# Dowód cyfrowy w procedurze karnej

## 1.1. Wprowadzenie

Zagadnienie dowodu cyfrowego w postępowaniu karnym podlegało już analizie i opisowi w literaturze, gdzie odnoszono się do jego elementów zarówno prawnych, jak i technicznych[26]. Nastąpił jednak dynamiczny rozwój form przestępczości i technologii informatycznych, a komputeryzacja społeczeństwa stała się faktem. Wraz z nią zmienił się także sposób postrzegania „danych komputerowych", które zatraciły walor nowości i swoistą obcość. Uzasadnia to ponowne spojrzenie na przedmiotowe zagadnienie i próbę przedstawienia jego uwspółcześnionego obrazu.

Omówienie praktycznych zagadnień związanych z dowodzeniem winy sprawcom przestępstw popełnionych z wykorzystaniem komputerów i sieci teleinformatycznych wymaga przybliżenia wielu podstawowych pojęć i zjawisk z tym związanych. Pojęcie „przestępczość komputerowa", z którym związane jest występowanie cyfrowego materiału dowodowego, stanowi zatem naturalny punkt wyjścia do dalszych dociekań. Z tego powodu przed przystąpieniem do zasadniczych rozważań przedstawiona została propozycja definicji przestępczości komputerowej w rozumieniu, jakie przypisane zostało temu pojęciu w ramach niniejszej publikacji.

Zagadnienie „dowodu cyfrowego" ma niezwykle istotne znaczenie praktyczne dla toczących się postępowań. Sposób, w jaki korzystamy współcześnie

[26] W szczególności należy wymienić w zasadzie jedyną polską publikację naukowo-prawniczą wyczerpująco opisującą to zagadnienie, tj. *Dowody elektroniczne w procesie karnym* A. Lacha. To wysokiej jakości opracowanie pozostaje pod wieloma względami aktualne, jednak opublikowane zostało w 2004 r., a więc przed ponad 15 laty, A. Lach, *Dowody elektroniczne w procesie karnym*, Toruń 2004.

ze sprzętów komputerowych, powoduje, że dowodem mogą być praktycznie dowolnego rodzaju dane utworzone w toku popełnienia czynu zabronionego[27]. Dowodami w sprawie karnej (lecz nie tylko – problematyka dowodów cyfrowych dotyczy przecież w równym stopniu procedury cywilnej) mogą być zarejestrowane konwersacje, wiadomości tekstowe, w tym zarówno pliki utworzone przez użytkowników celowo, jak i automatycznie wygenerowane przez system operacyjny. Nie ma w tym zakresie żadnych ograniczeń ani co do rodzajów danych mogących być dowodem, ani co do zakresu spraw karnych, w których mogą one odgrywać taką rolę[28].

Obecny stan jest w znacznej mierze realizacją przewidywań formułowanych w przeszłości, gdy „dowody cyfrowe" stanowiły w istocie *novum*. Na początku XXI wieku amerykańscy badacze i praktycy M. Noblett, M.M. Pollitt i L. Presley pisali, że „pamiętnik seryjnego mordercy może być dziś utrwalony prędzej na dyskietce lub dysku twardym niż w papierowym notatniku"[29]. To przewidywanie stało się rzeczywistością chociażby wówczas, gdy w 2009 r. masowy zabójca George Sodini śmiertelnie postrzelił 4 osoby i ranił 9 w ataku na centrum fitness w pobliżu Los Angeles. W czasie bezpośrednio poprzedzającym zdarzenie dokumentował przygotowania w formie dostępnego publicznie cyfrowego dziennika (bloga), w którym szczegółowo opisywał swoje plany[30]. Oczywiście, przykłady przydatności dowodów cyfrowych można z powodzeniem mnożyć. Niemniej warto pamiętać, że mogą one znaleźć zastosowanie nawet w najpoważniejszych sprawach karnych o dużym ciężarze gatunkowym, a zarazem niemających bezpośredniego związku ze sprzętami komputerowymi w zakresie znamionowym.

Zasadnicza część niniejszego rozdziału została poświęcona kompleksowemu opisowi „dowodu cyfrowego" w postępowaniu karnym na gruncie teoretycznym – technicznym i prawno-kryminalistycznym. W celu zachowania

[27] Jak również w razie wystąpienia dowolnej innej formy stadialnej czy zjawiskowej w odniesieniu do czynu zabronionego.

[28] W jednej z głośnych spraw karnych ostatnich lat istotną rolę poszlakową w sprawie o zabójstwo odgrywała historia wyszukiwań internetowych oskarżonej. Zob. nsz/mat, *Dowody prokuratury na winę Katarzyny W.*, TVN24 z 9 stycznia 2013 r., https://www.tvn24.pl/wiadomosci-z-kraju,3/dowody-prokuratury-na-wine-katarzyny-w,299053.html, dostęp 19 czerwca 2020 r.

[29] M. Noblett, M.M. Pollitt, L. Presley, *Recovering and Examining Computer Forensic Evidence*, „Forensic Science Communications" 2004, nr 2(4), https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/oct2000/computer.htm, dostęp 19 czerwca 2020 r.

[30] L. Mungin, *In diary, shooting suspect Soares despair, intent to kill*, CNN z 5 sierpnia 2009 r., http://edition.cnn.com/2009/CRIME/08/05/gym.shooting.diary/index.html, dostęp 19 czerwca 2020 r.; pełna treść dziennika sprawcy dostępna pod adresem: http://i.cdn.turner.com/cnn/2009/images/08/05/sodini.pdf, dostęp 19 czerwca 2020 r.

przejrzystości wywodu, jak i dla dochowania wierności aspektom technicznym rozstrzygnięte zostaną kwestie terminologiczne i definicyjne odnoszące się do rozgraniczenia pojęć o podstawowym znaczeniu, takich jak „dane" i „informacja" czy dane „cyfrowe" i „elektroniczne". Przy uwzględnieniu podziałów, wcześniej proponowanych w literaturze, określona zostanie także kryminalistyczno-procesowa klasyfikacja cyfrowego materiału dowodowego uwzględniająca wiele kryteriów o znaczeniu praktycznym. Opisom tym towarzyszy niezbędne objaśnienie zagadnień technicznych. Odnosi się to w szczególności do zjawisk fizycznych istotnych dla zrozumienia współczesnych metod zapisu danych i ich nośników.

## 1.2. Przestępczość komputerowa – kwestia definicji

W ciągu kilkudziesięciu lat rozwoju technologii komputerowych pojawiały się oraz zyskiwały i traciły popularność różne formy przestępstw i nadużyć związanych z użyciem sprzętu komputerowego. Z tego powodu problem „przestępczości komputerowej", oceniany z perspektywy nauk penalnych i w ujęciu historycznym, jest niejednolity i towarzyszy mu niezwykły wręcz chaos terminologiczny. Eufemizmem byłoby przy tym stwierdzenie, że w dotychczasowej literaturze przedmiotu nie ma powszechnie akceptowanej definicji tego, co najogólniej nazwać by można „przestępstwami i nadużyciami związanymi z użyciem komputera"[31]. To właśnie jednak z tak nieprecyzyjnie określanymi czynami najczęściej wiązane jest pojęcie „dowody cyfrowe". Związek pomiędzy ich występowaniem a faktem wykorzystania sprzętów komputerowych w ramach *modus operandi* sprawcy wydaje się oczywisty, stąd sformułowanie – chociażby doraźnej – definicji tego pojęcia jest celowe dla potrzeb niniejszej publikacji.

Opierając się wyłącznie na dotychczasowych opracowaniach literaturowych i dokumentach publicznych, nie sposób ustalić z całym przekonaniem, czym w istocie jest owa „przestępczość komputerowa" i czym (jeżeli w ogóle) różni się np. od „cyberprzestępczości", „przestępczości teleinformatycznej", „nadużyć komputerowych" czy „przestępczości związanej z komputerami" (historycznie bywały wykorzystywane i inne terminy, w tym zupełnie nietrafiające w technologiczny kontekst zjawiska, jak np. „przestępczość elektroniczna"[32]). Rozmaite postulaty definicyjne

[31] Ze względu na nieporozumienia, jakie przywoływanie takich ogólnych nazw wywoływało w dotychczasowej literaturze, należy podkreślić, że sformułowanie „przestępstwa i nadużycia związane z użyciem komputera" zostało w tym miejscu użyte jedynie roboczo. Mnogość rozmaitych nazw tego samego zjawiska lub doń zbliżonych powoduje, że trudno jest użyć określenia neutralnego, w żaden sposób nieodwołującego się do dotychczas wykorzystywanych.

[32] Zob. np. S. Amro, *Cybercrime in Saudi Arabia: fact or fiction?*, „International Journal of Computer Science Issues" 2017, nr 14(2), s. 37.

i przypisywane tym pojęciom zakresy znaczeniowe bywają sporne, niejasne, wzajemnie ze sobą sprzeczne, a niekiedy wprost błędne i świadczące o częściowym przynajmniej ich niezrozumieniu. Próby ujednolicania i porządkowania siatki pojęciowej podejmowane dotychczas w polskim piśmiennictwie[33] niestety nie są w tym zakresie w pełni wystarczające. Dla rozumienia tych pojęć w konkretnym czasie ważne były nierzadko okoliczności historyczno-społeczne, dlatego niewykluczone, że znaczenie pojęcia „przestępczość komputerowa" zasługuje na odrębne omówienie z takiej właśnie perspektywy. Pozostaje to jednak poza zakresem niniejszego opracowania.

Byłoby to znacznie mniej problematyczne z fenomenologicznego punktu widzenia, gdyby różnie brzmiącymi terminami na określanie tych samych zjawisk posługiwano się konsekwentnie. Niestety, tym samym wyrażeniom nadawane bywały krzyżujące się zakresowo lub przeciwstawne sobie znaczenia, przez co istniejąca siatka pojęciowa jest wyjątkowo niespójna i niejednorodna[34]. Biorąc pod uwagę zmieniające się przez lata formy sprawcze „przestępczości komputerowej", prawdą jest, że nie jest ona ani nigdy nie była zjawiskiem jednorodnym, co poniekąd uzasadnia posługiwanie się także innymi terminami o zbliżonym znaczeniu[35]. Już w 2000 r. trafnie podsumował to A. Adamski, pisząc, że „tego rodzaju bliskoznaczne pojęcia są często wykorzystywane w literaturze w znaczeniu operacyjnym i definiowane odnośnie do potrzeb danej publikacji, co wobec braku ogólnej definicji ustawowej takich czynów powoduje, że terminy te mają często bardziej publicystyczny niż naukowy charakter"[36].

Powyższe stwierdzenie z całą pewnością dotyczy terminu „cyberprzestępczość". Trafnie ironizuje J. Kosiński, pisząc, że przedrostek *cyber-* to „prefiks idealny, a większość czytelników i słuchaczy nie ma pojęcia, co znaczy, ale może on poprzedzać dowolne słowo, aby całość wydawała się atrakcyjna i jednocześnie dziwna, straszna lub naukowa"[37]. Stanowi to jego niewątpliwą zaletę w czasach, gdy niezbędne jest stosowanie prostych haseł wywoławczych dla wzbudzenia jakiegokolwiek zainteresowania poważnymi problemami.

Nie usuwa to jednak potrzeby zachowania precyzji językowej w ramach rozważań naukowych. Sama łatwość stosowania przedrostka *cyber-* wobec każdego możliwego problemu związanego z komputerami jest bez wątpienia

[33] Zob. m.in. postulaty podnoszone w: M. Siwicki, *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012, nr 7–8; J. Wasilewski, *Przestępczość w cyberprzestrzeni – zagadnienia definicyjne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, nr 15.

[34] J. Wasilewski, *Przestępczość…*, s. 150–151.

[35] Por. A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 30–33.

[36] A. Adamski, *Prawo…*, s. 30.

[37] J. Kosiński, *Paradygmaty cyberprzestępczości*, Warszawa 2015, s. 31.

cennym elementem jego sukcesu[38]. Wydaje się jednak, że jego powszechność wynikła bardziej z mody językowej utrwalonej w oficjalnych dokumentach (z których najdonioślejszym wydaje się być Konwencja o cyberprzestępczości[39], również jednak niedefiniująca tego terminu), niż z realnej potrzeby. Tworzone z jego użyciem terminy noszą więc znamiona nowomowy – nie mają jednoznacznych i ogólnie akceptowanych definicji, nie są niezbędne dla opisania istniejących zjawisk, a problemy z nimi związane są niemierzalne[40]. Istnieją jednak przesłanki stojące za tym, aby za *cyber*-przestępstwa uznać te, które mają związek z wykorzystaniem sieci teleinformatycznych[41], *a contrario* z wyłączeniem czynów związanych z wykorzystaniem komputera niepodłączonego do sieci. W tym znaczeniu pojęcie to bliskie jest również wykorzystywanemu, choć częściej już w przeszłości, pojęciu „przestępczość internetowa"[42] i takie jego rozumienie zostanie przyjęte w niniejszym opracowaniu.

Na marginesie tych rozważań warto jednak z całą mocą podkreślić, że jakiekolwiek inspiracje i powiązania etymologiczne przedrostka *cyber-* z nauką cybernetyki nie uzasadniają posługiwania się takimi terminami, jak: „przestępczość cybernetyczna", „wojna cybernetyczna", „uzbrojenie cybernetyczne"[43] „atak cybernetyczny"[44], nagminnie stosowanymi w przekazach medialnych,

[38] Wiele wskazuje na to, że swoją popularność w kontekście technologii sieciowych przedrostek ten zawdzięcza popkulturze lat 80. XX w.; to w jej ramach powstało – obecne dziś także w aktach normatywnych – pojęcie cyberprzestrzeni. Zob. J. Lillemose, M. Kryger, *The (Re)invention of Cyberspace*, Kunstkritikk z 24 sierpnia 2015 r., http://www.kunstkritikk.com/kommentar/the-reinvention-of-cyberspace/, dostęp 19 czerwca 2020 r.

[39] Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r., ratyfikowana przez Polskę w 2015 r. (Dz. U. z 2015 r. poz. 728).

[40] Trafny przegląd argumentów przeciwko powszechnemu stosowaniu terminów „cybercośtam" (cyt.) przedstawił K. Liderman, opierając się na zasadzie „brzytwy Ockhama", w: K. Liderman, *Bezpieczeństwo informacyjne*, Warszawa 2012, s. 60–66; K. Liderman, *Cyberprzestrzeń i inne „definicje"*, w: J. Kosiński (red.), *Przestępczość teleinformatyczna*, Szczytno 2015, s. 9–18.

[41] Na powiązanie istoty *cyber*-przestępczości z wykorzystaniem sieci teleinformatycznych wskazują m.in. częściowe definicje w regulacjach wewnętrznych, wykładnia językowa, a także wyniki badania opinii wśród ekspertów i biegłych informatyków. Zob.: § 16a ust. 1 zarządzenia nr 2 KGP z dnia 1 kwietnia 2016 r. w sprawie regulaminu Komendy Głównej Policji (Dz. Urz. KGP z 2016 r. poz 13 ze zm.). Por.: P. Ciszek, *Cyberprzestępczość i jej zwalczanie z innej perspektywy*, w: J. Kosiński (red.), *Przestępczość teleinformatyczna*, Szczytno 2015, s. 25–26; P. Ciszek, *Analiza percepcji cyberprzestępczości w środowisku eksperckim*, w: J. Kosiński (red.), *Przestępczość teleinformatyczna*, Szczytno 2016, s. 11–51.

[42] K. Gradoń, *Internet crime*, w: M.E. Beare (red.), *Encyclopedia of Transnational Crime and Justice*, Thousand Oaks, CA, 2012.

[43] J. Gawinecki, B. Hołyst, *Identyfikacja zagrożeń cyberprzestrzeni i przeciwdziałanie im*, w: B. Hołyst (red.), *Technika kryminalistyczna w pierwszej połowie XXI wieku – wybrane problemy*, Warszawa 2014, s. 13–15.

[44] Zob. m.in. *Zmasowany atak hakerów. Premier zwołała sztab kryzysowy*, „Newsweek" z 28 czerwca 2017 r., http://www.newsweek.pl/polska/atak-hakerow-zaatakowane-polskie-firmy,

a niekiedy też w publikacjach naukowych. Cybernetyka oraz informatyka jako dyscypliny naukowe zupełnie oddaliły się od siebie, a utożsamianie ich czy zamienne stosowanie w nazewnictwie jest całkowicie nieuprawnione i świadczy o niezrozumieniu i myleniu tych pojęć[45].

Aby zachować jednolitość siatki pojęciowej w ramach niniejszej publikacji i dla jej celów, jako punkt wyjścia proponuję przyjęcie uznanego na ogół przez praktykę i utrwalonego w literaturze polskiej podziału „przestępstw komputerowych" zaprojektowanego przez A. Adamskiego. Z perspektywy kryminalistycznej i procesowej najbardziej wartościowe jest opisane przez tego autora pojęcie „przestępstwo komputerowe w znaczeniu procesowym" – skupione wokół występowania w danej sprawie dowodów cyfrowych. Przedstawiona poniżej klasyfikacja stanowi zaś rozwinięcie i doprecyzowanie tego pojęcia (i niektórych innych).

Za najszersze należy uznać, także występujące w literaturze, pojęcie „nadużycia komputerowe". Są nimi wszystkie nieetyczne działania związane z użyciem komputera niezależnie od zakresu ich kryminalizacji (nadużyciem w tym sensie będzie zarówno przestępstwo *stricte* komputerowe, jak i np. prowadzenie „podwójnego życia" w Internecie). Tak rozumiane nadużycia też mogą znajdować się w kręgu zainteresowań organów ścigania – np. dostarczać informacji operacyjnych na temat planowanych przestępstw czy stanowić nowe zachowania, których kryminalizację należy rozważyć (czego przykładem może być przyjęcie stosunkowo niedawno art. 200a[46] Kodeksu karnego[47]).

Węższą, choć wciąż bardzo szeroką, kategorię stanowi pojęcie „przestępstwa komputerowe *sensu largo*" (lub: „przestępstwa związane z wykorzystaniem/użyciem komputera"). Odnosi się ono do niehomogenicznego zbioru przestępstw[48], w związku z którymi w dowolnym systemie informatycznym pozostaną dane istotne z punktu widzenia ścigania sprawcy lub dowodzenia jego winy. Z perspektywy kryminalistyczno-procesowej to ta grupa zdarzeń ma więc znaczenie dla omawianej problematyki

artykuly,412431,1.html, dostęp 19 czerwca 2020 r. Posługiwanie się, absolutnie błędnym, sformułowaniem „atak cybernetyczny" w publicznej przestrzeni medialnej jest przy tym nagminne.

[45] M. Szmit (red.), A. Baworowski, A. Kmieciak, P. Krejza, A. Niemiec, *Elementy informatyki sądowej*, Warszawa 2011.

[46] Przepis dodano ustawą z dnia 5 listopada 2009 r. o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego, ustawy – Kodeks karny wykonawczy, ustawy – Kodeks karny skarbowy oraz niektórych innych ustaw (Dz. U. z 2009 r. Nr 206, poz. 1589) – w celu dostosowania polskiego prawa do postanowień Konwencji Rady Europy z Lanzarote o ochronie dzieci przed seksualnym wykorzystaniem i niegodziwym traktowaniem w celach seksualnych (Dz. U. z 2015 r. poz. 608).

[47] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2020 r. poz. 1444 ze zm.), dalej: kk.

[48] A więc tylko czynów objętych kryminalizacją.

dowodów cyfrowych. W jej ramach wyróżnić można kilka wzajemnie niewykluczających się kategorii:

– „przestępstwa *stricte* komputerowe" – czyli zamachy skierowane na systemy, dane i programy komputerowe, w których stają się one przedmiotem przestępstwa (np. czyny polegające na włamaniu się do systemu informatycznego i zakłóceniu jego funkcjonowania). Obecność systemów informatycznych stanowi na ogół znamię takiego czynu, a jego popełnienie nie jest co do zasady możliwe poza środowiskiem komputerowym[49] (jak np. w przypadku czynu z art. 287 czy 269a k.k.);
– „przestępstwa komputerowe (przeciwko określonemu dobru chronionemu)" – czyli wszystkie czyny zabronione (nie wyłączając *stricte* komputerowych), w których system informatyczny stanowi narzędzie zamachu przeciwko dobru chronionemu i stanowi to znamię czynu zabronionego w myśl ustawy karnej, choć to samo przestępstwo mogłoby być popełnione również bez jego wykorzystania (np. w zakresie czynu z art. 267 kk);
– „inne przestępstwa komputerowe dla celów dowodowych" (lub przestępstwa z elementem komputerowym) – są kategorią obejmującą dwie powyższe kategorie oraz wszystkie pozostałe czyny, których znamienia ustawowego nie stanowi wykorzystanie systemu informatycznego (np. art. 286 § 1 kk), lecz mieszczących się w pojęciu „przestępstw komputerowych *sensu largo*" ze względu na powstanie w związku z ich popełnieniem[50] danych w formie cyfrowej o ewentualnym znaczeniu dowodowym. Będzie tak co do zasady w przypadku każdego przestępstwa, w toku którego wykorzystany został sprzęt komputerowy. Czyny tej kategorii mają więc najważniejsze znaczenie z punktu widzenia kryminalistyki, gdyż definiowane są poprzez powstanie dowodów cyfrowych przestępstwa.

Czyn należący do dowolnej z powyższych kategorii może jednocześnie stanowić *cyber*-przestępstwo lub nie – w zależności od tego, czy w realiach konkretnej sprawy została wykorzystana sieć teleinformatyczna, czy też czyn był popełniony wyłącznie offline. Mimo że współcześnie większość przestępstw tego typu popełniana jest z wykorzystaniem sieci (zwłaszcza

[49] Por. *Computer only crimes*, w: A.M. Marshall, B.C. Tompsett, *Spam 'n' chips – a discussion of Internet crime*, „Science and Justice" 2002, nr 42(2); H. Cornwall, *Datatheft, Computer Fraud, Industrial Espionage and Information Crime*, London 1990.

[50] Ale już nie bezpośrednio ze ściganiem – skorzystanie z systemu informatycznego przez przedstawicieli organów ścigania, m.in. w celu dla uzyskania danych osobowych w drodze sprawdzenia ich w policyjnej bazie danych, również pozostawi „istotne dowodowo dane" we właściwym systemie informatycznym, choć nie będą to dane podlegające badaniom kryminalistycznym.

Internetu)[51], prawidłowy podział logiczny powyższych kategorii terminologicznych wymaga uwzględnienia tej odrębności.

Zaproponowana klasyfikacja nie pretenduje do miana uniwersalnej i jedynej słusznej. Podobnie jak inne dotychczasowe, ma ona charakter konwencjonalny: przyjęty na użytek niniejszej publikacji. Jej celem jest uwypuklenie elementów „przestępczości komputerowej" istotnych z kryminalistycznego punktu widzenia, bez podziału na jej „materialne" i „procesowe" rozumienie zaproponowane przez A. Adamskiego. W pewnym więc uproszczeniu, zawsze gdy mowa będzie o „przestępstwach komputerowych" (bez wskazania ich konkretnego rodzaju), należy przyjąć, że zwrot ten dotyczy przestępstw komputerowych *sensu largo* – w których znaczenie dowodowe mają materiały pochodzenia cyfrowego. Na ogół będzie to oznaczało związek danego czynu z technologią komputerową w zakresie *modus operandi* lub w zakresie znamionowym, jednak niekoniecznie musi tak być.

## 1.3. Wokół pojęcia „dowód cyfrowy"

Z cyfrowym materiałem dowodowym związane są zdecydowanie mniejsze, niż w przypadku „przestępczości komputerowej", kontrowersje terminologiczne. Niemniej stosowane w ostatnich latach nazewnictwo również nie było jednolite. Potrzeba zachowania precyzji językowej, tak istotnej w naukach prawnych, wymaga przedstawienia uzasadnienia wyboru „dowodu cyfrowego" jako terminu poprawnego na gruncie procesowym i technicznym.

Nie bez znaczenia jest, że na początkowych etapach rozwoju przestępczości komputerowej najistotniejsze dla nauk penalnych były kwestie kryminalizacji nowych zachowań szkodliwych. Oczywiście, ogólną potrzebę uwzględnienia nowego rodzaju materiału dowodowego dostrzeżono stosunkowo wcześnie[52], jednak problem ten stanowił jedynie uzupełnienie dla rozważań materialnoprawnych. Posługiwano się wówczas niemalże wyłącznie pojęciem „dowód komputerowy" (ang. *computer evidence*) lub „dowód wygenerowany komputerowo" (ang. *computer-generated evidence*). Przez długi czas, przy ograniczonym zrozumieniu niszowej technologii, chodziło w zasadzie o jak najprostsze wskazanie faktu, że „dane z komputera" stanowią materiał dowodowy w sprawach „przestępstw komputerowych"[53]. Ograniczone

[51] Większość, lecz z całą pewnością nie wszystkie – co potwierdzają wyniki badania aktowego opisanego w rozdziale czwartym.

[52] Rozważania nad dopuszczalnością dowodów pochodzących z komputera prowadzono m.in. w Australii już w 1971 r., choć realne skutki tej debaty nastąpiły dopiero w latach 80. Zob. Law Reform Commision of Western Australia, *30th Anniversary reform implementation report*, Adelaide 2002, s. 90.

[53] D.B. Parker, *Computer Crime – Criminal Justice resource manual*, U.S. Department of Justice 1989, s. 66–68.

możliwości interfejsu pierwszych komputerów powodowały też, że wielokrotnie „dane komputerowe" były poddawane analizie po prostu w formie wydruków, które traktowano całkowicie dosłownie jako „dowody pochodzące z komputera". To uproszczone spojrzenie na problematykę „dowodu z komputera" zmieniało się wraz ze wzrostem dynamiki rozwoju przestępczości komputerowej, stopnia upowszechnienia technologii oraz jej możliwości praktycznych. Rozwój negatywnych zjawisk nie tylko wymuszał oficjalne ustosunkowanie się do związanych z tym problemów prawnych, lecz także wymagał wypracowania określonej terminologii. Z kolei rozwój techniki spowodował, że „dowody komputerowe" stawały się terminem stopniowo coraz bardziej przestarzałym i zastępowanym przez inne. Co ciekawe, bezpośrednim powodem odstąpienia od tego terminu było dostrzeżenie w połowie lat 90. XX wieku szerokiej gamy innych niż „komputery"[54] urządzeń elektronicznych, które mogły być źródłem danych o znaczeniu dowodowym. Uważano wręcz, że dalsze posługiwanie się terminem „dowód komputerowy" wykluczałoby z zakresu tego pojęcia dane pochodzące np. z telefonów komórkowych[55].

Z dzisiejszej perspektywy podejście takie może być uznane za błędne – rozwój techniki zatarł granice pomiędzy „komputerem osobistym" a „innym sprzętem elektronicznym". Jest to prawdą chociażby w odniesieniu do nowoczesnych telefonów komórkowych (z braku polskojęzycznego określenia – smartfonów), których możliwości obliczeniowe i przetwarzania danych są obecnie bardzo duże, wielokrotnie większe niż chociażby cała łączna moc systemów komputerowych wykorzystywanych przez NASA w końcu lat 60.[56] W poniekąd żartobliwy sposób zwrócił na to uwagę także B. Schneier, który, wspominając przebieg wymiany serwisowej komputera kontrolującego domową lodówkę, komentował, że „tak naprawdę to nie jest lodówka z komputerem, ale komputer przechowujący jedzenie w niskiej temperaturze. W taki oto sposób wszystko staje się komputerem"[57].

Zasadność ustanawiania definicji legalnej „komputera" w obliczu ciągle zmieniającej się technologii jest kwestią sporną. Niemniej jednak definicję

[54] Powszechne rozumienie, czym jest „komputer", zmieniało się jednak w czasie. Uważam zarazem, że o ile w latach 90. dostępne telefony komórkowe faktycznie różniły się od komputerów, o tyle współcześnie granice te uległy zatarciu. Niemniej jednak zwrot „dowód komputerowy" rzeczywiście jest mniej uniwersalny niż „dowód cyfrowy".

[55] A. Lach, *Dowody elektroniczne*…, s. 29; M. Reith, C. Carr, G. Gunsch, *An examination of digital forensic models*, „International Journal of Digital Evidence" 2002, nr 1(3).

[56] T. Puiu, *Your smartphone is millions of Times more powerful than all of NASA's combined computing in 1969*, http://www.zmescience.com/research/technology/smartphone-power-compared-to-apollo-432/, dostęp 19 czerwca 2020 r.

[57] B. Schneier, *Dane i goliat. Ukryta bitwa o Twoje dane i kontrolę nad światem*, przeł. J. Zatorska, Gliwice 2017, s. 21.

„systemu komputerowego" zawiera wiążąca Polskę Konwencja o cyberprzestępczości z 2001 r., zgodnie z którą jest to „każde urządzenie lub grupa urządzeń wzajemnie połączonych lub związanych ze sobą z których jedno lub więcej, zgodnie z programem, wykonuje automatyczne przetwarzanie danych"[58]. W anglojęzycznej wersji Konwencji posłużono się zwrotem *computer system*, jednak w oficjalnym jej tłumaczeniu na język polski, spójnie z terminologią stosowaną w ustawodawstwie krajowym, użyto terminu „system informatyczny". Podobne, choć nieidentyczne definicje umieszczone były także w art. 7 pkt 2a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[59] (obecnie już nieobowiązującej, zastąpionej ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych[60]) oraz w art. 2 pkt 3 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[61]. Nie są to niestety definicje w pełni czytelne ani też wolne od nieścisłości technicznych, wyrażających się chociażby niejasnym i nie w pełni uzasadnionym użyciem słowa „informatyczny". Niemniej jednak tym właśnie pojęciem stosunkowo konsekwentnie posługuje się także Kodeks karny w opisie szeregu czynów zabronionych, stąd utrzymanie jednolitości w tym zakresie należy uznać za słuszne.

W 2004 r. A. Lach, podsumowując stosowaną terminologię, zwracał uwagę na posługiwanie się w języku prawnym i prawniczym zamiennie takimi zwrotami, jak: „dowód elektroniczny", „dowód cyfrowy", „dowód komputerowy", „dowód wygenerowany komputerowo", „dowód utworzony na skutek działania komputera", „dowód pochodzący z komputera" czy „dowód IT"[62]. Autor opowiedział się zarazem za stosowaniem w rozważaniach prawniczych pojęcia „dowód elektroniczny" ze względu na jego użycie w niektórych

[58] Art. 1 lit. a Konwencji o cyberprzestępczości.

[59] System informatyczny to „zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych". Por. ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922).

[60] Dz. U. z 2019 r. poz. 1781.

[61] Systemem informatycznym jest „zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2019 r. poz. 2460 ze zm.)". Por. ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344), dalej: uśde.

[62] A. Lach, *Dowody elektroniczne*…, s. 28–29, m.in. za: A. Adamski, *Prawo karne komputerowe,* Warszawa 2000, s. 192; M.B. Andersen, *Digital evidence. The evidentiary weight of digital documents*, „Computer Law and Security Report" 2000, nr 16(2); E. Wilding, *Computer evidence: a forensic investigations handbook*, London 1997; C. May, *Computer-based evidence. The identification and recovery of evidence in electronic format*, „Computer Law and Security Report" 2000, nr 16(3).