizacyjną Policji, zajmującą się zwalczaniem cyberprzestępczości[12], zgodnie z którymi w 2023 roku prowadzonych było przez tę jednostkę 317 postępowań przygotowawczych[13], natomiast w 2024 roku były to już 1253 postępowania[14]. Dane te świadczą po pierwsze o znacznej ilości przestępstw dokonywanych w cyberprzestrzeni, po drugie natomiast — o rosnącej świadomości społecznej odnośnie konieczności zgłaszania tego typu czynów zabronionych organom ścigania. Zaznaczyć jednak należy, że wskazywana statystyka obejmuje ilość postępowań prowadzonych w danym roku, nie zaś zakończonych wykryciem sprawcy. Autorka zaznacza tę zależność, bowiem z uwagi na miejsce występowania omawianej przestępczości oraz możliwości ukrywania śladów swojej działalności przez sprawców, ich wykrycie niejednokrotnie stwarza znaczne problemy.

[8] M. Stefanowicz, *Cyberprzestępczość — próba diagnozy zjawiska, „*Kwartalnik Policyjny" 2017, nr 4, s. 20.
[9] D. S. Wall, *Cybercrime: The Transformation of Crime in the Information Age,* 2017, s. 14.
[10] W. Filipkowski, *Cyberprzestępstwo o charakterze terrorystycznym w polskim prawie karnym „*Prawo w Działaniu. Sprawy Karne" 2023, nr 55, s. 77.
[11] N. Urbańska *Cyberprzestępczość i wynikające z niej zagrożenia,* „Cybersecurity & Cybercrime" vol. 1, 2025, nr 7, s. 63.
[12] Zadania Centralnego Biura Zwalczania Cyberprzestępczości: https://cbzc.policja.gov.pl/bzc/o-cbzc/podstawowe-zadania/5,Zadania-Centralnego-Biura-Zwalczania-Cyberprzestepczosci.html (dostęp: 16.10.2025 r.).
[13] Wyniki statystyczne Centralnego Biura Zwalczania Cyberprzestępczości https://cbzc.policja.gov.pl/bzc/statystyka/raporty-z-dzialalnosci/262,Raporty-z-dzialalnosci.html (dostęp: 16.10.2025 r.).
[14] *Ibidem*.

### 3. Włamania na konta na portalach społecznościowych w ujęciu prawnokarnym

Mając już pewien zarys tego, czym są cyberprzestępczość i cyberprzestępstwa, wypada zawęzić tematykę do czynów wskazywanych w tytule niniejszej publikacji, a mianowicie do włamań na konta na portalach społecznościowych, które stanowią jedną z najczęstszych form cyberprzestępczości. Czyny te mogą wyczerpywać znamiona kilku przestępstw określonych w kodeksie karnym, o czym w dalszej części.

W tym miejscu wskazać również wypada, co należy rozumieć pod pojęciem włamań na konta na portale społecznościowe, bowiem pojęcie to jest dość szerokie. Jako włamanie rozumieć należy zarówno dostanie się na cudze konto poprzez przełamanie zabezpieczeń do kont na portalach społecznościowych, tj. np. złamanie hasła, jak również sam nieuprawniony dostęp do takiego konta bez przełamywania zabezpieczeń, tj. dostęp wbrew woli właściciela danego konta, który może zaistnieć np. poprzez korzystanie z czyjegoś konta z uwagi na niewylogowanie się przez użytkownika czy też z uwagi na znajomość jego haseł[15].

Konta na portalach społecznościowych w Polsce posiada ponad 28 mln osób[16], co stanowi ponad 70% całej populacji. Większość z użytkowników mediów społecznościowych stanowią kobiety[17]. Liczba ta potwierdza fakt, iż życie wielu osób ma swoje centrum w świecie wirtualnym. Co więcej, znaczna część z nich, udostępnia wiele szczegółów ze swojego życia na mediach społecznościowych, upublicznia swoje zdjęcia itp. Nieustanny wzrost liczby użytkowników mediów społecznościowych, generuje jednak zwiększenie ryzyka włamań na konta na tych portalach. Dzieje się tak, dlatego że za pośrednictwem wskazanych kont, stosunkowo łatwo jest dokonać przestępstw polegających przykładowo na wyłudzeniu pieniędzy od znajomych ofiary, zniesławieniu czy znieważeniu danej osoby. Sprawcy wykorzystują media społecznościowe w swoich własnych celach, często myśląc, że są bezkarni z uwagi na anonimowość, którą zapewnia im internet.

Rozważania prawnokarne należy rozpocząć od samego uzyskania dostępu do cudzego konta na portalu społecznościowym, które penalizowane jest przez art. 267 k.k., tj. bezprawne uzyskanie informacji. Przedmiotem ochrony wskazywanego czynu zabronionego jest poufność informacji i możliwość dysponowania informacją z wyłączeniem innych osób[18], ale też prywatność osób, których te informacje dotyczą[19]. Zgodnie ze stanowiskiem Sądu Najwyższego, istotą wskazywanego występku jest uzyskanie przez sprawcę informacji dyskrecjonalnej, która nie jest dla niego przeznaczona[20]. W świetle omawianej tematyki, odnieść należy się przede wszystkim do fragmentu *kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej (...) przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie,* co odniesienie będzie

[15] Zob. Wyrok SO w Piotrkowie Trybunalskim z 20 maja 2025 r., sygn. akt IV Ka 246/25, LEX nr 3927770.
[16] Social media w Polsce w 2024 r. Kluczowe trendy i dane dla marketingu międzynarodowego: https://lemon-media.pl/social-media-w-polsce-w-2024-r-kluczowe-trendy-i-dane-dla-marketingu-miedzynarodowego (dostęp: 20.10.2025 r.).
[17] A. Chmielewska, M. Kondrat, *Popularność mediów społecznościowych w Polsce — analiza według płci* „Kobieta i Biznes/Women and Business" 2023, s. 17.
[18] P. Kozłowska-Kalisz [w:] *Kodeks karny. Komentarz aktualizowany*, red. M. Mozgawa, Warszawa 2026, art. 267, teza nr 1, LEX/el.
[19] K. Lipiński [w:] *Kodeks karny. Część szczególna. Komentarz,* red. J. Giezek, Warszawa 2021, art. 267, teza nr 3, LEX/el.
[20] Zob. Uchwała Sądu Najwyższego z 22 stycznia 2003 r., sygn. akt I KZP 43/02, OSNKW 2003, nr 1-2, poz. 5.

miało do uzyskania nieuprawnionego dostępu do cudzego konta na portalu społecznościowym. Wskazać również należy czym będzie się różniło rzeczone przełamanie zabezpieczeń od ich ominięcia. I tak przełamaniem zabezpieczeń może być włamanie się na konto społecznościowe poprzez atak siłowy, tzn. wpisywanie wielu kombinacji haseł, aż do uzyskania skutku w postaci odgadnięcia hasła i uzyskania dostępu do cudzego konta społecznościowego[21]. Ominięcie zabezpieczeń zaś polega na uzyskaniu dostępu do wskazanych kont bez konieczności przełamywania zabezpieczeń, wykorzystując przykładowo niezabezpieczony port, ale również fizyczny dostęp do urządzenia, na którym zalogowany jest użytkownik i przejęcie jego konta społecznościowego[22]. Konta na portalach społecznościowych, zabezpieczone są hasłami, co samo przez się wskazuje, że właściciel konta nie chce, aby osoby postronne miały do niego dostęp. Wobec powyższego, dokonując przełamania zabezpieczeń bądź ich ominięcia i uzyskując dostęp do cudzego konta, z pewnością sprawcy uzyskują również dostęp do informacji dla nich nieprzeznaczonych, a tym samym wypełnieją znamiona wskazywanego czynu. Problematyczne przy postępowaniach karnych dotyczących czynów wyczerpujących znamiona z art. 267 k.k., bywa jednak ustalenie sprawcy, bowiem często korzystają oni z różnego rodzaju oprogramowań szyfrujących rzeczywiste IP, co utrudnia ustalenie ich tożsamości, o czym w dalszej części niniejszej pracy.

Bezpośrednio związanym z nieuprawnionym dostępem do konta na portalu społecznościowym jest czyn uregulowany w art. 190a § 2 k.k., polegający na podszywaniu się pod inną osobę, wykorzystanie jej wizerunku, jej danych osobowych, bądź innych danych, za pośrednictwem, których osoba ta jest identyfikowana, a tym samym wyrządzenie tej osobie szkody majątkowej bądź osobistej. Wskazać w tym miejscu należy, że nie jest konieczne jednoczesne wystąpienie wykorzystania wizerunku osoby i jej danych osobowych, aby doszło do podszycia się, bowiem w omawianym przepisie zachodzi alternatywa rozłączna[23]. Przedmiotem ochrony jest tutaj wolność w rozumieniu wolności od strachu, ale również zdrowie — w odniesieniu do włamań na konta na portalach społecznościowych, przede wszystkim psychiczne, a także nienaruszalność korespondencji oraz prawo do zachowania prywatności[24]. W omawianym czynie dochodzi do swego rodzaju przywłaszczenia tożsamości osoby pokrzywdzonej[25]. Odnosząc się do włamań na konta na portalach społecznościowych, działaniem takim może być przykładowo podszycie się pod kogoś za pomocą jego profilu na portalu społecznościowym i udostępnianie wpisów odnośnie do świadczenia usług seksualnych[26]. Zaznaczyć jednak wypada, że do odpowiedzialności z art. 190a § 2 k.k., konieczne jest wystąpienie skutku w postaci szkody materialnej bądź osobistej wyrządzonej ofierze[27], a zgodnie ze stanowiskiem Sądu Najwyższego, sprawca musi działać w zamiarze bezpośrednim[28]. Odnosząc się jednak do przywołanego wyżej przykładu podszycia się za kogoś

[21] A. Behan [w:] *Kodeks karny. Komentarz,* red. J. Kulesza, Warszawa 2025, art. 267, teza nr 9, LEX/el.
[22] *Ibidem*.
[23] Wyrok SA w Krakowie z 8 stycznia 2019 r., sygn, akt II AKa 194/17, KZS 2019, nr 3, poz. 69.
[24] M. Mozgawa [w:] *Kodeks karny. Komentarz aktualizowany*, red. M. Mozgawa, Warszawa 2026, art. 190(a), teza nr 3, LEX/el.
[25] *Ibidem*, teza nr 11.
[26] Zob. Wyrok SR w Kętrzynie z 9 października 2025 r., sygn. akt II K 217/25, LEX nr 3936889.
[27] M. Mozgawa [w:] *Kodeks karny. Komentarz aktualizowany*, red. M. Mozgawa, Warszawa 2026, art. 190(a), teza nr 16, LEX/el.
[28] Wyrok SN z 27 stycznia 2017 r., sygn. akt V KK 347/16, LEX nr 2269116.

wykorzystując jego dane i wizerunek, a następnie umieszczanie tego typu ogłoszeń, pomimo braku jakiegokolwiek jego związku z branżą seksualną, z pewnością narażają taką osobę na szkodę osobistą. Omawiając czyny polegające na włamaniu na konto na portalu społecznościowym warto wspomnieć również o kwalifikowanym typie przestępstwa z art. 190a § 2 k.k. znajdującym się w § 3, który zaostrza karę w sytuacji, gdy następstwem takiego podszycia się jest targnięcie się pokrzywdzonego na własne życie. Jest to istotne z punktu widzenia tematyki, bowiem niejednokrotnie podszycie się może doprowadzić do ośmieszenia ofiary, zniszczenia jej wizerunku czy to prywatnego czy zawodowego/szkolnego, które prowadzić mogą do zachowań autodestrukcyjnych, w tym i do targnięcia się na życie[29], co związane jest ze wskazywanym już wyżej niejakim przeniesieniem życia do przestrzeni wirtualnej.

Omawiając przestępstwa popełniane za pośrednictwem Internetu i portali społecznościowych, nie sposób nie wskazać na zniesławienie polegające na godzeniu w dobre imię osoby fizycznej, osoby prawnej czy jednostki organizacyjnej, jakim cieszy się ona w swoim otoczeniu czy opinii publicznej[30]. Czyn ten penalizowany jest przez art. 212 k.k., a regulacja ta zapewnia ochronę przed samowolnymi atakami na dobre imię i cześć osób fizycznych, osób prawnych czy instytucji[31], a więc chroni dobra osobiste. Wskazać tu należy, że ochrona dóbr osobistych jest wielopoziomowa, bowiem wynika nie tylko z omawianego artykułu, ale również i z przepisów Kodeksu cywilnego[32] w odniesieniu do człowieka. Pokazuje to doniosłość dóbr osobistych i konieczność ich ochrony. Przedmiotem ochrony w omawianym czynie zabronionym będzie zatem szacunek, poważanie czy uznanie, a więc ogólnie rozumiana cześć zewnętrzna, tj. taka, jaką posiada się w pojęciu innych ludzi[33]. Jak wskazuje chociażby Sąd Okręgowy w Kielcach[34], przy przestępstwie zniesławienia, nie ma znaczenia skutek w postaci nieprzyjemności dla pokrzywdzonego w pracy czy życiu osobistym, bowiem do realizacji znamion wskazywanego czynu zabronionego, konieczne jest narażenie pokrzywdzonego na te nieprzyjemności, a nie samo ich wystąpienie. Przykładem zniesławienia może być publiczne pomawianie danej osoby, narażanie jej na utratę zaufania w środowisku, poprzez np. wskazywanie, że nie ma ona kompetencji do wykonywania swojej pracy czy, że jest skorumpowana w np. przypadku urzędników czy lekarzy. W przypadku włamań na konta na portalach społecznościowych, zniesławienie może nastąpić dwupłaszczyznowo — włamywacz może pomówić zarówno samą ofiarę rzeczonego włamania, jak i inne osoby w jej imieniu, np. umieszczając wpis na profilu. Omawiając instytucję zniesławienia, wskazać należy na fakt, iż wiele organizacji od lat postuluje za depenalizacją ów czynu, bowiem przepis art. 212 k.k. nadmiernie ingeruje w swobodę wypowiedzi[35]. Jest to zagadnienie szeroko

[29] C. P. Denwigwe, R. D. Uche, P. N. Asuquo, M. W. Ngbar, *Cyber-trolling, cyber-impersonation and social adjustment among secondary school students in Calabar Education Zone, Cross River State, Nigeria,* „British Journal of Education" 2019, nr 7, s. 50.
[30] J. Kulesza [w:] *Kodeks karny. Komentarz*, red. J. Kulesza, Warszawa 2025, art. 212, teza nr 1.
[31] Zob. wyrok TK z 30 października 2006 r., sygn. akt. P 10/06 (Dz. U. z 2006 r., nr 202, poz. 1492).
[32] Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. z 2025 r., poz. 1508), dalej: k.c.
[33] M. Mozgawa [w:] *Kodeks karny. Komentarz aktualizowany*, red. M. Mozgawa, LEX/el. 2026, art. 212, teza nr 2.
[34] Wyrok SO w Kielcach z 6 grudnia 2013 r., sygn. akt. IX Ka 908/13, LEX nr 1717784.
[35] J. Kotas, *Karać czy zasądzać — dylematy towarzyszące odpowiedzialności karnej za zniesławienie „*Nowa Kodyfikacja Prawa Karnego" 2020, t. LVI, s. 21.

komentowane, również z uwagi na nieustanny rozwój mediów społecznościowych, forów itp., jednak zdaniem autorki niniejszej publikacji, ochrona przed publicznym godzeniem w dobre imię, zwłaszcza za pośrednictwem portali społecznościowych, jest niezwykle ważna i powinna być zachowana. Oczywiście w sytuacji, gdy wskazywane twierdzenia nie polegają na prawdzie i służą jedynie wyrządzeniu szkody danej osobie.

Cyberprzestępstwa polegać również mogą na zniewadze zarówno w obecności osoby znieważanej, jak i bez jej obecności, ale w taki sposób, by do tej osoby dotarła, a penalizowana jest przez art. 216 k.k. i może co do zasady być popełniona przez każdego z uwagi na podmiot powszechny[36]. Przedmiotem ochrony, *a contrario* do wyżej omawianego przestępstwa zniesławienia z art. 212 k.k., jest cześć wewnętrzna danej osoby, a więc godność osoby fizycznej, która chroniona jest bez względu na wszelkie jej okoliczności podmiotowe, takie jak np. płeć, wiek czy pochodzenie[37]. Zniewaga wyrażona może być słowem mówionym, pisanym, drukiem czy wizerunkiem (np. przerobionym)[38] i była szeroko rozważana przez sądy. Przykładowo, Sąd Najwyższy[39] wskazuje, iż przestępstwo zniewagi polega na użyciu słów obelżywych lub ośmieszających, postawionych w formie niezracjonalizowanej. O uznaniu określonych sformułowań za znieważające, decydują w pierwszym rzędzie ogólnie przyjęte normy obyczajowe. Sąd Najwyższy wskazuje ponadto, że przestępstwo znieważenia popełnione może być zarówno w zamiarze bezpośrednim, jak i ewentualnym, gdy sprawca przewidując możliwość takiego skutku swojego zachowania, godzi się z tym[40]. Pozostając w tematyce portali społecznościowych i Internetu, wskazać należy, że art. 216 § 2 k.k., wprost wskazuje na znieważenie za pomocą środków masowego komunikowania, za które, podobnie jak w przypadku wyżej omawianego zniesławienia z art. 212 k.k., grozi surowsza odpowiedzialność aniżeli za zniewagę dokonaną bez tych środków, bowiem za zniewagę z § 1 grozi kara grzywny albo ograniczenia wolności, zaś za zniewagę za pomocą środków masowego komunikowania z § 2, grozi kara grzywny, ograniczenia wolności albo pozbawienia wolności do roku. Jest to zatem ponownie kwalifikowany typ omawianego czynu zabronionego. Na potrzeby zakresu objętego niniejszą publikacją, przyjąć należy, że zniewaga może być dokonana przez działanie, bowiem znieważenie osoby poprzez środki masowego komunikowania wyrażone musi być poprzez pewne działanie. Znieważenie podobnie, jak w przypadku zniesławienia popełnione może zostać dwupłaszczyznowo i godzić w godność samego właściciela konta, na które się włamano, jak i może nastąpić poprzez znieważenie innych osób za pośrednictwem tego konta, np. poprzez wysyłanie do znajomych ofiary włamania na konto na portalu społecznościowym, wiadomości zawierających określenia obraźliwe.

## 4. Cyberprzestępstwa w rzeczywistości i problematyka z nimi związana

Celem wskazania, jakie formy przybierają cyberprzestępstwa w rzeczywistości, autorka dokonała analizy wybranych spraw i orzeczeń sądowych, które dotyczyły omawianych wyżej

[36] Wyrok SN z 16 października 2012 r., sygn. akt V KK 391/11, LEX nr 1226788.
[37] M. Mozgawa [w:] *Kodeks karny. Komentarz aktualizowany*, red. M. Mozgawa, Warszawa 2026, art. 216, teza nr 1, LEX/el.
[38] *Ibidem*, teza nr 3.
[39] Postanowienie SN z dnia 7 maja 2008 r., sygn. akt III K 234/07, OSNKW 2008, nr 9, poz. 69.
[40] Wyrok SN z 17 stycznia 2023 r., sygn. akt V KK 228/22, LEX nr 3511435.

przestępstw dokonanych w związku z włamaniem na konta na portalach społecznościowych. Analiza ta pozwala na uchwycenie rzeczywistego przebiegu zdarzeń oraz złożoności zachowań sprawców, które często obejmują więcej niż jeden typ czynu zabronionego. Przykładem takiego zachowania jest przypadek polegający na nieuprawnionym uzyskaniu dostępu najpierw do skrzynki poczty elektronicznej, a następnie do konta użytkownika w serwisie Facebook. Sprawca, po przejęciu kontroli nad profilem, podejmował różnorodne działania, w tym kierował do znajomych pokrzywdzonego prośby o przekazanie pieniędzy za pomocą systemu płatności BLIK. Dodatkowo wysyłał wiadomości zawierające groźby karalne, treści obraźliwe oraz materiały o charakterze pornograficznym. Zachowanie sprawcy obejmowało również modyfikację danych profilowych, w tym zmianę nazwy konta na związaną z branżą erotyczną, co mogło prowadzić do dalszego naruszenia dóbr osobistych pokrzywdzonego.

W toku postępowania przygotowawczego, napotkano istotne przeszkody w postaci korzystania przez sprawcę czynu z VPN. Kwestii VPN wypada poświęcić kilka zdań, rozpoczynając od nakreślenia czym to jest. VPN (z ang. *virtual private network*) jest wirtualną siecią prywatną, rozszerzoną na sieć publiczną, pozwalającą jednak korzystać z wielu benefitów sieci prywatnej[41]. Dzięki zastosowaniu VPN, realny adres IP jest ukryty, bowiem strony widzą adres serwera VPN, a nie konkretnego urządzenia, co może dawać pewne poczucie anonimowości i niejednokrotnie stanowi przeszkodę w ustaleniu sprawcy.

Należy jednak podkreślić, że stosowanie VPN nie zapewnia pełnej anonimowości. W literaturze oraz praktyce wskazuje się, że możliwe jest ustalenie tożsamości użytkownika m.in. poprzez analizę metadanych, korelację czasową aktywności czy współpracę z dostawcami usług teleinformatycznych[42]. Rzeczywiste adresy IP przechowywane są również przez wielu dostawców VPN, wobec czego możliwym jest wystąpienie do konkretnego dostawcy o takie dane w toku postępowania karnego. VPN utrudnia identyfikację, jednak nie gwarantuje anonimowości. Wracając do omawianej sprawy, Sąd Rejonowy w Olsztynie, uznał jednak, że z uwagi na korzystanie przez sprawcę z VPN, nie jest możliwe jego wykrycie[43]. Wskazać jednak należy, że istnieją przypadki, gdy organy ścigania ustaliły sprawcę pomimo stosowania maskowania adresu IP, natomiast w takich sytuacjach, niejednokrotnie wymagane było podjęcie współpracy międzynarodowej[44], co rzecz jasna, generuje m.in. większe koszty postępowania.

Na podstawie analizy przedmiotowej sprawy, możliwe jest wywiedzenie pewnych ogólnych wniosków. Po pierwsze, jest to brak odpowiednich środków i narzędzi, będących w posiadaniu służb, które pozwoliłyby na skuteczne wykrywanie sprawców tego typu czynów. Często bywa tak, że technologia stosowana przez służby nie jest wystarczająca do tego, by

[41] K. Karuna Jyothi, B. Indira Reddy, *Study in virtual private network (VPN), VPN's Protocols and Security* International „Journal of Scientific Research in Computer Science, Engineering and Information Technology" 2018, t. 3, s. 919.
[42] V. K. Jain, J. Aggrawal, R. Dangi, S. S. Prasad Shukla, A. K. Yadav, G. Choudhary, *Unmasking the True Identity: Unveiling the Secrets of Virtual Private Networks and Proxies* „Next-Generation Communication Networks and Systems in Smart Cities: Enhancing Connectivity, Security, and Performance". (https://www.mdpi.com/2078-2489/16/2/126?utm (dostęp: 17.02.2026 r.).
[43] Postanowienie SR w Olsztynie z dnia 28 stycznia 2026 r., sygn. akt. II Kp 1572/25.
[44] K. Kiejnich-Kruk, *Szyfrowanie i maskowanie danych – wyzwania dla wymiaru sprawiedliwości i organów ścigania* [w:] *Pozyskiwanie dowodów elektronicznych przez organy ścigania i wymiaru sprawiedliwości*, Warszawa 2026, LEX/el.

skutecznie wykryć sprawcę czynu oraz ustalić jego okoliczności. Wskazać również należy na istotny problem transgraniczności cyberprzestrzeni, a także na ograniczenia proceduralne. Podkreślenia wymaga również, że stosowanie technologii takich jak VPN, istotnie zwiększa poziom skomplikowania postępowań. Wobec powyższego wskazać należy, że skuteczne przeciwdziałanie tego rodzaju przestępczości wymaga dalszego rozwoju zarówno narzędzi technicznych, jak i mechanizmów współpracy międzynarodowej oraz odpowiednich regulacji prawnych. Nie bez znaczenia pozostają konsekwencje dla pokrzywdzonych, bowiem tego typu czyny prowadzić mogą do naruszenia poczucia bezpieczeństwa, utraty zaufania do środowiska wirtualnego oraz wywoływać skutki psychologiczne, np. strach czy lęk.

Omawiana wyżej sprawa napotkała trudności przy wykryciu sprawcy czynu, jednak wskazać należy, że często sytuacja kształtuje się odmiennie. Istotną rolę odgrywają chociażby okoliczności popełnienia czynu. Sąd Rejonowy w Wałbrzychu, rozpatrywał sprawę włamania męża na konto żony na portalu Facebook[45]. Kobieta pozostawiła swój prywatny komputer w domu, podczas gdy była w pracy. Wówczas jej mąż przełamał zabezpieczenia do jej komputera oraz hasło do jej konta na portalu społecznościowym, przez co uzyskał nieuprawniony dostęp do informacji dla niego nieprzeznaczonych. Po powrocie do domu, kobieta miała problem z zalogowaniem się na wskazany portal, a wkrótce zaczęła podejrzewać męża o to, że włamał się na jej konto. Mąż wówczas poinformował, że rzeczywiście dokonał włamania, przejrzał czat i wydrukował korespondencje. W toku postępowania, mężczyzna wskazywał jednak, że komputer był do użytku wspólnego i podczas korzystania, zauważył, że żona nie wylogowała się ze swojego konta na Facebooku i wówczas przejrzał wiadomości. Przyznał również, że zna hasło do ów profilu oraz do poczty elektronicznej. Finalnie sąd uznał mężczyznę za winnego, a przyczyniła się do tego uzyskana od administratora portalu, lista zawierająca daty i godziny logowań, która wskazywała, iż logowania z domowego komputera miały miejsce w czasie, gdy pokrzywdzona była w pracy. Na podstawie opisywanej sprawy, dostrzec można, iż jest możliwe uzyskanie dat, godzin i miejsc logowań na portalu Facebook od jego administratora, co stanowi istotny dowód, pozwalający ustalić tożsamość sprawcy czynu. Wskazać jednak należy, że ta sprawa różni się znacznie od opisywanej wcześniej, bowiem nie zaistniały w niej przeszkody polegające na maskowaniu adresu IP czy konieczności ustalenia tożsamości sprawcy. W opisywanym stanie faktycznym, należało ustalić przede wszystkim okoliczności popełnienia czynu i winę konkretnej osoby, nie zaś poszukiwać winnego od początku, co w obiektywnej ocenie, zwiększa szansę na doprowadzenie do skazania osoby winnej, jak było w tym przypadku.

Warto omówić również sprawę rozpatrywaną przez Sąd Okręgowy w Poznaniu[46], w którym doszło do dokonania zmiany hasła na koncie na portalu Facebook oraz treści zawartych na tym koncie, tj. zdjęcia profilowego, usunięcia i dodania znajomych, a ponadto doszło do wysłania zdjęć małoletniej pokrzywdzonej do jej matki przez chat znajdujący się na wymienionym portalu oraz kontaktu z koleżankami pokrzywdzonej w ten sam sposób.

[45] Wyrok SR w Wałbrzychu z dnia 11 października 2017 r., sygn. akt. II K 1036/16, LEX nr 2421166.
[46] Wyrok SO w Poznaniu z dnia 22 maja 2015 r., sygn. akt. XVII Ka 384/15, POSP [https://orzeczenia.poznan.so.gov.pl/content/$N/153510000008506_XVII_Ka_000384_2015_Uz_2015-05-22_001?TSPD_101_R0=0806c18aaaab20003bfb22f5e00d67d77b69e7c3feeadd86c87fef14ae16cfe6014c9b1a17f61ee0084d76a3ce14300084f126289911ca7209ab7ebe806e66275356b79424a2ebaf652f4f39eb3271adcb78db863c21c466869ed8801adc386c].

Postępowanie sprawcy ponownie naraziło dobre imię i godność pokrzywdzonej. W niniejszej sprawie, podobnie jak w opisywanej wyżej, odnalezienie sprawcy nie stanowiło znacznych trudności, bowiem małoletnia pokrzywdzona wskazywała, że jedyną osobą, której przekazywała hasło do swojego konta, a także zdjęcie w bieliźnie, które zostało ustawione jako zdjęcie profilowe, jest właśnie oskarżony. Wobec powyższego, niemalże od początku wiadomym było, kto dokonał wskazywanych czynów, a więc w czasie postępowania koniecznym było ustalenie okoliczności popełnienia czynu oraz winy sprawcy. Podkreślić należy też rolę rodziców oraz edukację małoletnich w kwestii bezpieczeństwa w sieci oraz nieujawniania nikomu haseł dostępu do kont na portalach społecznościowych, aby uniknąć takich sytuacji, jak ta opisywana, a tym samym konsekwencji dla małoletniego — zarówno w kwestii zdrowia psychicznego, jak i kwestiach związanych z życiem społecznym. Rzecz jasna prowadzenie chociażby kampanii edukacyjnych odnośnie cyberprzestępstw, przeznaczonych dla ogółu społeczeństwa również jest wskazane i może podnieść bezpieczeństwo w przestrzeni wirtualnej oraz udaremnić popełnianie ww. przestępstw.

Na podstawie powyższych orzeczeń, dostrzec można pewną prawidłowość, a mianowicie fakt, że sprawy, które zakończyły się ujęciem i skazaniem sprawcy, co do zasady są sprawami, w których istniały uprzednie przesłanki pozwalające na zawężenie kręgu podejrzanych, a więc skuteczność postępowania była w dużej mierze uzależniona od istnienia punktu odniesienia umożliwiającego identyfikację potencjalnego sprawcy. Odmiennie kształtuje się sytuacja w sprawach, w których doszło do włamania na konto Facebookowe przez osobę niezidentyfikowaną, ciężej jest ustalić sprawcę, co wynika zarówno z braku wstępnych danych pozwalających na jego wytypowanie, jak i z wykorzystywania przez sprawców narzędzi technicznych służących maskowaniu aktywności w sieci (np. VPN). W ocenie autorki, zasadnym jest, aby wciąż rozwijać narzędzia wykorzystywane przez organy ścigania, a także wzmocnić współpracę międzynarodową, co pozwoli na skuteczne wykrywanie również sprawców używających VPN czy też innego oprogramowania kamuflującego rzeczywiste IP. Internet nie jest przestrzenią anonimową, a każda aktywność użytkownika pozostawia jakiś ślad. Natomiast działania służb w przypadkach włamań na konta społecznościowe czy ogólnie cyberprzestępstw, winny skutecznie prowadzić do ujawnienia tych śladów i wykrycia sprawcy, bowiem ma to znaczenie nie tylko dla wykrywania sprawców, lecz także dla realizacji funkcji prewencyjnej prawa karnego, oddziałującej zarówno na potencjalnych sprawców, jak i na ogół użytkowników przestrzeni cyfrowej.

## 5. Podsumowanie

Podsumowując kwestię cyberprzestępstw polegających na włamaniu na konta na portalach społecznościowych, zauważyć należy, że pomimo powszechnego dostępu do Internetu i stosunkowo dużej świadomości społecznej odnośnie do zagrożeń z nimi związanych, przestępstwa te zdarzają się dość często. Wskazuje to na fakt, iż bardzo dużą rolę w ochronie przed cyberprzestępstwami, stanowi edukacja odnośnie do bezpieczeństwa w sieci, w tym nieudostępniania nikomu danych do logowania na wskazywanych portalach czy korzystania z zabezpieczeń dwuetapowych. Edukacja w tym zakresie pomaga zwiększyć świadomość oraz czujność społeczeństwa. Pozwala to ograniczyć występowanie tego typu czynów zabronionych, jednak nie niweluje ich w zupełności. Wobec powyższego, koniecznym

jest również opracowanie odpowiednich i skutecznych metod postępowania przez służby w przypadku zaistnienia takich przestępstw, bowiem skuteczne przeciwdziałanie cyberprzestępczości wymaga nie tylko działań o charakterze prewencyjnym, lecz także odpowiedniego przygotowania instytucjonalnego organów ścigania, a także stosowania mechanizmów współpracy — w szczególności o charakterze międzynarodowym.

Walka z cyberprzestępstwami, zwłaszcza polegającymi na próbie ośmieszenia kogoś czy zniszczenia jego pozycji zarówno w środowisku prywatnym, jak i zawodowym, jest niezwykle ważna, ponieważ w aktualnych czasach, gdy internet jest powszechnie dostępny, a znaczna część społeczeństwa posiada profile na portalach społecznościowych, jednym czynem można zniszczyć czyjeś życie i doprowadzić go do rozstroju zdrowia psychicznego, a w skrajnych przypadkach, również do targnięcia się na życie. Wobec powyższego, konieczna jest walka wielopłaszczyznowa, obejmująca zarówno prewencję, jak i doprowadzanie do ukarania sprawców. Skala potencjalnych następstw uzasadnia potrzebę traktowania tego rodzaju czynów jako istotnego problemu społecznego.

W konsekwencji zasadne jest przyjęcie podejścia wielopłaszczyznowego, obejmującego działania w zakresie edukacji, prewencji, rozwoju narzędzi technicznych oraz skutecznego ścigania sprawców, co ostatecznie z pewnością przełoży się na ograniczenie występowania tego typu czynów zabronionych.

## Bibliografia

**Akty prawne:**
Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz. U. z 2025 r., poz. 383)
Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2025 r., poz. 1508).

**Literatura:**
Behan A. [w:] *Kodeks karny. Komentarz*, red. J. Kulesza, Warszawa 2025.
Chmielewska A., Kondrat M., *Popularność mediów społecznościowych w Polsce — analiza według płci* „Kobieta i Biznes/Women and Business" 2023, s. 16-24.
Denwigwe C. P., Uche R. D., Asuquo P. N., Ngbar M. W., *Cyber-trolling, cyber-impersonation and social adjustment among secondary school students in Calabar Education Zone, Cross River State, Nigeria.* „British Journal of Education" vol. 7, 2019, s. 44-52.
Filipkowski W., *Cyberprzestępstwo o charakterze terrorystycznym w polskim prawie karnym „*Prawo w Działaniu. Sprawy Karne" 2023, nr 55, s. 72-87.
Jain V. K., Aggrawal J., Dangi R., Prasad Shukla S. S., Yadav A. K., Choudhary G., *Unmasking the True Identity: Unveiling the Secrets of Virtual Private Networks and Proxies* „Next-Generation Communication Networks and Systems in Smart Cities: Enhancing Connectivity, Security, and Performance" 2025.
Kałdon B., *Cyberprzestrzeń jako zagrożenie dla człowieka XXI wieku* „Seminare. Poszukiwania naukowe" 2016, t. 37, nr 2, s. 87-101.
Karuna Jyothi K., Indira Reddy B., *Study in virtual private network (VPN), VPN's Protocols and Security* International „Journal of Scientific Research in Computer Science, Engineering and Information Technology" 2018, t. 3, s. 919-932.
Kiejnich-Kruk K., *Pozyskiwanie dowodów elektronicznych przez organy ścigania i wymiaru sprawiedliwości*, Warszawa 2026, LEX/el.
Kotas J., *Karać czy zasądzać — dylematy towarzyszące odpowiedzialności karnej za zniesławienie „*Nowa Kodyfikacja Prawa Karnego" 2020, t. LVI, s. 13-38.
Kulesza J. [w:] *Kodeks karny. Komentarz*, red. J. Kulesza, Warszawa 2025.
Lisowska-Kierepka A., *Przestępczość jako zjawisko geograficzne? Przegląd badań nad zjawiskiem w świetle wybranych nauk* „Przegląd Geograficzny" 2020, nr 92, s. 267-290.
Lipiński K. [w:] *Kodeks karny. Część szczególna. Komentarz*, red. J. Giezek, Warszawa 2021.
Budyn-Kulik M., Kozłowska-Kalisz P., Kulik M., Mozgawa M., *Kodeks karny. Komentarz aktualizowany*, LEX/el. 2025.
Niemiec M., *Przestępstwo wypadku drogowego w pytaniach i odpowiedziach,* Warszawa 2019, LEX/el.
Stefanowicz M., *Cyberprzestępczość — próba diagnozy zjawiska, „*Kwartalnik Policyjny" 2017, nr 4, s. 19-23.
Urbańska N., *Cyberprzestępczość i wynikające z niej zagrożenia* „Cybersecurity & Cybercrime" 2025, t. 1, nr 7, s. 61-74.
Wall D. S., *Cybercrime: The Transformation of Crime in the Information Age,* 2017, s. 1-288.
Wiatrowska A., *(Nie)Bezpieczne korzystanie z Internetu przez młodych dorosłych — raport z badań* „Annales Universitatis Mariae Curie-Skłodowska Lublin-Polonia" 2024, t. XXXVII, nr 4, s. 65-76.
Zegarow P., *Analiza. Psychologiczne aspekty cyberbezpieczeństwa „*NASK Cyberpolicy" 2019, s. 1-6.

**Orzecznictwo:**
Postanowienie SN z dnia 7 maja 2008 r., sygn. akt III K 234/07, OSNKW 2008, nr 9, poz. 69.
Postanowienie SR w Olsztynie z dnia 28 stycznia 2026 r., sygn. akt. II Kp 1572/25, niepubl.

Uchwała Sądu Najwyższego z 22 stycznia 2003 r., sygn. akt I KZP 43/02, OSNKW 2003, nr 1-2, poz. 5.
Wyrok SA w Krakowie z 8 stycznia 2019 r., sygn, akt II AKa 194/17, KZS 2019, nr 3, poz. 69.
Wyrok SO w Piotrkowie Trybunalskim z 20 maja 2025 r., sygn. akt IV Ka 246/25, LEX nr 3927770.
Wyrok SN z 27 stycznia 2017 r., sygn. akt V KK 347/16, LEX nr 2269116.
Wyrok SN z 16 października 2012 r., sygn. akt V KK 391/11, LEX nr 1226788.
Wyrok SN z 17 stycznia 2023 r., sygn. akt V KK 228/22, LEX nr 3511435.
Wyrok SO w Kielcach z 6 grudnia 2013 r., sygn. akt. IX Ka 908/13, LEX nr 1717784.
Wyrok SO w Poznaniu z dnia 22 maja 2015 r., sygn. akt. XVII Ka 384/15, POSP.
Wyrok SR w Kętrzynie z 9 października 2025 r., sygn. akt II K 217/25, LEX nr 3936889.
Wyrok SR w Wałbrzychu z dnia 11 października 2017 r., sygn. akt. II K 1036/16, LEX nr 2421166.
Wyrok TK z 30 października 2006 r., sygn. akt. P 10/06 (Dz. U. z 2006 r., nr 202, poz. 1492).