Pojęcia kluczowe: *bezprawność, obrona konieczna, okoliczności wyłączające bezprawność czynu, kontratypy, przestępstwa internetowe*

Tomasz Jankowiak

O obronie koniecznej przed przestępstwami internetowymi

Abstrakt

Przedmiotem badań poruszonych w niniejszym artykule jest nieomawiana dotychczas kwestia obrony koniecznej przed przestępstwami internetowymi popełnianymi na odległość, w szczególności przed hackingiem. W publikacji przy użyciu metody dogmatycznoprawnej przeanalizowano m.in. możliwe działania obronne przed przestępstwem internetowym w sytuacji, gdy ofiara ma bezpośredni kontakt z napastnikiem; możliwość obrony koniecznej przed atakiem hackerskim przy użyciu oprogramowania informatycznego *honeypot* oraz przedstawiono postulat *de lege ferenda* w zakresie ustanowienia nowego kontratypu w części szczególnej Kodeksu karnego.

I. Wprowadzenie

Problematyka przestępstw popełnianych przy użyciu nowych technologii była już przedmiotem wielu rozważań w literaturze poświęconej polskiemu systemowi prawa karnego. Liczne publikacje zostały także poświęcone kontratypowi obrony koniecznej, w szczególności w zakresie wykładni jego znamion. Bliższej ocenie nie poddano jednak dotychczas możliwości odpierania w ramach kontratypu obrony koniecznej bezprawnych zamachów stanowiących przestępstwa internetowe popełniane na odległość. Szczególnie praktyczną doniosłość – wobec nieustającego postępu technologicznego – może mieć w powyższym zakresie zagadnienie obrony koniecznej przed atakiem hackerskim.

Celem niniejszego tekstu i tym samym przedmiotem badań jest zatem dokonanie ustaleń zmierzających do odpowiedzi na pytanie, czy i w jakim zakresie możliwa jest obrona konieczna przed przestępstwami internetowymi, przy uwzględnieniu podziału tych przestępstw na takie, które są popełniane całkowicie na odległość, i takie, które na odległość popełniane są tylko częściowo. W szczególności przeanalizowana

DOI: 10.54383/0031-0344.2025.10.5

zostanie możliwość obrony koniecznej przed hackingiem. Na podstawie poczynionych rozważań zostanie także przedstawiony postulat *de lege ferenda* w zakresie ustanowienia nowego kontratypu w części szczególnej ustawy z dnia 6.06.1997 r. Kodeks karny[1]. Powyższe zostanie zrealizowane przy użyciu metody dogmatyczno-prawnej.

II. Przestępstwa internetowe i przestępstwa popełniane na odległość – uwagi ogólne

Szczególne znaczenie dla omawianej problematyki ma pojęcie przestępstwa popełnianego na odległość, gdyż do zbioru takich przestępstw należy m.in. zbiór przestępstw internetowych. Wskazać należy, że przestępstwa popełniane na odległość charakteryzują się tym, że część lub wszystkie znamiona strony przedmiotowej czynu zabronionego stanowiącego takie przestępstwo realizowane są w innym miejscu aniżeli miejsce działania sprawcy. Mogą one mieć zarówno skutkowy, jak i bezskutkowy charakter. Przykładem takiego skutkowego przestępstwa może być stypizowane w art. 268a § 1 Kodeksu karnego zniszczenie danych informatycznych np. przy użyciu złośliwego oprogramowania. Jako przykład takiego przestępstwa bezskutkowego wskazać można stypizowaną w art. 216 Kodeksu karnego zniewagę popełnioną za pośrednictwem środków masowego komunikowania[2]. W obu powyższych przykładach co najmniej część znamion strony przedmiotowej czynu zabronionego realizowana jest poza miejscem działania sprawcy.

Przestępstwa internetowe stanowią natomiast grupę przestępstw polegających na wykorzystaniu możliwości istniejących w sieci Internet[3] i są one ze swej natury jednocześnie przestępstwami popełnianymi na odległość. Przestępstwa internetowe dzieli się na przestępstwa internetowe *sensu stricto* oraz przestępstwa internetowe *sensu largo*. Pierwsze z nich to takie przestępstwa, których główne czynności wykonawcze zostały dokonane za pomocą Internetu. Manifestują się one w obrębie sieci i zaistnieć mogły tylko dzięki oferowanym przez Internet usługom. W przypadku przestępstw internetowych *sensu largo* czynności podejmowane za pośrednictwem Internetu nie

1 Ustawa z dnia 6.06.1997 r. Kodeks karny (t.j. Dz.U. z 2024 r. poz. 17 z późn. zm.), dalej: Kodeks karny.

2 Zniewagę jako przestępstwo bezskutkowe słusznie kwalifikują: J. Długosz-Jóźwiak (w:) *Kodeks karny. Część szczególna. Komentarz do artykułów 117–221, tom I*, red. M. Królikowski, R. Zawłocki, Warszawa 2023, komentarz do art. 216, nb. 30; J. Raglewski (w:) *Kodeks karny. Część szczególna. Tom II. Część II. Komentarz do art. 212–277d*, red. W. Wróbel, A. Zoll, Warszawa 2017, komentarz do art. 216, teza 26 oraz A. Muszyńska (w:) *Kodeks karny. Część szczególna. Komentarz*, red. J. Giezek, Warszawa 2021, komentarz do art. 216, teza 20. Zob. jednak pogląd odmienny: M. Surkont, *Problem skutkowego charakteru zniesławienia*, „Palestra" 1978/4 (244), s. 21–22.

3 D. Michalecki, *Przestępstwa internetowe – zapobieganie i zwalczanie*, „Kontrola Państwowa" 2023/5, s. 74. Podobnie: M. Sowa, *Ogólna charakterystyka przestępczości internetowej*, „Palestra" 2001/5–6 (521–522), s. 29; A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 33 (przypis nr 4) oraz F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016, s. 127.

 DOI: 10.54383/0031-0344.2025.10.5

stanowią realizacji ich znamion czynności wykonawczej, a użycie Internetu jest jedynie jednym ze środków prowadzących do celu realizującego się poza siecią[4].

Przedmiotem niniejszych rozważań będą co do zasady przestępstwa internetowe *sensu stricto*, będące przestępstwami popełnianymi na odległość. Z punktu widzenia dalszych rozważań funkcjonalne będzie dokonanie podziału przestępstw popełnianych na odległość na takie, które są popełniane całkowicie na odległość, i takie, które na odległość popełniane są tylko częściowo. W przypadku pierwszych z nich zachodzi bezpośredni kontakt ofiary i sprawcy. Natomiast w przypadku przestępstw popełnianych całkowicie na odległość sprawca przestępstwa oraz jego ofiara nie mają ze sobą kontaktu w ogóle lub mają ze sobą kontakt wyłącznie za pośrednictwem środków komunikacji na odległość. Dokonanie powyższego podziału będzie miało kluczowe znaczenie dla określenia możliwych działań w ramach instytucji obrony koniecznej.

II.I. Przestępstwa popełniane częściowo na odległość

W przypadku przestępstw popełnianych częściowo na odległość co najmniej część znamion czynu zabronionego jest realizowana na odległość, przy jednoczesnym bezpośrednim kontakcie sprawcy z ofiarą.

Jako przykład takiego przestępstwa można wskazać następującą sytuację: sprawca, znajdując się obok ofiary po wcześniejszej groźbie popełnienia na jej szkodę przestępstwa zniesławienia w razie niedokonania określonej czynności, wobec braku dokonania przez ofiarę żądanej czynności, pomawia ją przy użyciu środków porozumiewania się na odległość o takie postępowanie lub właściwości, które mogą poniżyć ją w opinii publicznej.

W tej sytuacji – zakładając, że nie wystąpiła dodatkowo żadna okoliczność wyłączająca przestępność czynu – popełniane są dwa przestępstwa: stypizowana w art. 190 § 1 Kodeksu karnego groźba karalna oraz stypizowane w art. 212 § 1 Kodeksu karnego zniesławienie. Przestępstwem, które w opisanej wyżej sytuacji można zakwalifikować jako przestępstwo popełniane częściowo na odległość, jest zniesławienie. Sprawca znajduje się bowiem obok ofiary, tj. ma z nią bezpośredni kontakt, ale na odległość jest realizowane znamię czynności wykonawczej tego czynu zabronionego. Jak natomiast słusznie wskazuje się w literaturze, znamię czynności wykonawczej zniesławienia może zostać zrealizowane za pomocą wszelkich technicznych środków przekazu informacji, w tym SMS oraz Internetu[5].

4 M. Sowa, *Ogólna charakterystyka*…, s. 29 oraz F. Radoniewicz, *Odpowiedzialność karna*…, s. 127.

5 J. Długosz-Jóźwiak (w:) *Kodeks karny*…, komentarz do art. 212, nb. 26, tak też: W. Kulesza, *Rozdział VI. Przestępstwa przeciwko czci i nietykalności cielesnej* (w:) *System Prawa Karnego. Przestępstwa przeciwko dobrom indywidualnym, tom X*, red. J. Warylewski, Warszawa 2016, s. 1155, nb. 89 oraz T. Fołta, A. Mucha, *Zniesławienie i znieważenie w Internecie*, „Prokuratura i Prawo" 2006/11, s. 49–53.

DOI: 10.54383/0031-0344.2025.10.5

II.II. Przestępstwa popełniane całkowicie na odległość

Przestępstwa popełniane całkowicie na odległość charakteryzują się tym, że są popełniane na odległość w pełnej okazałości. Oznacza to, że wszelkie znamiona czynu zabronionego realizowane są na odległość, a sprawca w chwili popełnienia czynu nie ma w ogóle kontaktu z ofiarą albo kontakt między sprawcą a ofiarą odbywa się wyłącznie za pośrednictwem środków porozumiewania się na odległość.

Przestępstwami tego typu są m.in.: propagowanie zakazanych treści, czyli wszystkie te czyny zabronione, które można popełnić „za pomocą słowa", polegające na publicznym głoszeniu i prezentowaniu treści, które są przez prawo zakazane[6] – w tym omawiane już wyżej zniesławienie – o ile podczas ich popełniania ofiara i sprawca czynu nie mają ze sobą bezpośredniego kontaktu. Nadto można tak zakwalifikować czyn zabroniony stypizowany w art. 286 § 1 Kodeksu karnego, tj. oszustwo, w szczególności w postaci *phishingu*[7]; a także stypizowany w art. 267 § 1 Kodeksu karnego nieuprawniony dostęp do informacji uzyskany poprzez hacking, definiowany jako nieuprawnione wejście do systemów lub sieci komputerowych[8].

III. Obrona konieczna przed przestępstwami internetowymi popełnianymi częściowo na odległość

W przypadku przestępstw internetowych popełnianych częściowo na odległość ofiara co do zasady – o ile sprawca nie ograniczy jej swobody poruszania się – ma znaczne możliwości działania w ramach instytucji obrony koniecznej, niemalże takie same jak w przypadku zamachu, który w ogóle nie jest popełniany na odległość.

W razie bowiem zaistnienia bezpośredniego zamachu na dobra prawne ofiary (w tym sytuacji, gdy jeszcze nie są naruszane jej dobra prawne, ale występuje wysoki stopień prawdopodobieństwa, że zostaną zaatakowane w najbliższej chwili[9]), ofiara będzie mogła zniszczyć lub uszkodzić urządzenie, za pośrednictwem którego jest dokonywany bezprawny zamach, o ile uzna to za konieczne i efektywne w danej sytuacji, a jej przekonanie pokrywa się z obiektywną oceną realiów faktycznych sytuacji. Zniszczenie przedmiotu stanowiącego narzędzie zamachu lub jego uszkodzenie w taki sposób, że niemożliwe będzie kontynuowanie zamachu przy jego użyciu, jest niewątpliwie skuteczną formą obrony i jest to działanie konieczne dla odparcia omawianego zamachu.

6 M. Sowa, *Ogólna charakterystyka*…, s. 30.

7 Zob. F. Radoniewicz, *Odpowiedzialność karna*…, s. 107–108 oraz D. Chaładyniak, *Wybrane zagadnienia bezpieczeństwa danych w sieciach komputerowych*, „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki" 2015/13, s. 47.

8 A. Adamski, *Karalność hackingu*, „Przegląd Sądowy" 1998/11–12, s. 150, tak też: J. Piórkowska-Flieger (w:) *Kodeks karny. Komentarz*, red. T. Bojarski, Warszawa 2016, komentarz do art. 267, teza 3 oraz P. Kozłowska-Kalisz (w:) *Kodeks karny. Komentarz aktualizowany*, red. M. Mozgawa, LEX 2024, komentarz do art. 267, teza 6.

9 Wyrok SN z 4.02.2002 r. (V KKN 507/99), OSNKW 2002/5–6, poz. 38.

 DOI: 10.54383/0031-0344.2025.10.5

Taki sposób obrony cechuje się zatem walorem współmierności[10], tym bardziej że ofiara, broniąc się w ten sposób, nie narusza integralności cielesnej sprawcy. Wydaje się, że zaatakowanie rzeczy, za pośrednictwem której sprawca dokonuje zamachu, spośród możliwych oraz skutecznych środków i sposobów ochrony, jest najmniej dotkliwe dla sprawcy i tym samym taki sposób obrony powinna wybrać ofiara zamachu[11].

Ewentualnie w takiej sytuacji ofiara zamachu mogłaby zatrzymać sprawcę wraz z przedmiotem służącym do popełnienia zamachu, tylko że – przy spełnieniu przesłanek ustanowionych w art. 243 ustawy z dnia 6.06.1997 r. Kodeks postępowania karnego[12] – będzie to stanowiło realizację uprawnienia i nie będzie czynem bezprawnym, a co za tym idzie, nie będzie to działanie w ramach kontratypu obrony koniecznej. Należy przy tym zaznaczyć, że możliwość dokonania ujęcia obywatelskiego ustanowionego w art. 243 Kodeksu postępowania karnego nie wyłącza ofierze zamachu prawa do obrony koniecznej. Art. 243 Kodeksu postępowania karnego kreuje bowiem uprawnienie, a nie obowiązek prawny[13], gdyż od nikogo nie można wymagać podejmowania zachowań heroicznych[14].

Na marginesie odnotować można, iż omawiane przestępstwa mogą mieć jednocześnie charakter przemocy psychicznej. Jest tak w szczególności w przypadku opisanego już wyżej przykładu przestępstwa zniesławienia poprzedzonego groźbą karalną. W razie zaś obrony koniecznej przed bezprawnym zamachem stanowiącym przemoc psychiczną postuluje się, aby ofiara nie wkraczała w sferę cielesną napastnika, o ile jest to możliwe[15].

IV. Obrona konieczna przed przestępstwami internetowymi popełnianymi całkowicie na odległość

W przypadku przestępstw internetowych popełnianych całkowicie na odległość sytuacja ofiary w zakresie możliwości skorzystania z instytucji obrony koniecznej jest całkowicie odmienna. Wobec braku przebywania bezpośrednio przy sprawcy zamachu

10 Por. wyrok SA w Lublinie z 18.08.2009 r. (II AKa 99/09), LEX nr 523956 oraz M. Mozgawa (w:) *Kodeks karny…*, red. M. Mozgawa, komentarz do art. 25, teza 15.

11 Por. wyrok SA we Wrocławiu z 10.02.2015 r. (II AKa 6/15), LEX nr 1661290 oraz A. Zoll (w:) *Kodeks karny. Część ogólna. Tom I. Część I. Komentarz do art. 1–52*, red. W. Wróbel, A. Zoll, Warszawa 2016, komentarz do art. 25, teza 52.

12 Ustawa z dnia 6.06.1997 r. Kodeks postępowania karnego (t.j. Dz.U. z 2024 r. poz. 37 z późn. zm.), dalej: Kodeks postępowania karnego.

13 L.K. Paprzycki (w:) *Komentarz aktualizowany do art. 1–424 Kodeksu postępowania karnego*, red. L.K. Paprzycki, LEX 2015, komentarz do art. 243, teza 2, tak też: W. Smardzewski, *Z problematyki ujęcia na gorącym uczynku*, „Nowe Prawo" 1980/3, s. 46 oraz R.A. Stefański, S. Zabłocki (w:) *Kodeks postępowania karnego. Tom II. Komentarz do art. 167–296*, red. R.A. Stefański, S. Zabłocki, Warszawa 2019, komentarz do art. 243, teza 1.

14 J. Giezek, *Teorie winy we współczesnej dogmatyce prawa karnego* (w:) *Prawo karne materialne. Część ogólna i szczególna*, red. M. Bojarski, Warszawa 2023, s. 213–214.

15 T. Jankowiak, *Granice obrony koniecznej przed przemocą psychiczną w ramach instytucji obrony koniecznej*, „Palestra" 2023/10 (791), s. 85.

DOI: 10.54383/0031-0344.2025.10.5

możliwość obrony koniecznej jest bowiem niemal wyłączona. W szczególności w takich sytuacjach nie stanowi obrony koniecznej korzystanie ze standardowego oprogramowania antywirusowego czy odłączenie atakowanego urządzenia od sieci Internet, gdyż takie działania nie realizują znamion żadnego typu czynu zabronionego i nie powodują naruszenia żadnych dóbr prawnych sprawcy bezprawnego zamachu.

Mimo powyższych ograniczeń wynikających z faktu braku bezpośredniego kontaktu ofiary ze sprawcą czynu możliwe jest w określonych okolicznościach faktycznych działanie w ramach kontratypu obrony koniecznej przed omawianymi przestępstwami. W szczególności możliwa jest obrona przed hackingiem i innymi bezprawnymi zamachami polegającymi na włamaniu się do systemu teleinformatycznego i do tych przestępstw odnosić się będą dalsze rozważania.

Zarówno hacking, jak i inne bezprawne zamachy mające na celu włamanie się do systemu teleinformatycznego co do zasady są popełniane całkowicie na odległość. Sprawcy takich działań najczęściej nie mają w ogóle kontaktu z ofiarą oraz przebywają w innym miejscu aniżeli miejsce położenia nośnika systemu informatycznego, do którego się włamują. W związku z powyższym można odnieść wrażenie, że wobec braku bezpośredniego kontaktu sprawcy z ofiarą nie ma ona możliwości działania w obronie koniecznej. Wbrew pozorom, w określonych sytuacjach istnieje jednak możliwość działania ofiary w obronie koniecznej przeciwko takiemu zamachowi.

Podkreślenia wymaga także, że również osoby trzecie mogą bronić dobra prawne ofiary w ramach pomocy koniecznej. Wówczas zastosowanie znajdują rozważania poczynione w rozdziale nr 3 niniejszego opracowania.

IV.I. Zwrotne zainfekowanie urządzenia sprawcy złośliwym oprogramowaniem za pośrednictwem *honeypot*

Dla dalszych rozważań kluczowe znaczenie będzie miało pojęcie *honeypot*. Jest ono używane dla określenia oprogramowania informatycznego lub wydzielonej sieci informatycznej stworzonej po to, aby na niej skupiały się ataki hackerskie[16]. Zasadniczym zadaniem *honeypot* jest wykrywanie i zbieranie danych na temat ataków hackerskich i złośliwego oprogramowania do nich wykorzystywanego, celem zwiększenia efektywności zabezpieczeń sieci informatycznej[17]. Przy wyżej opisanym standardowym wykorzystaniu *honeypot* posługiwanie się nim nie stanowi obrony koniecznej, gdyż nie są naruszane żadne dobra prawne sprawcy ataku hackerskiego oraz nie

16 P. Sokol, J. Míšek, M. Husák, *Honeypots and honeynets: issues of privacy*, „EURASIP Journal on Information Security" 2017/4, s. 1; tak też: F,.Arunanto, A. Baihaqi, S. Djanali, B.A. Pratomo, A.M. Shiddiqi, H. Studiawan, *Aggressive Web Application Honeypot for Exposing Attacker's Identity*, „1st: International Conference on Information Technology, Computer and Electrical Engineering (ICITACEE)", Institut Teknologi Sepuluh Nopember, 8.11.2014 r., s. 211 oraz L. Spitzner, *Honeypots: Tracking Hackers*, Boston 2002, s. 23.

17 D. Zielinski, H.A. Kholidy, *An Analysis of Honeypots and their Impact as a Cyber Deception Tactic*, https://arxiv.org/abs/2301.00045 (dostęp: 19.08.2024 r.).

 DOI: 10.54383/0031-0344.2025.10.5

realizuje to znamion żadnego czynu zabronionego. Warunkiem działania w ramach kontratypu jest bowiem bezprawność czynu, który ma zostać zalegalizowany[18], gdyż nie można wtórnie zalegalizować czynu, który jest już pierwotnie legalny.

W literaturze przedmiotu wskazano jednak także na inne możliwe zastosowanie *honeypot*, które można rozważać w kontekście kontratypu obrony koniecznej. W 2013 r. Alexey Sintsov przeprowadził eksperyment, w którym został stworzony *honeypot* infekujący zwrotnie urządzenie, z którego przeprowadzany był atak hackerski, instalując na nim *backdoor19* wykradający z niego dane umożliwiające jego identyfikację[20]. Autor eksperymentu zaznaczył także, że przy wykorzystaniu omawianego *backdoor* instalowanego przez *honeypot* możliwe jest także uzyskanie z zainfekowanego zwrotnie urządzenia takich danych jak: pliki z dysku twardego, pliki konfiguracyjne, obrazy, dokumenty, geolokalizacja atakującego, informacje o konfiguracji sieci, a nadto możliwe jest uruchomienie śledzenia trasy oraz tworzenie nagrań audio/wideo[21]. W kontekście dalszych rozważań odnotować należy, że możliwe jest także zainstalowanie przez taki *honeypot* na urządzeniu sprawcy innych oprogramowań, np. takich, które uszkodzą lub zniszczą urządzenie sprawcy ataku hackerskiego, uniemożliwiając mu dalsze atakowanie danego systemu teleinformatycznego.

Rozpatrując taką sytuację z punktu widzenia zaistnienia przesłanek warunkujących działanie w obronie koniecznej, wskazać należy, że sprawca narusza dobra prawne ofiary poprzez np. niszczenie należących do niej danych informatycznych, zakłócenie pracy należącego do niej systemu informatycznego lub naruszenie jej prywatności. Sprawca tym samym realizuje znamiona jednego z czynów zabronionych określonych w rozdziale XXXIII Kodeksu karnego (przestępstwa przeciwko ochronie informacji), a więc – przy braku zaistnienia okoliczności wyłączających bezprawność czynu – popełnia on bezprawny zamach. Zamach ten jest jednocześnie bezpośredni, o ile trwa on w chwili podejmowania działań obronnych lub z zachowania napastnika w konkretnej sytuacji jednoznacznie można wywnioskować, że przystępuje on do ataku oraz że istnieje wysoki stopień prawdopodobieństwa natychmiastowego ataku na dobro[22]. W kontekście hackingu przyjąć należy, że bezpośredni zamach zaczyna się w momencie zainfekowania atakowanego urządzenia, gdyż już wtedy sprawca

18 W. Wolter, *O kontratypach i braku społecznej szkodliwości czynu*, „Państwo i Prawo" 1963/10 (212), s. 505 i n.; W. Wolter, *Nauka o przestępstwie*, Warszawa 1973, s. 163, tak też A. Zoll, *Okoliczności wyłączające bezprawność czynu. Zagadnienia ogólne*, Warszawa 1982, s. 101.

19 *Backdoor* to ukryty, nieudokumentowany mechanizm dostępu do systemów komputerowych, umożliwiający nieautoryzowanym podmiotom zdalną kontrolę, obejście zabezpieczeń i wykonywanie działań. Służy on do kradzieży danych, sabotażu i innych nieautoryzowanych aktywności, https://www.comcert.pl/slownik/backdoor/ (dostęp: 19.08.2024 r.).

20 A. Sintsov, *Honeypot that can bite: Reverse penetration*, https://media.blackhat.com/eu-13/briefings/Sintsov/bh-eu-13-honeypot-sintsov-wp.pdf (dostęp: 19.08.2024 r.).

21 A. Sintsov, *Honeypot*…

22 A. Zoll (w:) *Kodeks karny*…, komentarz do art. 25, teza 19; tak też: wyrok SN z 11.12.1978 r. (II KR 266/78), OSNKW 1979/6, poz. 65 oraz wyrok SA w Katowicach z 16.12.2004 r. (II AKa 420/04), LEX nr 147213.

bezprawnie ingeruje w prawa właścicielskie ofiary zamachu względem jej urządzenia, bez jej zgody.

Analizując w tej sytuacji możliwe działania obronne przy użyciu *honeypot* w ramach kontratypu obrony koniecznej przed *hackingiem* i innymi bezprawnymi zamachami polegającymi na włamaniu się do systemu teleinformatycznego, trzeba zwrócić uwagę na to, że wśród warunków odpierania zamachu w ramach obrony koniecznej wyróżnia się głównie: działanie w celu odpierania zamachu, które obiektywnie da się zakwalifikować jako odpieranie zamachu oraz współmierność sposobu obrony do niebezpieczeństwa zamachu. Obrona konieczna nie ma natomiast charakteru subsydiarnego[23], chyba że działanie obronne polega na umyślnym godzeniu w życie napastnika[24].

Powyższe warunki spełnia działanie polegające na zainstalowaniu na urządzeniu sprawcy oprogramowania czyniącego je niezdatnym do dalszego przechwytywania danych z atakowanego systemu teleinformatycznego lub nawet niszczącego je. Takie działanie obronne niewątpliwie stanowi odpieranie zamachu i jest też podejmowane w tym celu. Sposób obrony jest zaś współmierny do niebezpieczeństwa zamachu, gdyż – jak się wydaje – jest to najmniej dotkliwa dostępna forma obrony koniecznej przed tego typu zamachem. Jego ofiara swym działaniem nie wkracza bowiem w sferę cielesną napastnika, a jedynie uszkadza lub niszczy urządzenie służące do zamachu. Powyższe działanie obronne charakteryzuje się także społeczną opłacalnością, gdyż uszkadzając lub niszcząc urządzenie służące do popełnienia hackingu, uniemożliwia się lub co najmniej ogranicza się możliwość zaatakowania innych systemów informatycznych przez sprawcę zamachu.

Zaznaczyć trzeba także, że co do zasady *honeypot* działa na zasadzie automatyzmu, tj. gdy wykryje atak, podejmuje określone akcje w zależności od tego, w jaki sposób został zaprogramowany. Należy zatem w tej sytuacji rozstrzygnąć, jaki wpływ na możliwość powołania się na kontratyp obrony koniecznej ma fakt, że zamach jest odpierany przez oprogramowanie działające na zasadzie automatyzmu. W literaturze kwestia możliwości instalowania zabezpieczeń mających na celu odpieranie przyszłych bezprawnych zamachów poprzez naruszenie dóbr prawnych potencjalnego napastnika jest sporna.

23 Wyrok SN z 31.10.1973 r. (II KR 139/73), OSNKW 1974/4, poz. 61; wyrok SN z 4.02.1972 r. (IV KR 337/71), OSNKW 1972/5, poz. 83; A. Krukowski, *Obrona konieczna na tle Polskiego prawa karnego*, Warszawa 1965, s. 70; A. Marek, *Obrona konieczna w prawie karnym. Teoria i orzecznictwo*, Warszawa 2008, s. 77; T. Jankowiak, *Granice obrony*…, s. 82.

24 Zob. art. 2 ust. 2 pkt 1 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności sporządzonej w Rzymie dnia 4.11.1950 r., zmienionej następnie Protokołami nr 3, 5 i 8 oraz uzupełnionej Protokołem nr 2 (Dz.U. z 1993 r. nr 61 poz. 284 z późn. zm.).

 DOI: 10.54383/0031-0344.2025.10.5

Przeciw możliwości instalowania tego typu zabezpieczeń opowiadają się: Jacek Giezek[25], Andrzej Marek[26], Kazimierz Buchała[27], Wincenty Grzeszczyk[28] oraz Jacek Satko[29]. Także Andrzej Zoll opowiadał się przeciwko[30] możliwości instalowania w ramach obrony koniecznej takich zabezpieczeń, lecz w nowszych opracowaniach przyjmuje on pogląd aprobujący możliwość takiego działania[31]. Za taką możliwością opowiadają się zaś: Władysław Wolter[32], Andrzej Wąsek[33], Adam Krukowski[34], Paweł Daniluk[35], Marek Mozgawa[36], Jacek Błachut[37], Jarosław Wawrowski[38] oraz Marek Derlatka[39].

Przeciwnicy możliwości instalowania w ramach obrony koniecznej zabezpieczeń, które w sposób automatyczny odpierają przyszłe bezprawne zamachy, podnoszą, że w takich sytuacjach nie ma mowy o obronie koniecznej. Ich zdaniem wynika to z faktu, iż nie ma wówczas jeszcze zamachu[40], a zagrożenie dobra chronionego prawem jest jedynie potencjalne, a nie bezpośrednie[41].

Jak się wydaje, powyższe wypowiedzi odnoszą się jednak do samej czynności instalowania zabezpieczeń, pomijając kwestię ich zastosowania. Jakkolwiek bowiem samo instalowanie tego typu zabezpieczeń co do zasady nie stanowi działania w obronie koniecznej – wobec braku bezpośredniego zamachu w tym momencie[42] – to ich zadziałanie w odpowiedzi na bezprawny zamach należy ocenić odmiennie. Konieczne jest tu jednoznaczne rozdzielenie czynności zainstalowania zabezpieczenia od jego zadziałania. Powyższe rozróżnienie powinno doprowadzić do wniosku

25 J. Giezek (w:) *Kodeks karny*…, red. J. Giezek, komentarz do art. 25 teza 7 oraz J. Giezek, *Okoliczności wyłączające bezprawność (kontratypy)* (w:) *Prawo karne*…, red. T. Bojarski, s. 173.

26 A. Marek (w:) *Kodeks karny. Komentarz*, red. A. Marek, Warszawa 2010, komentarz do art. 25, teza 19; A. Marek, *Obrona konieczna*…, s. 55-56 oraz A. Marek, J. Satko, *Okoliczności wyłączające bezprawność czynu. Przegląd problematyki. Orzecznictwo (SN 1918-99). Piśmiennictwo*, Zakamycze 2000, s. 20.

27 K. Buchała, A. Zoll, *Polskie prawo karne*, Warszawa 1995, s. 206–207.

28 W. Grzeszczyk, *Zamach uzasadniający prawo do obrony koniecznej*, „Prokuratura i Prawo" 2000/5, s. 129–130.

29 A. Marek, J. Satko, *Okoliczności wyłączające*…, s. 20.

30 K. Buchała, A. Zoll, *Polskie*…, s. 206–207.

31 Zob. A. Zoll (w:) *Kodeks karny*…, komentarz do art. 25, teza 23.

32 W. Wolter, *Nauka*…, s. 169.

33 A. Wąsek, *Kodeks karny. Komentarz, t. 1, (art. 1–31)*, Gdańsk 1999, teza 16, s. 301–303.

34 A. Krukowski, *Obrona konieczna*…, s. 39–40.

35 P. Daniluk (w:) *Kodeks karny. Komentarz*, red. R.A. Stefański, Warszawa 2023, komentarz do art. 25, nb. 26.

36 M. Mozgawa (w:) *Kodeks karny*…, komentarz do art. 25, teza 8 oraz M. Mozgawa, *Obrona konieczna w polskim prawie karnym (zagadnienia podstawowe)*, „Annales Universitatis Mariae Curie-Skłodowska, *sectio* G (*Ius*)" 2013/2, s. 179–180.

37 J. Błachut, *Wybrane problemy stosowania instytucji obrony koniecznej w prawie karnym*, „Monitor Prawniczy" 2005/4, s. 190–195.

38 J. Wawrowski, *Obrona konieczna a zabezpieczenia techniczne*, „Prokuratura i Prawo" 2006/9, s. 33–46.

39 M. Derlatka, *Glosa do postanowienia SN z dnia 1 lutego 2006 r., V KK 238/05*, „Palestra" 2007/1–2, s. 300.

40 J. Giezek (w:) *Kodeks karny*…, red. J. Giezek, komentarz do art. 25 teza 7 oraz J. Giezek, *Okoliczności wyłączające*…, s. 173; podobnie: A. Marek (w:) *Kodeks karny*…, komentarz do art. 25, teza 19; A. Marek, *Obrona konieczna*…, s. 55–56 oraz K. Buchała, A. Zoll, *Polskie*…, s. 206–207.

41 W. Grzeszczyk, *Zamach uzasadniający*…, s. 129–130.

42 Tak też: P. Daniluk (w:) *Kodeks karny*…, komentarz do art. 25, nb. 26.

aprobującego możliwość przyjęcia kontratypu obrony koniecznej w przypadku odparcia bezpośredniego zamachu przez wykorzystanie urządzenia działającego automatycznie.

Odnotowania wymaga także to, że art. 25 Kodeksu karnego nie nakłada obowiązku osobistego uczestnictwa w działaniu obronnym, a w momencie odpierania zamachu za pomocą zainstalowanego w tym celu urządzenia zostają spełnione wszystkie warunki upoważniające do działania w obronie koniecznej, tj. wystąpienie bezpośredniego i bezprawnego zamachu na jakiekolwiek dobro chronione prawem[43]. Nie można zatem różnicować sytuacji prawnej ofiary zamachu w zależności od tego, czy to ona uruchomiła działanie zabezpieczenia, czy zostało ono uruchomione automatycznie w reakcji na bezprawny zamach. Za Markiem Derlatką stwierdzić należy bowiem, że nie można doprowadzić do takiej sytuacji, w której „prawo" sprawcy zamachu do zaatakowania ofiary jest postawione nad prawem ofiary do spokojnego korzystania ze swych dóbr prawnych[44].

Część autorów także uzależnia możliwość obrony poprzez zastosowanie opisanych wyżej automatycznych zabezpieczeń od ostrzeżenia sprawcy o ich zainstalowaniu[45]. Właściwy jest jednak pogląd odmienny, niewymagający ostrzegania sprawcy przed istniejącym zabezpieczeniem[46], gdyż takie ostrzeżenie zmniejszy lub całkowicie zniweluje jego skuteczność. Przykładowo w przypadku obrony koniecznej przed hackingiem poprzez zwrotne zainfekowanie urządzenia sprawcy, ostrzeżenie sprawcy o zabezpieczeniach sprawi, że będzie on świadom zaistnienia ataku zwrotnego, co zaś może doprowadzić do jego odparcia, przy jednoczesnym kontynuowaniu przez sprawcę pierwotnego zamachu. Wskazać należy przy tym, że w przypadku działania w obronie koniecznej bez użycia automatycznych zabezpieczeń nie wymaga się ostrzegania sprawcy o podjęciu działań obronnych[47]. Raz jeszcze podkreślić trzeba zatem, że wobec braku regulacji ustawowej w tym zakresie, nie można różnicować sytuacji ofiar zamachu w zależności od tego, czy używają samodzielnie narzędzia służącego do obrony, czy to samo narzędzie uruchamia się automatycznie.

Stwierdzić należy więc, że tak samo, jak dopuszczalna jest obrona konieczna za pośrednictwem *honeypot* infekującego zwrotnie urządzenie służące do przeprowadzenia zamachu i powodującego w ten sposób jego zniszczenie lub uszkodzenie wówczas, gdy powyższe czyni człowiek, tak i jest dopuszczalna taka obrona wówczas, gdy infekcja zwrotna i tym samym zniszczenie lub uszkodzenie urządzenia napastnika następuje

43 J. Wawrowski, *Obrona konieczna*…, s. 37.

44 M. Derlatka, *Glosa*…, s. 300.

45 A. Zoll (w:) *Kodeks karny*…, komentarz do art. 25, teza 23; A. Krukowski, *Obrona konieczna*…, s. 39-40; M. Derlatka, *Glosa*…, s. 300; A. Wąsek, *Kodeks karny*…, teza 16, s. 302 oraz W. Wolter, *Nauka*…, s. 169.

46 Taki pogląd prezentują: M. Mozgawa (w:) *Kodeks karny*…, komentarz do art. 25, teza 8 oraz M. Mozgawa, *Obrona konieczna*…, s. 180 (przypis nr 51 *in medio*); J. Wawrowski, *Obrona konieczna*…, s. 40; wyrok SN z 20.02.1979 r. (III KR 20/79), LEX nr 21800.

47 Wyrok SN z 20.02.1979 r. (III KR 20/79), LEX nr 21800.

 DOI: 10.54383/0031-0344.2025.10.5

automatycznie. Od ofiary zamachu nie można natomiast wymagać ostrzegania sprawcy o zabezpieczeniach, których ona używa, gdyż zniweluje to ich skuteczność.

IV.II. Pozyskiwanie informacji na temat sprawcy a obrona konieczna

Wracając do opisanego wyżej eksperymentu przeprowadzonego przez Alexeya Sintsova, należy zaznaczyć, że zainstalowanie przez *honeypot* na urządzeniu sprawcy zamachu oprogramowania zbierającego informacje na jego temat (np. w celu przekazania ich organom ścigania) i ich przechwycenie nie będzie działaniem w obronie koniecznej. Nie jest to bowiem działanie mające na celu odparcie zamachu. W aktualnie obowiązującym stanie prawnym dozwolone jest zatem działanie polegające na zniszczeniu urządzenia, z którego dokonywany jest atak hackerski, ale czynem zabronionym jest pozyskanie z tego urządzenia – za pośrednictwem złośliwego oprogramowania – danych umożliwiających identyfikację lokalizacji lub tożsamości sprawcy zamachu (gdyż może to realizować znamiona czynu zabronionego stypizowanego w art. 267 § 1 Kodeksu karnego).

Powyżej opisana sytuacja jest o tyle niepożądana, że dozwolone jest działanie naruszające dobra prawne sprawcy zamachu, poprzez zniszczenie lub uszkodzenie jego mienia (gdyż jest to wówczas działanie w obronie koniecznej, stanowiące odpieranie bezprawnego zamachu, o ile zostaną spełnione wszelkie powyżej wskazane znamiona kontratypu obrony koniecznej), a jedynie pobranie danych z urządzenia sprawcy, np. w celu przekazania ich organom ścigania, stanowi czyn zabroniony, mimo że jego dolegliwość dla sprawcy zamachu – pod względem naruszenia jego dóbr prawnych – jest mniejsza.

IV.III. Propozycja ustanowienia nowego kontratypu

W tej sytuacji właściwe wydaje się zgłoszenie postulatu *de lege ferenda* w zakresie utworzenia nowego kontratypu, który w takich sytuacjach da ofierze zamachu w postaci przestępstwa polegającego na włamaniu się do systemu teleinformatycznego możliwość legalnego pozyskania danych jego sprawcy w celu przekazania ich Policji, Prokuraturze lub organom, o których mowa w art. 312 Kodeksu postępowania karnego, do skutecznego dochodzenia swoich praw w toku postępowania karnego.

Proponuję, aby powyższy nowy kontratyp został dodany jako art. 267 § 6 Kodeksu karnego o następującym brzmieniu:

Nie popełnia przestępstwa określonego w § 1–4, kto w celu ustalenia tożsamości sprawcy przestępstwa określonego w § 1–3, art. 268 § 2 w związku z § 1, art. 268a § 1 lub § 2 w zw. z § 1, art. 269a, art. 287 § 1 lub § 2 w związku z § 1, art. 294 § 1 w związku z art. 287 § 1, art. 294 § 3 w związku z art. 287 § 1 lub art. 294 § 4 w związku

DOI: 10.54383/0031-0344.2025.10.5

z art. 287 § 1 popełnionego na jego szkodę, uzyskuje dostęp do informacji zawartej w systemie informatycznym, za pośrednictwem którego zostało popełnione powyższe przestępstwo, w trakcie jego popełniania albo bezpośrednio po jego popełnieniu i wyłącznie w celu przekazania informacji Prokuraturze, Policji lub organom, o których mowa w art. 312 ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz. U. z 2025 r. poz. 46 i 304).

Dodanie niniejszego kontratypu w art. 267 § 6 Kodeksu karnego nie powinno budzić większych wątpliwości, biorąc pod uwagę fakt, że kontratyp ten legalizuje czyny zabronione ustanowione w art. 267 § 1–4 Kodeksu karnego. Powyższa konstrukcja przepisu jest także prawidłowa z punktu widzenia Działu I Rozdziału 9 Załącznika do Rozporządzenia Prezesa Rady Ministrów z dnia 20.06.2002 r. w sprawie „Zasad techniki prawodawczej" (t.j. Dz.U. z 2016 r. poz. 283), który reguluje zasady konstruowania przepisów prawnokarnych.

Uzasadniając brzmienie przepisu, zaznaczyć należy, że w porównaniu do art. 25 Kodeksu karnego jego zakres jest węższy. Wśród jego znamion nie ma bezprawnego zamachu, a są enumeratywnie wymienione przestępstwa, które charakteryzują się tym, że można je popełnić poprzez włamanie do systemu teleinformatycznego. Niniejszy kontratyp nie obejmuje bezprawnych zamachów niestanowiących przestępstwa, gdyż wśród znamion strony podmiotowej tego kontratypu znajduje się cel przekazania informacji Policji, Prokuraturze lub organom, o których mowa w art. 312 Kodeksu postępowania karnego, co ma wartość praktyczną wyłącznie w przypadku przestępstw.

W zakresie celowości dodania niniejszego kontratypu do polskiego systemu prawa karnego odesłać należy do poczynionych już uwag na temat tego, że w polskim prawie karnym dopuszczalna jest sytuacja, w której ofiara zamachu zniszczy lub uszkodzi urządzenie sprawcy zamachu polegającego na włamaniu się do systemu teleinformatycznego, ale jeśli ta sama ofiara zamachu jedynie pozyska informacje na jego temat, w celu przekazania ich organom ścigania, może wówczas ponieść odpowiedzialność karną za czyn zabroniony określony w art. 267 § 1 Kodeksu karnego. W aktualnym stanie prawnym można ponieść odpowiedzialność karną za mniejsze naruszenie dóbr prawnych sprawcy zamachu (poprzez uzyskanie informacji na jego temat), podczas gdy tej odpowiedzialności nie ponosi się w przypadku bardziej intensywnego wkroczenia w jego dobra prawne (poprzez zniszczenie lub uszkodzenie narzędzia służącego do przeprowadzenia zamachu). Jest to o tyle niepożądane, że niecelowe jest karanie obywateli za podjęcie działania mniej naruszającego dobra prawne sprawcy zamachu, podczas gdy mieli możliwość podjęcia działania bardziej godzącego w dobra prawne sprawcy. Ustanowienie proponowanego kontratypu wyeliminuje powyższą niepożądaną sytuację.

Wskazać należy także, że co do zasady brak negatywnej oceny – i tym samym wyłączenie bezprawności – zachowania podjętego w sytuacji kontratypowej wynika

 DOI: 10.54383/0031-0344.2025.10.5

z bilansu zysków i strat[48]. Wyłączenie bezprawności czynu realizującego znamiona niniejszego kontratypu charakteryzuje się zaś opłacalnością społeczną. W pierwszej kolejności odnotować trzeba, że ustanowienie niniejszego kontratypu może pozytywnie wpłynąć na wykrywalność przestępstw internetowych. Niewątpliwie natychmiastowe pozyskanie informacji na temat sprawcy za pośrednictwem oprogramowania zainstalowanego na jego urządzeniu przez *honeypot* będzie skuteczniejszą formą ustalenia danych sprawcy przestępstwa niż pozyskiwanie ich przez organy ścigania, gdy bezprawny zamach już się zakończy. Jest to o tyle ważne, że wedle opublikowanych w 2022 r. wyników badań sondażowych przeprowadzonych przez Najwyższą Izbę Kontroli, 85% przypadków spraw prowadzonych przez organy ścigania dotyczących przestępstw internetowych nie zostało wyjaśnionych (78% respondentów wskazało, że ich sprawa zakończyła się „niczym", w przypadku 3% respondentów było to umorzenie postępowania, kolejne 4% respondentów wskazało, że sprawa zakończyła się tym, że stracili pieniądze lub dane przechowywane na urządzeniu), jedynie w przypadku 1% respondentów sprawa zakończyła się wykryciem i skazaniem sprawcy, kolejne 1% respondentów poinformowało, że zostały odzyskane środki, ale nie wykryto i nie skazano sprawcy. W przypadku pozostałych respondentów sprawa się jeszcze nie zakończyła w chwili prowadzenia badań albo wybrali oni odpowiedź „nie wiem/trudno powiedzieć"[49]. Wskazana wykrywalność przestępstw w przypadku 1%, w porównaniu do ogólnej wykrywalności przestępstw stwierdzonych wynoszącej 71,1%[50], jest niska, co niewątpliwie stanowi jeden z elementów wpływających na atrakcyjność przestępstw tego typu.

Wykrycie sprawcy przestępstwa może w takiej sytuacji poskutkować zakończeniem jego działalności, co również wskazuje na opłacalność społeczną zachowania podjętego w ramach proponowanego kontratypu.

Stosunek proponowanego kontratypu do obrony koniecznej byłby podobny jak stosunek do niej obywatelskiego ujęcia uregulowanego w art. 243 Kodeksu postępowania karnego. Tak jak możliwość dokonania obywatelskiego ujęcia nie wyłącza ofierze zamachu prawa do obrony koniecznej, tak też nie wyłączałaby tego prawa możliwość pozyskania informacji na temat sprawcy zamachu w ramach proponowanego kontratypu. Kontratyp z zasady kreuje bowiem uprawnienie, a nie obowiązek prawny.

48 J. Giezek, *Rozdział III uwagi wprowadzające* (w:) *Kodeks karny*…, red. J. Giezek, teza 3.

49 Najwyższa Izba Kontroli, *Działania Państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości*, s. 48, https://www.nik.gov.pl/plik/id,27206,vp,30013.pdf (dostęp: 19.08.2024 r.).

50 Główny Urząd Statystyczny, *Wskaźnik wykrywalności sprawców przestępstw stwierdzonych za rok 2022*, https://bdl.stat.gov.pl/bdl/dane/podgrup/tablica (dostęp: 19.08.2024 r.).

V. Podsumowanie

Konkludując powyższe rozważania, należałoby stwierdzić, że ofiara bezprawnego zamachu stanowiącego przestępstwo internetowe popełniane niecałkowicie na odległość może uszkodzić lub zniszczyć rzecz służącą sprawcy zamachu do jego popełnienia.

W przypadku zaś obrony koniecznej przed przestępstwami internetowymi popełnianymi całkowicie na odległość dobra prawne ofiary chronić mogą osoby trzecie, odpierając zamach w ramach pomocy koniecznej. Sama ofiara w takich sytuacjach – w przypadku zamachu polegającego na włamaniu się do systemu informatycznego – może za pośrednictwem oprogramowania *honeypot* zwrotnie zainfekować urządzenie sprawcy celem jego uszkodzenia lub zniszczenia i tym samym odparcia zamachu. Działaniem w obronie koniecznej nie będzie natomiast pozyskanie informacji na temat sprawcy zamachu z zainfekowanego zwrotnie urządzenia, gdyż nie służy to odpieraniu zamachu. Ze względów celowościowych postulować należy dodanie do k.k. kontratypu mającego na celu zalegalizowanie takiego działania.

Tomasz Jankowiak

Student prawa na Wydziale Prawa i Administracji Uniwersytetu im. Adama Mickiewicza w Poznaniu

A student at the Faculty of Law and Administration of the Adam Mickiewicz University in Poznań.

ORCiD: 0000-0003-1025-2132

Abstract

Keywords: *unlawfulness, necessity defence, circumstances excluding the unlawfulness of an act, lawful excuses (justification), Internet crimes*

On necessity defence in respect of Internet crimes

The subject of the research discussed in this article is the issue of – so far neglected – necessity defence in respect of Internet crimes committed remotely, particularly hacking. In the publication, the author, using a dogmatic-legal me-

 DOI: 10.54383/0031-0344.2025.10.5

thod, analyses, among other things, possible actions aimed at defence against an Internet crime when the victim has direct contact with the attacker and the possibility of a necessity defence in the context of preventing a hacking attack with the use of honeypot software. The author also provides a lex ferenda proposal for the introduction of a new lawful excuse in the special part of the Criminal Code.

Bibliografia

1. **Adamski Andrzej,** *Karalność hackingu*, „Przegląd Sądowy" 1998/11–12
2. **Adamski Andrzej,** *Prawo karne komputerowe*, Warszawa 2000
3. **Arunanto Fx, Baihaqi Abdurrazak, Djanali Supeno, Pratomo Baskoro Adi, Studiawan Hudan, Shiddiqi Ary Mazharuddin,** *Aggressive Web Application Honeypot for Exposing Attacker's Identity*, „1st: International Conference on Information Technology, Computer and Electrical Engineering (ICITACEE)", Institut Teknologi Sepuluh Nopember, 8.11.2014 r.
4. **Błachut Jacek,** *Wybrane problemy stosowania instytucji obrony koniecznej w prawie karnym*, „Monitor Prawniczy" 2005/4
5. **Buchała Kazimierz, Zoll Andrzej,** *Polskie prawo karne*, Warszawa 1995
6. **Chaładyniak Dariusz,** *Wybrane zagadnienia bezpieczeństwa danych w sieciach komputerowych*, „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki" 2015/13
7. **Daniluk Paweł** (w:) *Kodeks karny. Komentarz*, red. R. Stefański, Warszawa 2023
8. **Derlatka Marek,** *Glosa do postanowienia SN z dnia 1 lutego 2006 r., V KK 238/05*, „Palestra" 2007/1–2
9. **Długosz-Jóźwiak Joanna** (w:) *Kodeks karny. Część szczególna. Komentarz do artykułów 117–221, tom I*, red. M. Królikowski, R. Zawłocki, Warszawa 2023
10. **Fołta Tomasz, Mucha Andrzej,** *Zniesławienie i znieważenie w Internecie*, „Prokuratura i Prawo" 2006/11
11. **Giezek Jacek** (w:) *Kodeks karny. Część szczególna. Komentarz*, red. J. Giezek, Warszawa 2021
12. **Giezek Jacek** (w:) *Prawo karne materialne. Część ogólna i szczególna*, red. M. Bojarski, Warszawa 2023
13. Główny Urząd Statystyczny, *Wskaźnik wykrywalności sprawców przestępstw stwierdzonych za rok 2022*, https://bdl.stat.gov.pl/bdl/dane/podgrup/tablica (dostęp: 19.08.2024 r.).
14. **Grzeszczyk Wincenty,** *Zamach uzasadniający prawo do obrony koniecznej*, „Prokuratura i Prawo" 2000/5
15. **Husák Martin, Míšek Jakub, Sokol Pavel,** *Honeypots and honeynets: issues of privacy*, „EURASIP Journal on Information Security" 2017/4

DOI: 10.54383/0031-0344.2025.10.5

16. **Jankowiak Tomasz,** *Granice obrony koniecznej przed przemocą psychiczną w ramach instytucji obrony koniecznej*, „Palestra" 2023/10 (791)
17. **Kholidy Hisham, Zielinski Daniel,** *An Analysis of Honeypots and their Impact as a Cyber Deception Tactic*, https://arxiv.org/abs/2301.00045 (dostęp: 19.08.2024 r.)
18. **Kozłowska-Kalisz Patrycja** (w:) *Kodeks karny. Komentarz aktualizowany*, red. M. Mozgawa, LEX 2024
19. **Krukowski Adam,** *Obrona konieczna na tle polskiego prawa karnego*, Warszawa 1965
20. **Kulesza Witold,** *Rozdział VI. Przestępstwa przeciwko czci i nietykalności cielesnej* (w:) *System Prawa Karnego. Przestępstwa przeciwko dobrom indywidualnym, tom X*, red. J. Warylewski, Warszawa 2016
21. **Marek Andrzej,** *Obrona konieczna w prawie karnym. Teoria i orzecznictwo*, Warszawa 2008
22. **Marek Andrzej, Satko Jacek,** *Okoliczności wyłączające bezprawność czynu. Przegląd problematyki. Orzecznictwo (SN 1918-99). Piśmiennictwo*, Zakamycze 2000
23. **Marek Andrzej** (w:) *Kodeks karny. Komentarz*, red. A. Marek, Warszawa 2010
24. **Michalecki Daniel,** *Przestępstwa internetowe – zapobieganie i zwalczanie*, „Kontrola Państwowa" 2023/5
25. **Mozgawa Marek,** *Obrona konieczna w polskim prawie karnym (zagadnienia podstawowe)*, „Annales Universitatis Mariae Curie-Skłodowska, sectio G (Ius)" 2013/2
26. **Mozgawa Marek** (w:) *Kodeks karny. Komentarz aktualizowany*, red. M. Mozgawa, LEX 2024
27. **Muszyńska Anna** (w:) *Kodeks karny. Część szczególna. Komentarz*, red. J. Giezek, Warszawa 2021
28. Najwyższa Izba Kontroli, *Działania Państwa w zakresie zapobiegnia i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości*, s. 48, https://www.nik.gov.pl/plik/id,27206,vp,30013.pdf (dostęp: 19.08.2024 r.).
29. **Paprzycki Lech Krzysztof** (w:) *Komentarz aktualizowany do art. 1–424 Kodeksu postępowania karnego*, red. L. K. Paprzycki, LEX 2015
30. **Piórkowska-Flieger Joanna** (w:) *Kodeks karny. Komentarz*, red. T. Bojarski, Warszawa 2016
31. **Radoniewicz Filip,** *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016
32. **Raglewski Janusz** (w:) *Kodeks karny. Część szczególna. Tom II. Część II. Komentarz do art. 212–277d*, red. W. Wróbel, A. Zoll, Warszawa 2017
33. **Sintsov Alexey,** *Honeypot that can bite: Reverse penetration*, https://media.blackhat.com/eu-13/briefings/Sintsov/bh-eu-13-honeypot-sintsov-wp.pdf (dostęp: 19.08.2024 r.).
34. **Smardzewski Waldemar,** *Z problematyki ujęcia na gorącym uczynku*, „Nowe Prawo" 1980/3
35. **Sowa Michał,** *Ogólna charakterystyka przestępczości internetowej*, „Palestra" 2001/5–6 (521–522)
36. **Spitzner Lance**, *Honeypots: Tracking Hackers*, Boston 2002
37. **Stefański Ryszard Andrzej, Zabłocki Stanisław** (w:) *Kodeks postępowania karnego. Tom II. Komentarz do art. 167–296*, red. R. Stefański, S. Zabłocki, Warszawa 2019

 DOI: 10.54383/0031-0344.2025.10.5

38. **Surkont Mirosław,** *Problem skutkowego charakteru zniesławienia*, „Palestra" 1978/4 (244)
39. **Wawrowski Jarosław,** *Obrona konieczna a zabezpieczenia techniczne*, „Prokuratura i Prawo" 2006/9
40. **Wąsek Andrzej,** *Kodeks karny. Komentarz, t. 1 (art. 1–31)*, Gdańsk 1999
41. **Wolter Władysław,** *Nauka o przestępstwie*, Warszawa 1973
42. **Wolter Władysław,** *O kontratypach i braku społecznej szkodliwości czynu*, „Państwo i Prawo" 1963/10 (212)
43. **Zoll Andrzej,** *Okoliczności wyłączające bezprawność czynu. Zagadnienia ogólne*, Warszawa 1982
44. **Zoll Andrzej** (w:) *Kodeks karny. Część ogólna. Tom I. Część I. Komentarz do art. 1–52*, red. W. Wróbel, A. Zoll, Warszawa 2016

DOI: 10.54383/0031-0344.2025.10.5