DOI: 10.51480/compress.2021.4-1.244

Justyna Jarocka
UNIWERSYTET W BIAŁYMSTOKU
0000-0002-8820-7094
jarockajustyna96@gmail.com

Podsłuch komputerowy jako środek zwalczania cyberprzestępczości w świetle ochrony tajemnicy komunikowania się

Computer Wiretapping as a Way to Combat Cybercrime in Light of Protecting the Privacy of Communication

ABSTRAKT

Cyberprzestępczość jest zjawiskiem, które stanowi coraz większy problem w świecie szybko rozwijających się technologii. W artykule przedstawiona zostanie tajemnica komunikowania się oraz wskazanie możliwości jej ograniczania. W kolejnej części artykułu zaprezentowane zostaną najważniejsze definicje cyberprzestępczości, zawarte w aktach międzynarodowych, a także scharakteryzowane poszczególne elementy składające się na daną definicję. Przedstawione zostaną również problemy pojawiające się w walce z cyberprzestępczością. Następnie omówiona zostanie ogólna charakterystyka tzw. podsłuchu komputerowego. Ostatnia część artykułu będzie próbą przeanalizowania zakresu podsłuchu komputerowego, uregulowanego w art. 237 Kodeksu postępowania karnego, pod kątem zwalczania cyberprzestępczości.

SŁOWA KLUCZOWE: PRZESTĘPSTWO KOMPUTEROWE, CYBERPRZESTĘPSTWO, PODSŁUCH KOMPUTEROWY

ABSTRACT

Cybercrime is a phenomenon that is becoming more and more problematic in the world of rapidly developing technologies. The paper presents the privacy of communication as well as the methods of limiting it. The next part of the paper shows the most important definitions of cybercrime as included in international acts and describes individual elements of these definitions. Problems arising in the fight against cybercrime are also presented. Then, a general characterization of so-called computer wiretapping is included. The last part of the paper is an attempt to analyze the material scope of the wiretapping, as regulated in article 237 of the Code of Criminal Procedure, in combating cybercrime.

KEYWORDS: CYBERCRIME, COMPUTER CRIME, COMPUTER WIRETAPPING

Jarocka, J. (2021), Podsłuch komputerowy jako środek zwalczania cyberprzestępczości w świetle ochrony tajemnicy komunikowania się, ***com.press,*** 4(1), s. 88–105. DOI: 10.51480/compress.2021.4-1.244 www.compress.edu.pl

WSTĘP

Ochrona tajemnicy komunikowania się jest wartością chronioną zarówno w aktach prawa międzynarodowego, jak i na gruncie Konstytucji RP (Dz. U. Nr 78, poz. 483 ze zm., dalej: Konstytucja RP). Z drugiej strony państwo, oprócz ochrony praw i wolności jednostki, za cel obiera m.in. zapewnienie bezpieczeństwa obywatelom (art. 5 Konstytucji RP). Implikuje to występowanie konfliktu wartości rozstrzyganego przez ustawodawcę przy uchwalaniu ustaw wprowadzających ingerujące czynności dowodowe. Za jedną z dyskusyjnych form pozyskiwania dowodów uznaje się podsłuchy. Wraz z rozwojem technologicznym wiele sfer życia jednostki przeniosło się do cyberprzestrzeni. Należy zauważyć, że sieć komputerowa stała się miejscem popełniania cyberprzestępstw oraz miejscem do wymiany informacji na ich temat. Rozwój ten stanowi wyzwanie dla całego systemu prawa, a w szczególności dla prawa karnego. Ponadto powoduje to konieczność wprowadzania skutecznych środków dowodowych. Za cel niniejszego artykułu obrano ukazanie tzw. podsłuchu komputerowego, ujętego w art. 241 ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (tekst jedn.: Dz. U. z 2021 r. poz. 534, dalej: k.p.k.) jako instytucję prawa karnego procesowego służącą do zwalczania cyberprzestępczości. Mając na uwadze jej ingerujący charakter m.in. w prawo do prywatności (art. 47 Konstytucji RP) oraz ochronę tajemnicy komunikowania się (art. 49 Konstytucji RP), ukazany zostanie wciąż aktualny konflikt wartości we współczesnym świecie.

OCHRONA TAJEMNICY KOMUNIKOWANIA SIĘ ORAZ MOŻLIWOŚCI JEJ OGRANICZANIA

Przy omawianiu zagadnienia związanego z kontrolą i utrwalaniem rozmów bardzo ważne jest zwrócenie uwagi na prawa i wolności jednostki, zwłaszcza na związaną z nimi wolność komunikowania się, w której zakres wchodzi ochrona tajemnicy komunikowania się. Uregulowana jest ona w art. 49 Konstytucji RP, jak również w prawie międzynarodowym, np. w art. 8 Europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności z 1950 r. (Dz. U. z 1993 r. Nr 61, poz. 284 ze zm., dalej: EKPC), który odnosi się do pewnych standardów stosowania podsłuchu.

Warto podkreślić, że zakres przedmiotowy ochrony na gruncie art. 8 ust. 1 EKPC należy rozumieć w sposób szeroki. Obejmuje on nie tylko treść rozmów telefonicznych, ale również informacje dotyczące czasu trwania

połączeń, dane dotyczące połączeń przychodzących i wychodzących czy dat połączeń (Rogalski, 2019). W art. 8 EKPC ujęto wszelkie formy technicznego przekazywania wiadomości, w szczególności wymianę korespondencji w poczcie elektronicznej i informacji internetowych, jak również rozmów telefonicznych. Zagadnienie to jest również przedmiotem licznych orzeczeń. Wskazany artykuł ma również zastosowanie do przekazywania wiadomości przy wykorzystaniu urządzeń prywatnych, publicznych czy też stanowiących wyposażenie biurowe (Garlicki, 2010). Wskazano również, iż kontrola musi być dokonywana przez władze publiczne, ponieważ nagrywanie prywatnych rozmów telefonicznych przez rozmówcę i prywatne użycie takich nagrań nie narusza art. 8 EKPC (wyrok ETPC z 25.10.2007 r. w sprawie Van Vondel p. Holandii, skarga nr 38258/03, par. 49).

Egzekwowanie ochrony prawa do prywatności oraz wolności tajemnicy komunikowania się spoczywa głównie na organie sądowym w postaci Europejskiego Trybunału Praw Człowieka z siedzibą w Strasburgu. Podstawowym zadaniem ETPC jest rozpatrywanie skarg obywateli, którzy sygnalizują pewne nieprawidłowości w postępowaniu organów władzy publicznej. To właśnie orzecznictwo tego organu sądownictwa międzynarodowego wyznacza granice stosowania podsłuchu komputerowego. W doktrynie zauważa się, że w sprawach rozpoznawanych przez ETPC najczęstszym przykładem ingerencji państwa w życie prywatne i korespondencję było stosowanie różnych dopuszczalnych form podsłuchu telefonii komórkowej i stacjonarnej. Sam ETPC podkreślał wielokrotnie, że czynność ta stanowi ingerencję w prawo wyrażone w art. 8 ust. 1 EKPC (Rogalski, 2019). Należy również zauważyć, że na gruncie EKPC ochrona praw i wolności ma niezwykle szeroki wymiar. Warto jednak zwrócić uwagę na pewne wyłączenie w zakresie ochrony wolności i praw, zawarte w art. 15 EKPC. Przewidziano w nim możliwość uchylenia się przez strony Konwencji od przyjętych na jej gruncie standardów w zakresie ochrony praw i wolności wyłącznie w przypadku wojny lub zaistnienia innego niebezpieczeństwa publicznego zagrażającego życiu narodu. Postawiono jednak warunek, że wykorzystywane środki nie będą sprzeczne z innymi zobowiązaniami wynikającymi z prawa międzynarodowego.

Artykuł 49 Konstytucji RP reguluje wolność i ochronę tajemnicy komunikowania się, które uznawane są za wolności o charakterze osobistym. Przyjmuje się, że wolność i tajemnica komunikowania się są jednym z aspektów prawa do prywatności. Trybunał Konstytucyjny wskazuje, iż wolność komunikowania się jest przejawem prawa do prywatności i obejmuje nie tylko tajemnicę korespondencji, ale również wszelkiego rodzaju kontakty międzyosobowe (Rogalski, 2019, za: wyrok TK z 2.07.2007 r., K 41/05). Z uwagi

na rangę tej wolności, jak również chęć podkreślenia przez ustawodawcę jej wartości, została ona wyodrębniona w osobnym przepisie. Przedstawiciele doktryny podkreślają, że wolność i ochrona tajemnicy komunikowania się są jednymi z podstawowych zasadach ustrojowych każdego demokratycznego państwa prawa (Szczechowicz, 2009). Wolność komunikowania się jest możliwością porozumiewania się jednostki w dowolnej formie przy pomocy środków przekazu na odległość zarówno z osobami jej znanymi, jak i obcymi. Tajemnica komunikowania się wyraża się natomiast w zakazie zmuszania uczestników komunikacji do ujawniania jej treści oraz w niedopuszczalności zapoznawania się z jej treścią przez osoby trzecie (Wiliński, 2011). Wskazuje się, iż komunikowanie się należy rozumieć bardzo szeroko, gdyż obejmuje ono wszelkiego rodzaju formy i sposoby przekazywania treści, niezależnie od ich nazwy. Podkreśla się również fakt, iż z art. 49 Konstytucji RP wyraźnie wynika, że tajemnicą komunikowania się objęte są nie tylko treść przekazów, ale również fakt i okoliczności komunikowania się (Piątek, 2013). Wynika to także z orzecznictwa TK, który stwierdził, że wolnością komunikowania się została objęta nie tylko treść wiadomości, ale również wszelkie okoliczności procesu porozumiewania się, takie jak: informacje o wybieranych numerach telefonów, dane osobowe uczestników procesu porozumiewania się, dane obrazujące czas i częstotliwość połączeń czy dane o numerze IP i numerze IMEI. Z orzecznictwa TK wynika ponadto, że bez znaczenia pozostaje sfera życia, której dotyczy rozmowa, gdyż żadna ze sfer nie została wyjęta spod ochrony konstytucyjnej. Ochronie podlega więc komunikacja międzyludzka dotycząca sfery prywatnej, zawodowej, gospodarczej i innych. Istotną kwestią jest wskazanie przez TK, że zgodnie z zasadą demokratycznego państwa prawnego, wyrażoną w art. 2 Konstytucji RP, w przypadku gdy mamy do czynienia z wolnością jednostki, a nie korzystaniem przez nią z prawa podmiotowego, konieczne jest założenie możliwości anonimowego występowania jednostek w przestrzeni publicznej (wyrok TK z 30.07.2014 r., K 23/11). Wart podkreślenia jest fakt, że ochrona tajemnicy komunikowania się nie powinna być mylona z obowiązkiem zachowania w tajemnicy treści konwersacji, ciążącym na jej uczestnikach. Uchybienie temu obowiązkowi może stanowić naruszenie tajemnicy prawnie chronionej, np. państwowej, zawodowej, przedsiębiorstwa bądź też nadużyciem zaufania rozmówców. Dodatkowo z art. 49 Konstytucji RP nie płynie także obowiązek zachowania tajemnicy treści przekazywanych informacji czy też okoliczności rozmowy (Wild, 2016).

W tym miejscu należy wskazać, że wolność i ochrona tajemnicy komunikowania się nie mają charakteru absolutnego i istnieje możliwość ich

ograniczania w drodze ustawy. Ograniczenia w zakresie tej wolności mogą być ustanowione w przypadkach, w których korzystanie z niej naruszałoby inne dobra chronione konstytucyjnie, takie jak np. bezpieczeństwo państwa, porządek publiczny, zdrowie, moralność, prawa i wolności innych osób (Banaszak, 2012). Poza tym istnieje możliwość ograniczenia omawianych praw i wolności z uwagi na stan wyjątkowy oraz stan wojenny. W doktrynie podkreśla się, że regulacje ustawowe w zakresie ograniczeń wolności komunikowania się oraz ochrony tajemnicy komunikowania się powinny zostać dokładnie określone przez organy, które mogą ustanowić takie ograniczenia (Winczorek, 2008). Na potrzeby niniejszej publikacji należy wspomnieć o grupie ograniczeń zawartych w rozdziale 26 Kodeksu postępowania karnego, która dotyczy kontroli i utrwalania rozmów. Ograniczenia te wynikają z konieczności „walki z przestępczością, która stanowi zagrożenie dla wielu konstytucyjnych wartości" (Rogowska, 2014, s. 204). Przepisy zawarte w tym rozdziale dają podstawy do zarządzenia przez sąd, na wniosek prokuratora, kontroli i utrwalania rozmów telefonicznych, a także innych rozmów lub przekazów informacji oraz korespondencji przesyłanej pocztą elektroniczną.

OGÓLNA CHARAKTERYSTYKA CYBERPRZESTĘPCZOŚCI

W ostatnich latach jesteśmy świadkami postępu technologicznego, który dotyczy wielu sfer życia człowieka. Rozwój globalnej sieci, zwanej internetem, jak również technologii służącej do porozumiewania się na odległość i w znacznym stopniu ułatwiającej funkcjonowanie człowieka niesie ze sobą, oprócz niewątpliwie wielu pozytywnych efektów, również te negatywne. Zauważyć można zjawiska o charakterze patologicznym czy wręcz przestępczym. Różnią się one od pozostałych przestępstw specyficznymi cechami. Ogromna liczba danych, zasięg geograficzny oraz brak kontroli sprawiły, że internet zaczął być wykorzystywany przez przestępców do popełniania czynów zabronionych, stwarzając jednocześnie liczne trudności wymiarowi sprawiedliwości w ich ściganiu (Hołyst, 2011).

Na początku należałoby zdefiniować pojęcia przestępstwa komputerowego, jak również cyberprzestępczości. Nie ma definicji legalnej przestępstwa komputerowego. Pojęcie to zaczęło kształtować się w latach 70. XX wieku. W doktrynie przestępczością komputerową określa się kryminologiczne zjawisko zachowania przestępnego związanego z funkcjonowaniem elektronicznego przetwarzania danych, godzące bezpośrednio w przetworzoną

informację, jak również jej nośnik czy sprzęt komputerowy (Jakubski, 1996). Zauważa się również, że na gruncie prawa karnego materialnego przestępstwa komputerowe oznaczają zazwyczaj dwie grupy czynów, tj. zamachy skierowane na systemy, dane i programy komputerowe, w których system komputerowy jest przedmiotem lub środowiskiem zamachu, oraz przestępstwa, w których komputer stanowi narzędzie przestępstwa. Definicję przestępstwa komputerowego możemy również stworzyć na polu karnoprocesowym, w którym będzie ona ściśle związana z faktem, że w systemie komputerowym mogą znajdować się dowody na popełnienie przestępstwa. Wskazuje się więc, że przestępstwem komputerowym są wszystkie czyny zabronione przez prawo karne, których ściganie generuje potrzebę uzyskania przez ograny wymiaru sprawiedliwości dostępu do informacji przetwarzanych w systemach informatycznych. Tak sformułowane pojęcie określa przypadki, w których system komputerowy stanowi zarówno narzędzie, jak i przedmiot zamachu (Adamski, 2000).

Rozwój nowoczesnej technologii oraz upowszechnienie internetu sprawiły, że powstał jednak problem terminologiczny z uwagi na fakt, iż pojęcie przestępstwa komputerowego zaczęło być niewystarczające. Komputery mogą być przedmiotem lub środowiskiem zamachu, jak również posłużyć do naruszania dóbr prawnie chronionych przez prawo karne, w tym w szczególności do rozpowszechniania informacji zakazanych przez prawo, jak również pełnić rolę incydentalną przy popełnianiu przestępstwa (Siwicki, 2012). Zaczęto więc skłaniać się ku określaniu tego rodzaju przestępstw mianem cyberprzestępczości. Nie wypracowano jednak jednolitej definicji tego pojęcia. Wynika to z faktu, iż definicja ta ewoluuje wraz z postępem technologicznym. Przedstawiciele doktryny określają cyberprzestępczość jako wszelkiego rodzaju czyny zabronione, do popełnienia których użyto technologii informatycznej, jak również czyny skierowane przeciwko systemom informatycznym i danym (Golonka, 2016). Na uwagę zasługują definicje wypracowane na gruncie prawa międzynarodowego. Definicję cyberprzestępczości przyjął X Kongres ONZ w sprawie zapobiegania przestępczości i traktowania przestępców, dzieląc cyberprzestępczość na tę w ujęciu wąskim i szerokim. W znaczeniu wąskim pojęcie to odnosi się do przestępstw komputerowych i polega na wszelkim nielegalnym działaniu skierowanym przeciwko bezpieczeństwu systemów komputerowych i elektronicznie przetwarzanych przez te systemy danych, wykonywane z wykorzystaniem operacji elektronicznych. W znaczeniu szerokim odnosi się do przestępstw dotyczących komputerów, które polegają na wszelkim nielegalny działaniu, popełnionym przy użyciu lub skierowanym przeciwko systemom czy sieciom

komputerowym, włączając w to m.in. nielegalne posiadanie oraz udostępnianie lub rozpowszechnianie informacji za pomocą komputera bądź sieci (Siwicki, 2013). W komunikacie Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów z 22 maja 2007 r. termin „cyberprzestępczość" używany jest do określenia trzech rodzajów przestępstw. Pierwszy obejmuje tradycyjne przestępstwa, takie jak oszustwo czy paserstwo, jednak z wykorzystaniem elektronicznych sieci informatycznych i systemów informatycznych. Drugi rodzaj dotyczy publikowania nielegalnych treści w mediach elektronicznych, np. pornografii dziecięcej, natomiast trzeci odnosi się do przestępstw typowych dla sieci łączności elektronicznej, tj. hakerstwo czy ataki przeciwko systemom informatycznym (Stefanowicz, 2017).

Cyberprzestępczość można podzielić na dwie kategorie: przestępstwa, których przedmiotem ataku jest komputer oraz przetwarzanie danych w systemach. Drugą kategorię stanowią przestępstwa z wykorzystaniem internetu, w których komputer jest tylko środkiem do ich popełnienia. Do pierwszej kategorii można zaliczyć między innymi następujące czyny karalne: podawanie się za inną osobę, nieuprawnione uzyskanie informacji, sabotaż komputerowy, rozpowszechnianie złośliwych oprogramowań oraz oszustwo komputerowe. Przedstawiciele doktryny do drugiej kategorii przestępstw zaliczają m.in.: obrazę uczuć religijnych, czyli przestępstwa przeciwko wolności sumienia i wyznania, szeroko pojętą mowę nienawiści, objawiającą się np. propagowaniem totalitarnych ustrojów czy nawoływaniem do nienawiści z powodu różnic poglądowych, pochwalanie lub propagowanie zachowań o charakterze pedofilskim, zbywanie własnego lub cudzego dokumentu tożsamości lub oszustwa popełnione za pośrednictwem internetu, np. na portalach aukcyjnych (Stefanowicz, 2017).

Internet stał się miejscem prowadzenia działalności przestępczej oraz masowego udostępniania nielegalnych i szkodliwych treści. Wskazuje się, że wszelkiego rodzaju dane gromadzone w internecie są narażone na nielegalne wykorzystanie poprzez dokonywanie m.in. „oszustw, kradzieży tożsamości, włamań do kont bankowości elektronicznej i kradzieży zgromadzonych środków pieniężnych czy ukierunkowanych ataków opartych na socjotechnice (*phishing, spearphishing, whalling*)" (Gryszczyńska, 2018). Zauważa się również, że cyberprzestępczość staje się prostsza w miarę postępu technologicznego. Dodatkowo internet niesie ze sobą swego rodzaju łatwość i masowość rozpowszechnia nielegalnych i szkodliwych informacji, m.in. treści o charakterze pornograficznym, rasistowskim, faszystowskim i ksenofobicznym. Łatwość ta przejawia się w tym, że to „Internet oferuje anonimowy i często pozbawiony kontroli dostęp do informacji" (Siwicki,

2011). Udostępnianie takich treści może stanowić naruszenie wielu norm Kodeksu karnego. Przykład stanowią: propagowanie faszyzmu lub innego ustroju totalitarnego, określone w art. 256 k.k. czy publiczne prezentowanie treści pornograficznych – art. 202 k.k.

Analizie warto poddać art. 202 k.k., który penalizuje publiczne prezentowanie treści pornograficznych, a w § 3–4c określa przestępstwa związane z udziałem małoletnich. Karze podlegają następujące zachowania: produkcja, utrwalanie, sprowadzanie, przechowywanie lub posiadanie albo rozpowszechnianie lub prezentowanie treści pornograficznych z udziałem małoletniego. Należy w tym miejscu przytoczyć tezę Sądu Najwyższego, który zdefiniował pornografię dziecięcą jako „jakikolwiek materiał, który wizualnie przedstawia dziecko uczestniczące w rzeczywistej lub udawanej czynności wyraźnie seksualnej lub jakiekolwiek przedstawianie narządów płciowych dziecka głównie w celach seksualnych" (postanowienie SN z 15.01.2020 r., V KK 655/19). Zauważyć należy, że rozwój technologiczny, a co za tym idzie – coraz powszechniejszy dostęp do internetu, wpływają na to, iż każda z czynności określonych w art. 202 k.k. może być dokonana za pomocą komputera, co pozwala zakwalifikować je do cyberprzestępczości. Stwarza to poważne zagrożenie rozrastania się przestępczości, której ofiarami stają się małoletni.

Wskazać należy również zjawisko cyberterroryzmu, który polega na „wykorzystaniu technik informacyjnych, tj. komputerów, oprogramowań, urządzeń telekomunikacyjnych, Internetu, w celu osiągnięcia zamierzonych przez daną grupę celów" (Chałubińska-Jentkiewicz, Nowikowska, 2020). Działania cyberterrorystów skupiają się m.in. na działaniach propagandowych, atakowaniu celów wirtualnych czy wykorzystywaniu cyberprzestrzeni do powodowania fizycznych zniszczeń. Przyjmuje się ponadto, że „ataki na informacje przechowywane w systemie komputerowym mogą mieć dwojaki charakter: jako chęć podważenia wiarygodności systemu albo kradzież informacji" (Chałubińska-Jentkiewicz, Nowikowska, 2020). Zagrożenie cyberatakami prowadzi do rozszerzania uprawnień służb bezpieczeństwa mających za zadanie ochronę społeczeństwa przed zagrożeniami związanymi z cyberterroryzmem. Polega ona na ograniczeniu prawa do prywatności poprzez poddawanie kontroli coraz nowszych obszarów życia obywateli za pomocą narzędzi i uprawnień przyznawanych służbom bezpieczeństwa. Stwarza to konflikt pomiędzy bezpieczeństwem społeczeństwa a jego wolnością.

Należy również wskazać na zagrożenia oraz trudności wynikające z cyberprzestępczości. Pierwszą trudność stanowi wykrywanie cyberprzestępstw. Związane jest to z ich specyfiką, która wyraża się w szczególnej kategorii podmiotów odpowiedzialnych za takie czyny, jak również powiązany z tym

problem ustalenia konkretnego sprawcy (Hołyst, 2020). Podmiotami tymi są często grupy hakerskie, stanowiące hermetyczne społeczności, z której rekrutowani są sprawcy przestępstw internetowych. Zagrożeniem jest ponadto rozwój technologii, a w szczególności technologii mobilnej. Użytkownicy smartfonów, tabletów czy innych urządzeń mobilnych w dużo mniejszym stopniu dbają o bezpieczeństwo tych urządzeń, co stwarza możliwość nadużyć oraz daje sposobność do cyberataków w nieznanych dotychczas formach. Kolejną trudnością, na którą należałoby zwrócić uwagę, są dynamiczne zmiany zachodzące w internecie, jak również postęp technologiczny, za którym nie nadążają przepisy prawa. Rozwój narzędzi służących do anonimizacji osoby w internecie stanowi niewątpliwie poważny problem. Sprawcy przestępstw korzystają z sieci TOR czy serwisów proxy, stając się bardzo trudni do wykrycia, co prowadzi do wzrostu wykorzystywania tych narzędzi do popełniania przestępstw (Stefanowicz, 2017). Kolejną trudność stanowią różnice legislacyjne pomiędzy poszczególnymi krajami, co powoduje wydłużenie, a w niektórych przypadkach uniemożliwienie ścigania sprawcy. Wnioski organów ścigania rozpatrywane są według prawa obowiązującego w danym państwie, a w przypadku braku penalizacji danego czynu w uregulowaniach prawnych takie wnioski są rozpatrywanie odmownie. Należy mieć na uwadze, że w bardzo wielu przypadkach tylko odpowiednio szybka reakcja organów ścigania pozwoli na ujęcie sprawcy, a niekiedy zapobieżenie poważnym konsekwencjom związanym np. z ujawnieniem informacji zagrażających bezpieczeństwu państwa.

Nie oznacza to jednak braku wielostronnej współpracy na szczeblu międzynarodowym w zakresie skutecznego pozyskiwania dowodów. Przedstawiciele doktryny podają, że podstawę współpracy stanowi fakt nieograniczonych możliwości szybkiego przemieszczania się przestępców, zwłaszcza działających w zorganizowanych grupach. Jednym z najskuteczniejszych instrumentów walki z przestępczością i terroryzmem jest przechwytywanie i rejestrowanie transmisji telekomunikacyjnych i teleinformatycznych, a więc również rozmów telefonicznych. Chodzi tu głównie o stosowanie przez organy ścigania i wymiaru sprawiedliwości podsłuchu telefonicznego oraz podsłuchu komputerowego (Kosmaty, 2008). Jednym z najważniejszych aktów prawnych, będących przejawem międzynarodowej współpracy, jest sporządzona w dniu 29 maja 2000 r. w Brukseli Konwencja o pomocy prawnej w sprawach karnych pomiędzy państwami członkowskimi Unii Europejskiej (Dz. U. z 2007 r. Nr 135, poz. 950), której przepisy zaczęły obowiązywać w Polsce z dniem 26 października 2005 r. na mocy ratyfikacji z 2004 r. W świetle Konwencji przechwycenie przekazu telekomunikacyjnego

może nastąpić na potrzeby toczącego się postępowania karnego w jednym z państw członkowskich Unii Europejskiej. Na gruncie Konwencji wyróżnia się następujące sytuacje: przechwytywanie przekazów telekomunikacyjnych podmiotów znajdujących się na terytorium innego państwa członkowskiego, przechwytywanie przekazów telekomunikacyjnych na własnym terytorium za pośrednictwem dostawców usług oraz przechwytywanie przekazów telekomunikacyjnych bez pomocy technicznej innego państwa członkowskiego.

OGÓLNA CHARAKTERYSTYKA TZW. PODSŁUCHU KOMPUTEROWEGO

Instytucji kontroli i utrwalania rozmów telefonicznych został poświęcony rozdział 26 k.p.k. umieszczony w dziale V obejmującym swą treścią regulację dowodów. Przedstawiciele doktryny konstruują definicję wskazującą, że podsłuch jest tajnym, czyli dokonywanym bez wiedzy osób będących uczestnikami procesu komunikacji, uzyskiwaniem lub utrwalaniem treści rozmów prowadzonych przy użyciu środków łączności za pomocą urządzeń technicznych. Obejmuje on również kontrolę rozmów dokonywanych poza systemem teleinformatycznym, pod warunkiem że osoba dokonująca tej kontroli nie jest uczestnikiem kontrolowanej rozmowy (Zakrzewski, Jarocha, 1997).

Instytucja tzw. podsłuchu komputerowego została uregulowana w art. 241 k.p.k., który wskazuje, że przepisy art. 237–239 k.p.k. stosuje się odpowiednio do kontroli oraz do utrwalania przy użyciu środków technicznych treści innych rozmów lub przekazów informacji, w tym korespondencji przesyłanej pocztą elektroniczną. Przekazy tychże informacji mogą być dokonywane za pomocą dowolnych urządzeń używanych przez organy ściągania w danym państwie (Dudka, Paluszkiewicz, 2018). Jedna z uchwał Sądu Najwyższego wskazuje, że chodzi o przesyłanie treści rozmów niemających charakteru rozmów telefonicznych za pośrednictwem sieci teleinformacyjnej, tj. poprzez przewody, systemy radiowe, optyczne lub jakiekolwiek inne urządzenia wykorzystujące energię elektromagnetyczną (Kmiecik 2002, za: uchwała SN z 21.03.2000, I KZP 60/99). Ponadto funkcjonuje rozwiązanie, które zakłada, iż przechwytywanie przez organy danych informatycznych jest możliwe nie tylko w drodze podsłuchu tradycyjnego, ale także przy pomocy podsłuchu komputerowego. W piśmiennictwie wskazuje się, że w związku z postępem technologicznym należy obie aktywności nazwać zbiorczo teleinformatyką, bez potrzeby kreowania podziału na podsłuch telefoniczny i podsłuch komputerowy (Rogalski, 2019). Tematyce dotyczącej tych czynności

poświęcono wiele uwagi ze względu na postępującą informatyzację i rozwój cyberprzestępczości, co skutkuje wyróżnieniem specyficznej kategorii dowodów – tzw. dowodów elektronicznych. Ponadto zagadnienie dowodów elektronicznych pozostaje w kręgu zainteresowań nie tylko procesualistów, ale również specjalistów z dziedziny kryminalistyki, którzy na jej gruncie wykształcili pojęcie tzw. śladu elektronicznego (Jagiełło, 2019).

Analizując powyższe regulacje, należy zaznaczyć, że przepisy polskiego Kodeksu postępowania karnego, tj. art. 237 i n., mają zastosowanie wyłącznie w przypadku podsłuchu procesowego stosowanego w trakcie postępowania karnego, które prowadzone jest na terytorium Polski. „Legalność podsłuchu telefonicznego, dokonywanego przez organy obcego państwa, w ramach toczącego się na jego obszarze postępowania, należy oceniać według przepisów obowiązujących w państwie, w którym czynność ta jest dokonywana" (wyrok SN z 19.09.2000 r., V KKN 331/00). Oceniając możliwość wykorzystania tak zebranych dowodów w postępowaniu karnym, które toczy się w Polsce, należy odwołać się do art. 587 k.p.k., który dotyczy możliwości odczytania na rozprawie protokołów z czynności dowodowych sporządzonych na wniosek polskiego sądu lub prokuratora. Z przepisu nie wynika zakaz wykorzystania materiałów, które zostały uzyskane od organów zagranicznych na wniosek polskiego sądu lub prokuratora. Istotna jest natomiast kwestia, że sposób przeprowadzenia czynności nie może być sprzeczny z zasadami porządku prawnego obowiązującego w Rzeczypospolitej Polskiej (Skorupka, 2020, za: wyrok SN z 19.09.2000 r., V KKN 331/00).

ANALIZA ZAKRESU PRZEDMIOTOWEGO ZASTOSOWANIA PODSŁUCHU POD KĄTEM ZWALCZANIA CYBERPRZESTĘPCZOŚCI

Zakres przedmiotowy zastosowania podsłuchu uregulowany jest w art. 237 k.p.k., zgodnie z którym kontrolę i utrwalanie rozmów telefonicznych stosuje się w celu wykrycia i uzyskania dowodów dla toczącego się postępowania lub zapobieżenia popełnieniu nowego przestępstwa. Analogicznie, zgodnie z art. 241 k.p.k., przepisy o podsłuchu telefonicznym należy stosować również do podsłuchu komputerowego, więc zasadne jest przeanalizowanie regulacji zawartych w art. 237 k.p.k. pod kątem zwalczania cyberprzestępczości.

Artykuł 237 § 1 k.p.k. reguluje cele stosowania tej czynności dowodowej, nie wskazując jednak na ścisłe ich powiązanie z przestępstwami określonymi w katalogu przestępstw z § 3. Czyni to jednak w sposób jednoznaczny

§ 3, stanowiąc, że kontrola i utrwalanie rozmów telefonicznych są dopuszczalne tylko wtedy, gdy toczące się postępowanie lub uzasadniona obawa popełnienia nowego przestępstwa dotyczą enumeratywnie wyliczonych przestępstw. W doktrynie wskazuje się, że nieakceptowalne jest zarządzenie podsłuchu telefonicznego, jeżeli postępowanie prowadzone jest w sprawie o inne przestępstwo niż wymienione w art. 237 § 3 k.p.k. oraz dla zapobieżenia popełnieniu nowego przestępstwa, ale innego niż wymienione w art. 237 § 3 k.p.k. (Rogalski, 2019). Zauważa się ponadto, że możliwość zastosowania podsłuchu jest ograniczona do enumeratywnie wyliczonych w art. 237 § 3 k.p.k. przestępstw, które zakreślają granice przedmiotowe, a ponadto, że w przypadku katalogu chodzi o najcięższe przestępstwa, w stosunku do których kontrola i utrwalanie rozmów mogą okazać się celowe (Marszał, 1996). Słusznie stwierdza się też, że niedopuszczalne jest zarządzenie podsłuchu w sprawie toczącej się o inne przestępstwo w celu wykrycia i utrwalenia dowodów. Jednakże za dopuszczalne należy uznać zarządzenie podsłuchu w sprawie prowadzonej o przestępstwo niewymienione w art. 237 § 3 k.p.k., w przypadku gdy podsłuch miałby na celu zapobieżenie popełnieniu przestępstwa ujętego w zamkniętym katalogu tegoż przepisu.

Biorąc pod uwagę bezsporny, na gruncie doktryny, związek dopuszczalności stosowania podsłuchu oraz katalogu przestępstw z art. 237 § 3 k.p.k., do oceny zakresu przedmiotowego konieczne jest przeanalizowanie ujętych w nim przestępstw pod kątem ich ciężaru gatunkowego, który – jak wyżej wspomniano – uzasadnia stosowanie podsłuchu. Przedstawiciele doktryny wysuwają tezę, że wymienione w art. 237 § 3 k.p.k. przestępstwa charakteryzują się dużym stopniem społecznej szkodliwości czynu i dużym ciężarem gatunkowym (Rogalski, 2019). Wydawać by się mogło, że nie wszystkie przestępstwa spełniają podstawowego kryterium proporcjonalności, wyrażone w orzecznictwie ETPC, który stoi na stanowisku, że należy rozróżnić zagrożenie przestępstwami o charakterze terrorystycznym od zagrożenia powodowanego przez przestępstwa pospolite. Dlatego ciężar gatunkowy sprawy powinien, obok znaczenia postępowania karnego, odgrywać rolę wiodącą w procesie decyzyjnym sądu co do zarządzenia kontroli (Szczechowicz, 2009). Należy zauważyć, że przestępstwa przeciwko życiu czy te dokonywane w związku z działalnością zorganizowanych grup przestępczych poprzez udział w nich, czy też takie kategorie przestępstw, jak gromadzenie broni i materiałów wybuchowych, handel ludźmi czy przestępstwa narkotykowe (pkt 13) bezspornie zasługują na miano przestępstw, które spełniają kryteria ograniczenia praw jednostki ugruntowanych w art. 31 ust. 3 Konstytucji RP oraz orzecznictwie ETPC wydawanym na podstawie art. 8 ust. 2 EKPC.

Ich zwalczanie służy ochronie wartości w postaci podstawowego dobra, jakim jest bezpieczeństwo lub porządek publiczny, zdrowie, wolność i prawa innych osób. Zależność pomiędzy ograniczeniem praw jednostki w postaci zastosowania podsłuchu, którego celem jest zapewnienie bezpieczeństwa, jest dostrzegalna i nie budzi sporów, ponieważ przestępstwa te charakteryzują się wysokim ciężarem gatunkowym, a ich zwalczanie jest priorytetowe.

Wątpliwy jest natomiast ciężar gatunkowy zawartych w katalogu przestępstw skarbowych oraz przestępstw przeciwko wartości w postaci dobra wymiaru sprawiedliwości, które mogą dotyczyć również czynów penalizowanych na gruncie prawa karnego skarbowego ujętych w kategorii wykroczeń. Należy więc zauważyć, że zakwalifikowanie przez ustawodawcę danego czynu jako wykroczenia podaje w wątpliwość stopień jego szkodliwości, nie kwalifikując go jako przestępstwa. Stąd spostrzeżenie, że wykroczenia skarbowe nie powinny stanowić podstawy do ingerowania w sferę wolności jednostki, ponieważ może to rodzić odczucie nadużycia dopuszczalności stosowania podsłuchu w postępowaniach karnych toczących się o przestępstwa z art. 237 § 3 pkt 16a–16d k.p.k., dokonane w związku z wykroczeniem skarbowym. Dodatkowo ustawodawca nie określił, w przypadku przestępstw z art. 237 § 3 pkt 16a–16g k.p.k., w stosunku do jakiej kategorii przestępstw należy je odnieść. Warto zauważyć, że te kategorie przestępstw nie nawiązują wprost do wartości uzasadniających ograniczanie wolności jednostki. Z pewnością wymiar sprawiedliwości, a w szczególności wymienione wyżej przestępstwa wiążą się z dobrem w postaci bezpieczeństwa lub porządku publicznego, ale nie stanowią jego podstawy. Można więc wskazać w przypadku tych kategorii przestępstw na zagrożenie dla zasady proporcjonalności, jednej z najważniejszych na gruncie orzecznictwa ETPC.

W tym miejscu należy wskazać na możliwość zastosowania podsłuchu w stosunku do cyberprzestępstw. Jak wskazano w poprzednim punkcie niniejszego artykułu, cyberprzestępczość można podzielić na dwie kategorie przestępstw: przestępstwa, których przedmiotem ataku jest komputer oraz przetwarzanie danych w systemach, oraz przestępstwa z wykorzystaniem internetu, w których komputer jest tylko środkiem do ich popełnienia. Katalog zawarty w art. 237 § 3 k.p.k. wymienia przestępstwa, które mogą być zaliczone głównie do przestępstw, w których internet jest środkiem pomocniczym. Dla przykładu możemy tu wskazać szpiegostwo lub ujawnienie informacji niejawnych o klauzuli tajności „tajne" lub „ściśle tajne" (pkt 10), fałszowanie oraz obrót fałszywymi pieniędzmi, środkami lub instrumentami płatniczymi albo zbywalnymi dokumentami uprawniającymi do otrzymania sumy pieniężnej, towaru, ładunku albo wygranej rzeczowej

albo zawierającymi obowiązek wpłaty kapitału, odsetek, udziału w zyskach lub stwierdzenie uczestnictwa w spółce (pkt 12), jak również podrabianie lub przerabianie faktur lub używanie faktur podrobionych lub przerobionych w zakresie okoliczności faktycznych mogących mieć znaczenie dla określenia wysokości należności publicznoprawnej lub jej zwrotu albo zwrotu innej należności o charakterze podatkowym oraz wystawianie i używanie faktur poświadczających nieprawdę co do okoliczności faktycznych mogących mieć znaczenie dla określenia wysokości należności publicznoprawnej lub jej zwrotu albo zwrotu innej należności o charakterze podatkowym (pkt 12a). W pozostałych przypadkach internet może służyć jako narzędzie do komunikacji między przestępcami czy też jako źródło informacji. Jednakże nie można, w większości przestępstw zawartych w art. 237 § 3 k.p.k., wskazać na bezpośredni związek internetu z popełnieniem przestępstwa, co nie pozwala zakwalifikować ich do cyberprzestępstw.

PODSUMOWANIE

Powyższa analiza cyberprzestępczości oraz tzw. podsłuchu komputerowego pozwala wysnuć wnioski, że jest to problem, który staje się coraz bardziej znaczący we współczesnym świecie. Rozwój technologii, a co za tym idzie zwiększająca się liczba użytkowników internetu oraz postępująca cyfryzacja życia stwarzają dodatkowe możliwości przestępcom, dlatego należy stanąć na stanowisku, że tzw. podsłuch komputerowy będzie odgrywać coraz ważniejszą rolę. Ponadto warto zwrócić uwagę, że postęp technologiczny miał wpływ również na terminologię określającą cyberprzestępstwo. Początkowe używanie określenia „przestępstwo komputerowe" należy uznać za zbyt ogólne. Wynika to z faktu, iż w związku z obecnością komputera w praktycznie każdej dziedzinie życia, jak również rozwojem technologii mobilnej, która pozwala na dostęp do internetu i wykonywanie operacji bez konieczności używania komputera, definiowanie zjawiska cyberprzestępczości poprzez wskazanie komputera jako narzędzia służącego do popełnienia przestępstwa jest niewystarczające.

Cyberprzestępczość jest zjawiskiem charakteryzującym się dużą dynamiką związaną z rozwojem nowoczesnej technologii, a co za tym idzie stwarzaniem przestrzeni do popełniania przestępstw (Golonka, 2016). Uregulowanie podsłuchu komputerowego skłania do refleksji, iż nowelizacja przepisów i rozszerzenie katalogu przestępstw z art. 237 § 3 k.p.k. przez ustawodawcę jest niewystarczające. Zdaje się, że ustawodawca rozszerza zakres

przedmiotowy zastosowania podsłuchu pod kątem walki z przestępstwami finansowymi godzącymi w Skarb Państwa. Nie uwzględnia zmieniającej się rzeczywistości, a co za tym idzie, pojawiania się nowych przestępstw, które mogą zostać popełnione w cyberprzestrzeni. Należałoby rozszerzyć katalog przestępstw o te związane z cyberprzestępczością, np. cyberstalking, jak również przestępstwa związane z pedofilią czy pornografią dziecięcą.

Warto również zwrócić uwagę, że problemem w walce z cyberprzestępczością jest często jej międzynarodowy charakter, co powoduje niekiedy konflikt uregulowań prawnych oraz wydłużenie czasu rozpatrywania wniosków przez odpowiednie instytucje, co niekiedy skutkuje brakiem odpowiednio szybkiej reakcji, a w konsekwencji bezkarnością przestępców. Istnieją jednak uregulowania pozwalające na międzynarodową współpracę w walce z cyberprzestępczością.

Ponadto, mając na uwadze fakt, że kontrola nie może mieć charakteru abstrakcyjnego, należy interpretować dopuszczalność stosowania podsłuchu w świetle ustanowionych zakresów, a interpretacja nie powinna mieć charakteru rozszerzającego uprawnienia organów władzy publicznej. Warto podkreślić, że ingerencja w podstawowe prawa człowieka może nastąpić jedynie w wypadkach, które mogą zostać uznane za konieczne w demokratycznym społeczeństwie. W doktrynie stwierdza się, że występuje większe przyzwolenie na stosowanie podsłuchu w zakresie zwalczania terroryzmu, czyli w przypadkach, gdy mamy do czynienia z daleko idącymi negatywnymi skutkami działań przestępczych, natomiast mniejsze dla przestępstw pospolitych (Szczechowicz, 2009). Należy zwrócić uwagę, że usprawiedliwieniem zarządzenia podsłuchu i związanym z tym wkroczeniem w sferę wolności obywatelskiej jest zapewnienie bezpieczeństwa i porządku publicznego. Zaznaczyć trzeba, że konieczne jest zachowanie zasady proporcjonalności, aby chronić prawo do prywatności i tajemnicę komunikowania się oraz nie dopuścić do nadużywania instytucji podsłuchu. Warto również podkreślić, że niezbędny jest odpowiedni system kontroli zachowania zasady proporcjonalności.

BIBLIOGRAFIA

Adamski, A. (2020). *Prawo karne komputerowe*. Warszawa: C.H. Beck.

Banaszak, B. (2012). *Konstytucja Rzeczypospolitej Polskiej. Komentarz*. Warszawa: C.H. Beck.

Chałubińska-Jentkiewicz, K., Nowikowska, M. (2020). *Bezpieczeństwo, tożsamość, prywatność – aspekty prawne*, Warszawa: Legalis.

Dudka, K., Paluszkiewicz, H. (2018). *Postępowanie karne*. Warszawa: Wolters Kluwer.

Garlicki, L. (2010). Komentarz do art. 8 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności. W: L. Garlicki (red.), *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności. Tom I. Komentarz do artykułów 1–18*. Warszawa: Legalis.

Golonka, A. (2016). Cyberprzestępczość – międzynarodowe standardy zwalczania zjawiska a polskie regulacje karne. *Studia Prawnicze. Rozprawy i Materiały, 1 (18),* 63–84.

Gryszczyńska, A. (2018). Karnoprawna ochrona danych przestrzennych wobec nowych zagrożeń związanych z rozwojem cyberprzestępczości. W: G. Szpor (red.). *Internet. Informacja przestrzenna. Spatial Information*. Warszawa: Legalis.

Hołyst, B. (2011). *Wiktymologia*. Warszawa: LexisNexis.

Hołyst, B. (2020). *Kryminologia*. Warszawa: Wolters Kluwer.

Jagiełło, D. (2019). *Taktyka kryminalistycznych czynności dowodowych*. Warszawa: C.H. Beck.

Jakubski, K.J. (1996). Przestępczość komputerowa – zarys problematyki. *Prokuratura i Prawo, 12*, 34–50.

Kmiecik, R. (2002). Przegląd orzecznictwa Sądu Najwyższego – Izby Karnej w zakresie zagadnień kryminalistyczno-dowodowych w postępowaniu karnym (w latach 1997–2001). *Prokuratura i Prawo, 7–8,* 46–48.

Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów „W kierunku ogólnej strategii zwalczania cyberprzestępczości" 22 maja 2007 r. Pobrane z: http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52007DC0267 (09.01.2021).

Kosmaty, P. (2008). Podsłuch komputerowy. Zarys problematyki. *Prokurator,4,* 34–48.

Marszał, K. (1996). Podsłuch w polskim procesie karnym de lege lata i de lege ferenda. W: L. Tyszkiewicz (red.).*Problemy nauk penalnych. Prace ofiarowane Pani Profesor Oktawii Górniok* (s. 345–355). Katowice: Wydawnictwo Uniwersytetu Śląskiego.

Piątek, S. (2013). *Prawo telekomunikacyjne. Komentarz.* Warszawa: C.H. Beck.

Rogalski, M. (2019). *Podsłuch procesowy i pozaprocesowy. Kontrola i utrwalanie rozmów na podstawie kpk oraz ustaw szczególnych.* Warszawa: LEX.

Rogowska, A. (2014). Wolność i ochrona tajemnicy komunikowania się. W: M. Jabłoński (red.), *Realizacja i ochrona konstytucyjnych wolności i praw jednostki w polskim porządku prawnym.* Pobrane z: https://www.bibliotekacyfrowa.pl/dlibra/publication/51986 (09.01.2021).

Siwicki, M. (2011). *Nielegalna i szkodliwa treść w Internecie. Aspekty prawnokarne*. Warszawa: LEX.

Siwicki, M. (2012). Podział i definicja cyberprzestępstw. *Prokuratura i Prawo, 7–8,* 241–251.

Siwicki, M. (2013). *Cyberprzestępczość*. Warszawa: C.H. Beck.

Skorupka, J. (2020). Komentarz do art. 237 k.p.k. W: J. Skorupka (red.), *Kodeks Postępowania Karnego, Komentarz*. Warszawa: Legalis.

Stefanowicz, M. (2017). Cyberprzestępczość – próba diagnozy zjawiska. *Kwartalnik policyjny*, *4*, 19–23.

Szczechowicz, K. (2009). *Podsłuch telefoniczny w polskim procesie karnym*. Olsztyn: Wydawnictwo UWM Olsztyn.

Wild, M. (2016). Komentarz do art. 49 Konstytucji RP. W: M. Sajfan, L. Bosek (red.), *Konstytucja RP, t. I, Komentarz do art. 1–86*. Warszawa: Legalis.

Wiliński, P. (2011). *Proces karny w świetle Konstytucji*. Warszawa: Wolters Kluwer.

Winczorek, P. (2008). *Komentarz do Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.* Warszawa: Liber.

Zakrzewski, R., Jarocha, W. (1997). Dopuszczalność stosowania kontroli korespondencji i podsłuchu. *Kontrola Państwowa*, *1*, 115.