ISSN: 2083-5701
e-ISSN: 2545-2568
GICID: 71.0000.1500.1589

MEDIA I SPOŁECZEŃSTWO
MEDIOZNAWSTWO • KOMUNIKOLOGIA • SEMIOLOGIA • SOCJOLOGIA MEDIÓW • MEDIA A PEDAGOGIKA

Nr 14/2021
https://doi.org/10.53052/MiS.2021.14.15

Weronika Stawińska[1]
Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie
ORCID ID: 0000-0002-1495-6615
e-mail: stawinska.weronika@gmail.com

Pandemia a zjawisko cyberprzestępczości

ABSTRAKT

Artykuł koncentruje się na przedstawieniu zjawiska cyberprzestępczości, które niewątpliwie nasiliło się w czasach pandemii COVID-19. Artykuł pokazuje, w jaki sposób przeniesienie poszczególnych aspektów życia na płaszczyznę wirtualną wpłynęło na zmniejszenie poziomu bezpieczeństwa w sieci. Dodatkowo wskazano przykłady działań mających na celu zwiększenie poziomu cyberbezpieczeństwa.

SŁOWA KLUCZOWE: cyberprzestępczość, cyberbezpieczeństwo, pandemia COVID-19

Wprowadzenie

W dobie pandemii COVID-19 internet zaczął być eksploatowany na coraz to nowych płaszczyznach. Zagrożenie, jakie spowodowało na całym świecie rozprzestrzenianie się COVID-19, znalazło niewątpliwie odzwierciedlenie w otaczającej rzeczywistości, w tym rzeczywistości prawnej. Zmianie uległy zarówno przepisy proceduralne, jak i przepisy prawa materialnego. Istotnym jest, że w niektórych przypadkach wprowadzone zmiany legislacyjne mają charakter trwały, bowiem ich czas obowiązywania przekracza czas trwania stanu epidemii. Oprócz zmian w prawie, podczas zagrożenia chorobą COVID-19 zmienił się również sposób ludzkiego postępowania. W zdecydowanej większości przypadków, tam gdzie było to możliwe, zmienił się model pracy: przejście na pracę zdalną, podobnie w przypadku edukacji czy robienia zakupów. Natomiast głównym źródłem informacji, zamiast tradycyjnych mediów jak chociażby gazety, stał się internet i portale informacyjne. Z uwagi na powyższe, dotychczasowe zagrożenia, występujące na tradycyjnych płaszczyznach, przeniosły się na płaszczyznę wirtualną. W takich okolicznościach należy stwierdzić, że wszelka aktywność

[1] Data złożenia tekstu do Redakcji „MiS": 30.01.2021 r.; data zatwierdzenia tekstu do druku: 10.05.2021 r.

podejmowana w cyberprzestrzeni może stać się potencjalnym miejscem występowania cyberprzestępczości.

Niniejszy artykuł ma charakter przeglądowy[2], a postawione pytanie badawcze dotyczy kwestii, czy istniejące regulacje prawne w sposób efektywny chronią społeczeństwo przed cyberprzestępczością. Hipoteza zakłada, że poziom ochrony przewidziany na poziomie legislacyjnym nie jest wystarczający. W celu odpowiedzi na tak sformułowane pytanie badawcze[3], w pierwszej kolejności na podstawie przeglądu piśmiennictwa przedstawiono pojęcie zjawiska cyberprzestępczości, które staje się coraz bardziej powszechne oraz na podstawie konkretnych przykładów opisano, na czym polega cyberprzestępczość. W następnej kolejności, w kontekście pytania badawczego, wskazano regulacje prawne zwalczające powyżej opisany przestępczy proceder. W dalszej części artykułu dokonano przeglądu najnowszych danych opublikowanych w raporcie Interpolu na temat wpływu pandemii na zjawisko cyberprzestępczości. Przeprowadzona analiza dowodzi, że zjawisko cyberprzestępczości niewątpliwie wzrasta, co pozwoliło sformułować wnioski, że wraz z nasilającym się zjawiskiem cyberprzestępczości wzrasta potrzeba bardziej efektywnej walki z cyberprzestępczością. Natomiast w ostatniej części artykułu zaproponowano rozwiązania – w tym o charakterze legislacyjnym, mające zwalczać cyberprzestępczość i prowadzić do wzrostu bezpieczeństwa w sieci.

Potrzeba publikacji w mediach omawianego zagadnienia o charakterze prawno-społecznym wynika z faktu, że społeczeństwo wiedzę o obowiązującym prawie czerpie właśnie z mediów. Pomimo funkcjonowania zasady *ignorantia iuris nocet*– oznaczającej, że nieznajomość prawa szkodzi[4], głównym źródłem wiedzy w społeczeństwie nie są publikowane na stronach rządowych i w Dzienniku Ustaw akty prawne, a właśnie artykuły publikowane w poszczególnych mediach. Niniejsze ukazuje, jak ważną rolę w procesie kształtowania świadomości prawnej społeczeństwa odgrywają artykuły o tematyce prawniczej[5].

Pojęcie cyberprzestępczości

W polskim porządku prawnym, w tym również w Kodeksie karnym[6], nie znajduje się definicja legalna cyberprzestępczości. W takich okolicznościach należy sięgnąć do opracowanej w doktrynie definicji przestępczości z uwzględnieniem

[2] J. Apanowicz, *Metodologia ogólna*, Gdynia 2002, s. 129.

[3] A. Jeszka, *Problemy badawcze i hipotezy w naukach o zarządzaniu*, „Organizacja i kierowanie", 5/2013, s. 31-32.

[4] T. Woś, *Trybunalskie i sądowe stosowanie zasady „ignorantia iuris nocet" na gruncie praktyki orzeczniczej w Polsce*, „Filozofia Publiczna i Edukacja Demokratyczna ", 7/2018, s. 182.

[5] H. Batorowska, R. Klepka, O. Wasiuta, *Media jako instrument wpływu informacyjnego i manipulacji społeczeństwem*, Kraków 2019, s. 7.

[6] Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny, Dz. U. 1997 nr 88 poz. 553.

jego komputerowego wymiaru – przestępstw komputerowych[7]. Pod pojęciem przestępczości rozumie się zatem „zbiór czynów zabronionych przez ustawę pod groźbą kary, które to czyny popełnione zostały na obszarze danej jednostki terytorialnej i w danym czasie”[8]. Natomiast w przypadku cyberprzestępczości będą to czyny zabronione popełnione za pomocą informatycznych sieci elektronicznych oraz systemów informatycznych[9]. Wskazać można również na ujednoliconą definicję cyberprzestępczości, która wskazuje, że jest to „każdy rodzaj działalności niezgodny z normami prawa wewnętrznego lub międzynarodowego, którego skutek przekracza granice państwa, zaś jej narzędzie lub też cel stanowi urządzenie w postaci komputera”[10].

Choć w polskim porządku prawnym funkcjonuje wiele regulacji, chociażby w przedmiocie korzystania z sieci informatycznych, żadna z nich nie odnosi się w sposób kompleksowy do zjawiska cyberprzestępczości. W tym miejscu, dla przykładu, należy wskazać ustawę o świadczeniu usług drogą elektroniczną[11], z tym zastrzeżeniem, że reguluje ona w większości sposób wykonywania usług drogą elektroniczną. Ponadto obowiązuje ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[12], która określa organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu.

Na szczeblu międzynarodowym na uwagę zasługuje natomiast Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r.[13], która odnosi się do poszczególnych czynów zabronionych popełnionych przy użyciu komputera. To właśnie w myśl art. 1 Konwencji każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwo w jej prawie wewnętrznym umyślnego, bezprawnego dostępu do całości lub części systemu teleinformatycznego. W takim stanie prawnym niewątpliwie do skutecznej walki z cyberprzestępczością niezbędne jest odwołanie się do kilku aktów prawnych.

Na samym początku należy wskazać, że zagadnienie cyberprzestępczości to zagadnienie, którego nie należy deprecjonować, nie tylko z uwagi na skalę zjawiska, ale również z uwagi na stopień grożącego niebezpieczeństwa. Jak wynika z raportu Interpolu Cybercrime: COVID-19 Impact, opracowanego na miesiąc sierpień 2020 r.,

[7] J. Wasilewski, *Przestępczość w cyberprzestrzeni – zagadnienia definicyjne*, „Przegląd bezpieczeństwa wewnętrznego”, 15/16, s. 161.

[8] H. Chmielewski, W. Woźniak, *Organiczne i afektywne uwarunkowania przestępczości*, „Łódzkie Studia Teologiczne”, 14/2005, s. 241.

[9] M. Stefanowicz, *Cyberprzestępczość– próba diagnozy zjawiska*, „Kwartalnik Policyjny” 4/2017, s. 20.

[10] W. Konaszczuk, *Legislacyjne rozwiązania w zakresie przeciwdziałania cyberprzestępczości w prawie podatkowym*, Instytut Wymiaru Sprawiedliwości, Warszawa 2018, s. 5.

[11] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz. U. 2002 nr 144 poz. 1204.

[12] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz. U. 2018 poz. 1560.

[13] Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. Dz. U. 2015 poz. 728.

w dobie COVID-19 zdecydowanie wzrosło zjawisko cyberprzestępczości. Zagrożeni pozostają nie tylko prywatni użytkownicy sieci, ale również znaczące przedsiębiorstwa czy podmioty państwowe. Ma to niebagatelne znaczenie, bowiem cyberprzestępczość – o ile zostaje wykryta, skutkuje nie tylko odpowiedzialnością karną i finansową, ale również dotkliwą utratą wizerunku i zaufania klientów[14].

Przykłady i skala cyberprzestępczości

W otaczającej rzeczywistości społeczno-prawnej przestępcy sięgają po coraz bardziej wyrafinowane i zuchwałe metody oszustwa, do których należy chociażby *phishing, maware, ransomware* czy *hacking*.

Phishing jest w istocie złośliwą kradzieżą danych. Wskazana metoda cyberprzestępczości polega na rozsyłaniu sfabrykowanych wiadomości e-mail czy stron internetowych, często stron informacyjnych, które mają skłonić np. do podania danych osobowych czy przekazania środków finansowych – celem jest wyłudzenie ważnych danych (np. dane do logowania lub numer karty kredytowej), są to m.in. wiadomości, które namawiają do *poprawy danych osobowych*. Zdarzają się również wiadomości, w których jest się proszonym o zalogowanie do bankowości elektronicznej za pomocą przesłanego linku, gdyż w przeciwnym razie utraci się możliwość korzystania z niej, konto zostanie zablokowane bądź zamówiona paczka nie zostanie wysłana. W takiej sytuacji cyberprzestępcy podszywają się pod instytucje i witryny darzone zaufaniem (np. urząd lub bank)[15].

Kolejną metodą jest *malware*, czyli złośliwe oprogramowania, które w istocie są aplikacjami o szkodliwym, a zarazem przestępczym oddziaływaniu na użytkownika komputera. Celem takich ataków może być również kradzież danych osobowych, pieniędzy czy poszczególnych kodów dostępu[16].

W praktyce odnotowano również działanie nazywane *ransomware*, polegające na wymuszeniu okupu. Przestępcy blokują użytkownikowi systemu dostęp do niego, a następnie proponują zdjęcie blokady po uiszczeniu odpowiedniej kwoty pieniędzy, za pomocą anonimowych płatności[17].

Dodatkowo wskazuje się na *hacking*, czyli uzyskanie nielegalnego dostępu do systemu bądź nielegalne pozyskanie informacji, poprzez ominięcie zabezpieczeń. W doktrynie podkreśla się, że zgodnie z art. 2 Konwencji Rady Europy o cyberprzestępczości, aby móc pociągnąć sprawcę do odpowiedzialności, musi nastąpić bezprawne uzyskanie dostępu do systemu, więc gdy działania zostaną podjęte przez osobę upoważnioną, niemożliwe będzie pociągnięcie do

[14] Raport Interpolu *Cybercrime: COVID-19 Impact*, Lyon 2020, s. 4-5 (https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19 dostęp na 04.01.2021).
[15] A. Rogowski, *Phishing*, „Kwartalnik Policyjny", 4/2017, s. 56-57.
[16] W. Kamieniecki, *Współtworzymy system cyberbezpieczeństwa Polaków*, „Kwartalnik Policyjny", 4/2017, s. 7.
[17] J. Sordyl, *Ransomware – wymuszenie okupu w sieci*, „Kwartalnik Policyjny", 4/2017, s. 46.

odpowiedzialności za podjęte działania *hackingu*[18].

Należy mieć na uwadze, że cyberprzestępcy obecnie wykorzystują ludzką żądzę informacji i niepokój, jaki niesie pandemia koronawirusa. W takich okolicznościach to właśnie COVID-19 jest wykorzystywany do popełniania przestępczego procederu, poprzez przekierowanie użytkowników sieci na strony internetowe, niejednokrotnie imitujące poszczególne media, portale informacyjne o tematyce COVID-19. W tym zakresie użytkownicy sieci powinni być szczególnie ostrożni, skąd czerpią bieżące informacje i czy przy okazji nie narażają się na cyberataki.

W tym miejscu, dla pokazania skali przestępczego procederu, należy wskazać na opracowane przez Interpol statystyki cyberprzestępczości:

1. aż 59 % wszystkich przypadków stanowią niezamawiane wiadomości elektroniczne, informacje handlowe, potocznie nazywane spamem – oraz metoda – *phishing*. Obydwa z tych przykładów mają najczęściej losowy zasięg, tym samym nie są wymierzone w konkretne osoby;
2. 36 % stanowią przypadki *ransomeware* oraz *malware*;
3. 22 % złośliwe domeny, rzekomo o medialnym, informacyjnym charakterze, często o tematyce związanej z COVID-19;
4. 14 % fałszywe informacje, wykorzystujące ludzką żądzę informacji oraz panującą dezinformację[19].

Ponadto należy mieć na uwadze, że zjawisko cyberprzestępczości nie jest zjawiskiem jednolitym oraz zdecydowanie wykraczającym poza ramy przedstawionych statystyk. Obejmuje ono bowiem również takie kategorie zachowań jak kradzież własności intelektualnej czy cyberstalking. Jest to zatem ogół działań o charakterze przestępczym, mających miejsce w sieci informatycznej.

Cyberstalking – to sformułowanie pochodzące z języka angielskiego oznacza śledzenie i polega na inwigilacji konkretnej osoby drogą elektroniczną, a dodatkowo na nękaniu jej komunikatami, a nawet groźbami o niechcianym charakterze. Dodać należy, że z reguły w tym celu wykorzystywane są media społecznościowe, a ofiara takiego przestępstwa najczęściej nie jest sprawcy zupełnie obca[20].

Regulacje prawne

Odpowiedzią polskiego ustawodawcy na szerzące się przestępstwo *stalkingu* było wprowadzenie dodatkowego typu czynu zabronionego, stypizowanego w art. 190a k.k., zgodnie z którym: kto przez uporczywe nękanie innej osoby lub osoby jej najbliższej wzbudza u niej uzasadnione okolicznościami poczucie zagrożenia,

[18] M. Siwicki, *Cyberprzestępczość*, C. H. Beck, Warszawa 2013, s. 104-107.

[19] Raport Interpolu *Cybercrime: COVID-19 Impact*, Lyon 2020, s. 8 (https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19 (dostęp na 04.01.2021).

[20] J. Pyżalski, *Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży*, Oficyna Wydawnicza „Impuls", Kraków 2012, s. 126-126.

poniżenia lub udręczenia lub istotnie narusza jej prywatność, podlega karze pozbawienia wolności od 6 miesięcy do lat 8. Tej samej karze podlega ten, kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek, inne jej dane osobowe lub inne dane, za pomocą których jest ona publicznie identyfikowana, w celu wyrządzenia jej szkody majątkowej lub osobistej (§ 2). Jeżeli następstwem czynu określonego w § 1 lub 2 jest targnięcie się pokrzywdzonego na własne życie, sprawca podlega karze pozbawienia wolności od lat 2 do 12 (§ 3). Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego (§ 4). Niestety, jak podkreśla się w literaturze przedmiotu, pomimo uregulowania odpowiedzialności karnej za przestępstwo *stalkingu* wciąż istnieje poczucie bezkarności wśród prześladowców, z uwagi na okoliczność, że osoby pokrzywdzone nie zgłaszają popełnienia przestępstwa oraz nie wnoszą o ściganie[21].

Odnośnie do cyberprzestępstw dotyczących kradzieży własności intelektualnej należy natomiast wskazać podstawowe typy przestępstw, uregulowane w kodeksie karnym, takie jak: nielegalne uzyskanie programu komputerowego – art. 278 § 2, przywłaszczenie prawa majątkowego – art. 284, paserstwo programu komputerowego – art. 293 § 3 oraz oszustwo komputerowe – art. 287.

W takich okolicznościach należy stwierdzić, że skoro cyberprzestępczość nie ma charakteru jednolitego, to również walka z cyberprzestępczością charakteryzuje się niejednolitym charakterem. Walka z cyberprzestępczością może polegać między innymi na korzystaniu w trakcie pracy zdalnej z zabezpieczonej sieci vpn, szkoleniu pracowników i informatyków, publikowaniu artykułów w mediach docierających do szerokiego grona odbiorców, ale również na współpracy z organami ścigania. W tym zakresie należy pamiętać, że w Policji funkcjonuje wyodrębnione Biuro do Walki z Cyberprzestępczością, które koordynuje działania prowadzone przez komendy wojewódzkie Policji w zakresie czynności operacyjno-rozpoznawczych. Należy podkreślać, że zagadnienie walki z cyberprzestępczością jest niezmiernie ważne, aby w społeczeństwie przestało pokutować przeświadczenie, zgodnie z którym internet jawi się jako Dziki Zachód, miejsce, w którym prawa nie ma, a jeśli jest – to nie jest ono egzekwowane[22].

Walkę z cyberprzestępczością zdecydowanie wspierają przepisy karne. Regulacje karne penalizujące poszczególne zachowania znajdują się w Kodeksie karnym w przepisach rozdziału XXXIII, zatytułowanego „Przestępstwa przeciwko ochronie informacji". Wśród stypizowanych w części szczegółowej Kodeksu karnego przestępstw wskazuje się na:

[21] M. Cyrklaff-Gorczyca, *Cyberstalking jako forma przemocy z wykorzystaniem technologii informacyjno-komunikacyjnych*, K. Materska, B. Taraszkiewicz (red.), *Ekologia informacji a zasoby informacyjne w bibliotekach i cyberprzestrzeni*, Wydawnictwo upamiętniające 100-rocznicę powstania Stowarzyszenia Bibliotekarzy Polskich, Słupsk 2017, s. 209.

[22] J. Bart, R. Markiewicz, *Internet a prawo*, Towarzystwo Autorów i Wydawców Prac Naukowych UNIVERSITAS, Kraków 1998, s. 9.

- nieuprawnione uzyskanie dostępu do informacji czy systemu informatycznego – art. 267 § 1 i § 2 k.k.;
- nielegalny podsłuch i inwigilację – art. 267 § 3 k.k.;
- ujawnienie nielegalnie pozyskanej informacji – art. 267 § 4 k.k.;
- naruszenie integralności zapisu informacji – art. 268 § 2 i 3 k.k.;
- naruszenie integralności danych informatycznych oraz utrudnianie dostępu do nich – art. 268a § 1 i 2 k.k.;
- zakłócenie pracy systemu komputerowego lub sieci teleinformatycznej – art. 269a k.k.;
- bezprawne wykorzystanie urządzeń, programów i danych – art. 269b § 1 k.k.

W związku z powyższym w literaturze przedmiotu podkreśla się, że wśród cyberprzestępstw wyróżnia się trzy główne kategorie zachowań. Po pierwsze są to przestępstwa będące w istocie oszustwami, które zostały popełnione przy użyciu elektronicznych sieci informatycznych. Po drugie cyberprzestępstwa obejmują udostępnienie, ujawnienie zabronionych treści – mogą to być na przykład treści pornograficzne, czy chociażby nawołujące do nienawiści. Po trzecie są to przestępstwa wymierzone przeciwko sieciom elektronicznym czy to w formie ataków, czy sabotaży[23].

Z uwagi na ramy niniejszego artykułu niemożliwe jest odniesienie się do wszystkich cyberprzestępstw uregulowanych w Kodeksie karnym. Z tego powodu zostanie omówione przestępstwo stypizowane w art. 267 k.k., które z uwagi na jego powszechność, a również okoliczność wzmożonego użycia internetu w dobie COVID-19, może dotknąć szerokie spektrum osób.

Art. 267 § 1 k.k. stanowi: kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Należy jednakże mieć na uwadze, że ściganie tego przestępstwa odbywa się na wniosek osoby pokrzywdzonej. Z uwagi na szeroki katalog czynności należy zauważyć, że w praktyce przepis ten odnosi się do otwierania prywatnej korespondencji, odczytania SMS-ów, czy też do działań hakerskich. Niewątpliwie jest to cyberprzestępstwo, które jest skierowane przeciwko poufności informacji. Polega na uzyskaniu w dowolny sposób bezprawnego dostępu do danych oraz informacji, które przekazywane są w cyberprzestrzeni pomiędzy stronami komunikującymi się[24].

[23] M. Siwicki, *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 7-8/2012, s. 247.
[24] F. Radoniewicz, *Odpowiedzialność karna za przestępstwo hackingu*, „Prawo w działaniu– sprawy karne", 13/2013, s. 127.

Ponadto należy wskazać, że przepis ten jest emanacją gwarancji wyrażonej w art. 49 Konstytucji Rzeczypospolitej Polskiej, który stanowi, że zapewnia się wolność i ochronę tajemnicy komunikowania się. Ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony[25].

W art. 267 § 1 k.k. zostało zastosowane sformułowanie „dostęp do informacji", które powoduje penalizację już samej możliwości odczytu informacji. Zatem nieważne pozostaje, czy sprawca przestępstwa de facto zapoznał się z konkretnymi informacjami. W takich okolicznościach należy stwierdzić, że przepis ten rozszerza zakres gwarantowanej ochrony zagrożonego dobra prawnego[26].

Jednakże żeby stwierdzić, że dane zachowanie jest przestępstwem, muszą zostać spełnione wszystkie wymagania konieczne dla zaistnienia przestępstwa – musi być to więc m.in. działanie bezprawne – na przykład, żeby uznać, że dostęp do informacji został uzyskany w sposób bezprawny, niezbędne jest stwierdzenie, że dana osoba nie posiadała tytułu prawnego do uzyskania danej informacji w czasie dokonywania czynu zabronionego. Będzie to miało miejsce, gdy korespondencja była do niej adresowana. Dodatkowo, co istotne, rozszerzona została karalność w § 3 komentowanego przepisu, ponieważ owo przestępstwo zostaje dokonane w chwili założenia lub posłużenia się narzędziem określonego rodzaju, z zamiarem bezprawnego uzyskania informacji – zatem postać kierunkowego zamiaru bezpośredniego. W takich okolicznościach, gdy niemożliwym będzie przypisanie sprawcy odpowiedzialności karnej z art. 267 § 1 k.k., należy rozważyć kwalifikację przestępstwa z art. 267 § 3 k.k.[27].

Odnośnie do art. 267 § 3 k.k. należy zwrócić dodatkowo uwagę, że organy ścigania będą musiały udowodnić kolejną rzecz. Niezbędne jest udowodnienie, że sprawca przestępstwa działał z zamiarem uzyskania informacji, ponieważ jak zostało wspomniane powyżej, przestępstwo z art. 267 § 3 k.k. jest przestępstwem kierunkowym. Przestępstwa takie wyróżniają się szczególnym nastawieniem woli sprawcy, a konkretniej nastawieniem woli w określonym kierunku. Przedmiotem badań tego elementu przestępstwa są szczególne motywy tudzież pobudki towarzyszące sprawcy przestępstwa[28].

Omawiając tematykę cyberprzestępczości, celem dopełnienia rozważań, należy wskazać, że cyberprzestępstwa są również uregulowane poza kodyfikacją karną. Jak już wcześniej zostało wspomniane, w polskim porządku prawnym funkcjonuje ustawa o świadczeniu usług drogą elektroniczną. W ustawie tej również są przewidziane przepisy karne, dotyczące cyberbezpieczeństwa. Zgodnie z art. 24

[25] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r., Dz. U. 1997 nr 78 poz. 483.

[26] J. Piórkowska-Flieger [w:] T. Bojarski, A. Michalska-Warias, J. Piórkowska-Flieger, M. Szwarczyk, *Kodeks karny. Komentarz*, LexisNexis, Warszawa 2009, s. 589.

[27] F. Radoniewicz, *Odpowiedzialność…*, *op.cit.*, s. 127-135.

[28] M. Nawrocki, *Przestępstwa kierunkowe a zamiar niby-ewentualny*, „Prokuratura i Prawo", 5/2012, s. 41.

ust. 1 ustawy, kto przesyła za pomocą środków komunikacji elektronicznej niezamówione informacje handlowe, podlega karze grzywny. Ściganie wykroczenia, o którym mowa w ust. 1, następuje na wniosek pokrzywdzonego (ust. 2).

Natomiast w myśl art. 25 ustawy orzekanie o tych czynach następuje w trybie przepisów o postępowaniu w sprawach o wykroczenia. W kontekście niniejszego artykułu przepis ten ma szczególne znaczenie, chociażby z uwagi na wiadomości będące właśnie niezamówioną informacją handlową, zwaną potocznie spamem, w której mogą znajdować się cyberataki – za pomocą wcześniej już wymienionej metody *phishingu*.

Mając na uwadze literalne brzmienie wskazanego przepisu, prawnie irrelewantny jest bezprawny sposób przesyłania niezamówionych informacji handlowych, o ile odbywa się to za pomocą środków komunikacji elektronicznej. Natomiast jeśli chodzi o przedmiot przekazu – będą to informacje nakierowane na osiągnięcie zamierzonego celu handlowego, w tym reklamy czy powiadomienia o aktualnych akcjach promocyjnych.

Ratio legis penalizacji *spammingu* jest zaradzenie procederowi godzenia w dobra osobiste człowieka oraz zapewnienie bezpieczeństwa komunikacji w wirtualnej sieci. *Spamming* ingeruje bowiem w prawo do prywatności oraz narusza wolność, w szczególności swobody konsumenta, który ma prawo świadomie uczestniczyć w obrocie gospodarczym oraz samodzielnie decydować o otrzymywanych informacjach handlowych. Powyższe nie wyklucza również celu, jakim jest zaprzestanie rozprzestrzeniania się wirusów i złośliwych oprogramowań, przesyłanych jak niezamówionych informacji handlowych[29].

Większość wyżej wskazanych przykładów cyberprzestępczości, biorąc pod uwagę tryb ścigania przestępstw, jest przestępstwami ściganymi na wniosek, które w polskim systemie prawnym stanowią wyjątek od reguły ścigania przestępstw z urzędu. Zgodnie bowiem z art. 10 k.p.k.[30] organ powołany do ścigania przestępstw jest obowiązany do wszczęcia i przeprowadzenia postępowania przygotowawczego, a oskarżyciel publiczny także do wniesienia i popierania oskarżenia o czyn ścigany z urzędu. Natomiast w myśl art. 12 § 1 k.p.k. w sprawach o przestępstwa ścigane na wniosek postępowanie z chwilą złożenia wniosku toczy się z urzędu. Organ ścigania poucza osobę uprawnioną do złożenia wniosku o przysługującym jej uprawnieniu.

Powyższe oznacza, że brak wniosku o ściganie pochodzącego od uprawnionego podmiotu będzie powodował niemożność wszczęcia i kontynuowania postępowania karnego, a w konsekwencji bezkarność sprawcy cyberprzestępstwa. Natomiast gdyby organ ścigania dalej procedował w przedmiocie czynu, co do

[29] M. Czyżak, *Spamming i jego karalność w polskim systemie prawnym*, „Pomiary Automatyka Kontrola", tom 55, 7/2009, s. 128.

[30] Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego, Dz. U. 1997 nr 89 poz. 555.

którego nie został złożony stosowny wniosek, zajdzie bezwzględna przyczyna odwoławcza wyrażona w art. 439 §1 pkt 9 k.p.k., skutkująca w postępowaniu apelacyjnym uchyleniem wyroku[31].

Podkreślić dodatkowo należy, że walkę z cyberprzestępczością wspiera proces wykrywania, a następnie ścigania i penalizowania cyberprzestępstw. Niewątpliwie skala ujawnionych cyberprzestępstw, wykrytych sprawców i pociągnięcie ich do odpowiedzialności karnej, wpływa pozytywnie na stopień zaufania obywateli do działalności państwa i organów państwowych, w tym organów wymiaru sprawiedliwości. Organy państwowe są bowiem zobowiązane do zapewnienia stanu bezpieczeństwa całemu społeczeństwu, który jest definiowany jako sytuacja, podczas której niezależnie od istniejącego zagrożenia działania podejmowane przez organy państwowe będą skuteczne i jednocześnie będą się cieszyły wśród obywateli zrozumieniem konieczności ich przeprowadzenia[32].

Niemniej jednak wykrywanie tych przestępstw uzależnione jest również od efektywnego wykorzystywania narzędzi o charakterze kryminalistycznym, zastosowania odpowiednich technik, które nieustannie się zmieniają – a zatem wymagają przeprowadzania szkoleń czy zabezpieczania cyfrowych śladów i dowodów rzeczowych, do których należą telefony komórkowe, komputery czy inne urządzenia elektroniczne. W takim świetle widoczne jest, że walka z cyberprzestępczością, tak samo jak zjawisko cybeprzestępczości, nie są pojęciami jednolitymi i zarówno dla procesu ich wykrywania, jak i penalizacji niezbędne jest podjęcie działań na wielu płaszczyznach. Powyższe dwa zagadnienia: cyberprzestępczości i walki z cyberprzestępczością niewątpliwie zyskują na wartości w dobie pandemii COVID-19[33].

Podsumowanie

W walce ze zjawiskiem cyberprzestępczości przedmiotem prac są rozwiązania prawne na szczeblach międzynarodowych, jak i krajowych. Obserwuje się, że używane przez ustawodawców sformułowania nierzadko nie są zbyt precyzyjne – wśród takich pojęć należy wymienić chociażby pojęcia jak informacja czy dane, w związku z czym postuluje się ich doprecyzowanie. Powyższe przekłada się na problemy interpretacyjne, a w konsekwencji na praktykę stosowania prawa. Dodatkowo organy ścigania stoją przed problemami takimi: w jaki sposób jednoznacznie udowodnić przestępcy zamiar zdobycia informacji, który niezwykle

[31] Z. Banasiak, *Przyjęcie zawiadomienia o przestępstwie publicznoskargowym w praktyce policyjnej*, „Prokuratura i Prawo", 2/2008, s. 101.

[32] S. Gładysz, *Zakres uprawnień organów państwa w świetle zagrożenia terrorystycznego*, „Przegląd bezpieczeństwa wewnętrznego", 18/2018, s. 122.

[33] S. Gwoździewicz, K. Tomaszycki, *Prawne i społeczne aspekty cyberbezpieczeństwa*, Międzynarodowy Instytut Innowacji, Warszawa 2017, s. 211.

łatwo przykryć chociażby wolą zbadania stosowanych zabezpieczeń komputerowych? Wówczas zgodnie z art. 269c k.k. taka osoba nie podlega karze za przestępstwo określone w art. 267 §2 k.k. lub art. 269a k.k., bowiem działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej albo opracowania metody takiego zabezpieczenia i niezwłocznie powiadomił dysponenta tego systemu lub sieci o ujawnionych zagrożeniach, a jego działanie nie naruszyło interesu publicznego lub prywatnego i nie wyrządziło szkody. Dodatkowo, celem zwiększenia cyberbezpieczeństwa, zwłaszcza w czasach pandemii COVID-19, mogłoby być zmienienie trybu ścigania wskazanych przestępstw z trybu wnioskowego na przestępstwa ścigane z urzędu oraz propagowanie wiedzy w społeczeństwie poprzez publikowanie opracowań na ten temat w szeroko rozumianych mediach. Ponadto, jak wskazuje się w literaturze przedmiotu, pozytywnie na zjawisko walki z cybeprzestępczością wpłynęłyby szkolenia prawników w przedmiocie cyberprzestępczości czy zajęcia z etyki dla informatyków i programistów, których wiedza i umiejętności są niezbędne dla istnienia i powodzenia przestępczego procederu[34].

Podsumowując, wirtualizacja życia w czasach pandemii COVID-19 z całą pewnością spowodowała w społeczeństwie szereg pozytywnych zachowań, takich jak samodoskonalenie się za pomocą szkoleń on-line, pobudzenie kreatywności, zapoznawanie się z kulturą przez internet, a nawet altruistyczne niesienie pomocy innym. Niemniej jednak zaobserwowano również zwiększenie destrukcyjnych zjawisk, takich jak cyberprzestępczość. W takich okolicznościach należy zadbać o zwiększenie świadomości prawnej społeczeństwa, tak aby grono ofiar, poszkodowanych zjawiskiem cybeprzestępczości, malało. Podstawą bezpieczeństwa jest bowiem świadomość zagrożeń i wiedza, jak się przed nimi chronić. W tym celu należy podkreślić, że każdy użytkownik internetu, który padł ofiarą cyberprzestępstwa, winien zgłosić zawiadomienie o możliwości popełnienia przestępstwa oraz wniosek o ściganie, tak aby dać możliwość działania organom ścigania, ponieważ jak już zostało wskazane, część przestępstw jest właśnie przestępstwami wnioskowymi. Powyższe ma na celu zwiększenie czujności użytkowników internetu, świadomości prawnej obywateli oraz poprawy bezpieczeństwa w sieci**.**

[34] K. Mamak, *Wzrost znaczenia informatyków w obrazie przestępczości w cyfrowym świecie*, „Studia Metodologiczne", 38/2017, s. 99-101.

Bibliografia

Apanowicz J., *Metodologia ogólna*, Gdynia 2002.

Banasiak Z., *Przyjęcie zawiadomienia o przestępstwie publicznoskargowym w praktyce policyjnej*, „Prokuratura i Prawo", 2/2008.

Batorowska H., Klepka R., Wasiuta O., *Media jako instrument wpływu informacyjnego i manipulacji społeczeństwem*, Kraków 2019.

Bart J., Markiewicz R., *Internet a prawo*, Towarzystwo Autorów i Wydawców Prac Naukowych UNIVERSITAS, Kraków 1998.

Chmielewski H., Woźniak W., *Organiczne i afektywne uwarunkowania przestępczości*, „Łódzkie Studia Teologiczne", 14/2005.

Cyrklaff-Gorczyca M., *Cyberstalking jako forma przemocy z wykorzystaniem technologii informacyjno-komunikacyjnych*, K. Materska, B. Taraszkiewicz (red.), *Ekologia informacjia zasoby informacyjne w bibliotekach i cyberprzestrzeni*,Wydawnictwo upamiętniające 100-rocznicę powstania Stowarzyszenia Bibliotekarzy Polskich, Słupsk 2017.

Czyżak M., *Spamming i jego karalność w polskim systemie prawnym*, „Pomiary Automatyka Kontrola", tom 55, 7/2009.

Gładysz S., *Zakres uprawnień organów państwa w świetle zagrożenia terrorystycznego*, „Przegląd bezpieczeństwa wewnętrznego", 18/2018.

Gwoździewicz S., Tomaszycki K., *Prawne i społeczne aspekty cyberbezpieczeństwa*, Międzynarodowy Instytut Innowacji, Warszawa 2017.

Jeszka A., *Problemy badawcze i hipotezy w naukach o zarządzaniu*, „Organizacja i kierowanie", 5/2013.

Kamieniecki W., *Współtworzymy system cyberbezpieczeństwa Polaków*, „Kwartalnik Policyjny", 4/2017.

Konaszczuk W., *Legislacyjne rozwiązania w zakresie przeciwdziałania cyberprzestępczości w prawie podatkowym*, Instytut Wymiaru Sprawiedliwości, Warszawa 2018.

Mamak K., *Wzrost znaczenia informatyków w obrazie przestępczości w cyfrowym świecie*, „Studia Metodologiczne", 38/2017.

Nawrocki M., *Przestępstwa kierunkowe a zamiar niby-ewentualny*, „Prokuratura i Prawo", 5/2012.

Piórkowska-Flieger J. [w:] *Kodeks karny. Komentarz*, Bojarski T., Michalska-Warias A., Piórkowska-Flieger J., Szwarczyk M. (red.), LexisNexis, Warszawa 2009.

Pyżalski J., *Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży*, Oficyna Wydawnicza „Impuls", Kraków 2012.

Radoniewicz F., *Odpowiedzialność karna za przestępstwo hackingu*, „Prawo w działaniu sprawy karne", 13/2013.

Rogowski A., *Phishing*, „Kwartalnik Policyjny", 4/2017.

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

Siwicki M., *Cyberprzestępczość*, C. H. Beck Warszawa 2013.

Sordyl J., *Ransomware – wymuszenie okupu w sieci*, „Kwartalnik Policyjny", 4/2017.

Stefanowicz M., *Cyberprzestępczość próba diagnozy zjawiska*, „Kwartalnik Policyjny", 4/2017.

Wasilewski J. *Przestępczość w cyberprzestrzeni – zagadnienia definicyjne*, „Przegląd bezpieczeństwa wewnętrznego", 15/16.

Woś T., *Trybunalskie i sądowe stosowanie zasady „ignorantia iuris nocet" na gruncie praktyki orzeczniczej w Polsce*, „Filozofia Publiczna i Edukacja Demokratyczna „, 7/2018.

Źródła internetowe

Raport Interpolu *Cybercrime: COVID-19 Impact*, Lyon 2020, s. 4-5 (https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

dostęp na 04.01.2021).
Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r., Dz. U. 1997 nr 78 poz. 483.
Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. Dz. U. 2015 poz. 728.
Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego, Dz. U. 1997 nr 89 poz. 555.
Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, Dz. U. 1997 nr 88 poz. 553.
Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz. U. 2002 nr 144 poz. 1204.
Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz. U. 2018 poz. 1560.

The Pandemic and the Phenomenon of Cybercrime

Summary

The article focuses on the cybercrime phenomenon, which undoubtedly intensified during the Covid19 pandemic. It shows how the transfer of individual aspects of life to the virtual space has reduced the level of security in the network. Additionally, examples of activities aimed at increasing cyber security are provided.

Keywords: cybercrime, cybersecurity, the Covid-19 pandemic