Zagadnienia wstępne

Dynamiczny rozwój Internetu oraz sprzętu komputerowego zaczyna mieć dominujący wpływ na życie społeczne, ekonomiczne i polityczne. Rozwój technologii pozwolił na odnoszenie znacznych korzyści materialnych przez producentów i konsumentów korzystających z nowych udogodnień, jakich dostarcza Internet. Szybszy dostęp do informacji i przesyłanie danych czy możliwość połączenia się z Internetem praktycznie z każdego miejsca na świecie staje się wymogiem współczesnych czasów. Niestety równolegle z idącym postępem technologicznym powstają także nowe zagrożenia i patologie. Współczesne społeczeństwo jest uzależnione od komunikacji i dostępu do informacji. W dzisiejszych czasach obywatel nowoczesnego państwa jest osobą zazwyczaj posiadającą pracę, wykształcenie, miejsce zamieszkania, samochód, telefon komórkowy i komputer z dostępem do Internetu. Szansa na to, że taka osoba padnie ofiarą przestępstwa komputerowego, jest dziesięciokrotnie wyższa niż to, że zostanie okradziony w tradycyjny sposób[1]. Na początku lat 90. XX w. dostęp do Internetu posiadało około 3 milionów osób, z czego 73% pochodziło z USA, zaś 15% z Europy Zachodniej. Pozostała część użytkowników zamieszkiwała w Kanadzie, Australii, Japonii, Republice Korei i Izraelu. W ciągu dziesięciu lat liczba użytkowników Internetu wzrasta do około 369 milinów osób. W 2010 roku szacuje się, że ta liczba przekroczyła dwa miliardy użytkowników Internetu, pięć miliardów telefonów komórkowych, 255 miliardów stron internetowych, dziennie wysyła się ponad 294 milionów wiadomości elektronicznych e-mail i 5 miliardów wiadomości SMS[2]. Najnowsze dane użytkowników Internetu prezentują się następująco:

---

1 Por. W. Orliński: *Internet czas się bać*, Warszawa 2013.

2 M. Siwicki: *Cyberprzestępczość*, Warszawa 2013, s. 9

Tab. 1. Dane statystyczne wzrostu liczby użytkowników Internetu w latach 2000–2012 r.[3]

Regiony	Populacja (2012 r.)	Użytkownicy Internetu (31.12.2000 r.)	Użytkownicy Internetu **(30.06.2012 r.)**	Populacja %	Przyrost 2000–2012
Afryka	1,073,380,925	4,514,400	**167,335,676**	15,6%	3.606,7%
Azja	3,922,066,987	114,304,000	**1,076,681,059**	27,5%	841,9%
Europa	820,918,446	105,096,093	**518,512,109**	63,2%	393,4%
Bliski Wschód	223,608,203	3,284,800	**90,000,456**	40,2%	2.639,9%
Ameryka Północna	348,280,154	108,096,800	**273,785,413**	78,6%	153,3%
Ameryka Łacińska/ Karaiby	593,688638	18,068,919	**254,915,745**	42,9%	1.310,8%
Oceania/Australia	35,903,569	7,620,480	**24,287,919**	67,6%	218,7%
Świat łącznie	**7,017,846,922**	**360,985,492**	**2,405,518,376**	**34,3%**	**566,4%**

Razem z tak dużym wzrostem popularności Internetu rośnie także liczba popełnianych przestępstw za pośrednictwem sieci. Współczesny przestępca wykorzystuje komputer jako narzędzie do popełnienia przestępstwa, a cyberprzestrzeń jest „miejscem" jego popełnienia. Z uwagi na niezwykłą specyfikę miejsca popełnienia przestępstwa trzeba zaznaczyć, iż cyberprzestrzeń jest określeniem zbiorczym dla całości materii wirtualnej, w skład której wchodzi: Internet, sieci telefoniczne, sieci komputerowe i inne powiązane ze sobą urządzenia teleinformatyczne zdolne do przechowywania, wysyłania i odbierania materiałów cyfrowych. Trudność w zrozumieniu samej specyfiki cyberprzestrzeni jako miejsca popełnienia czynu przestępnego leży u podstaw konstrukcyjnych tej przestrzeni. Cyberprzestrzeń jest miejscem niematerialnym, ale odbijającym się w świecie rzeczywistym i wpływającym na jego zachowanie. Dodatkowo jest tworem ponadgranicznym i nieposiadającym swoistego centrum, ponieważ jako całość stanowi wszystkie połączone ze sobą urządzenia teleinformatyczne zdolne do wzajemnej komunikacji. Z punktu widzenia prawnego kwestie uregulowania i kontrola takiej przestrzeni bez konfliktów na tle prawa międzynarodowego i różnic w interpretacji przepisów przez przedstawicieli różnych państw jest niemożliwa. Sprawowanie kontroli w cyberprzestrzeni wymagałoby bowiem wprowadzenia ujednoliconego systemu prawnego dla wszystkich państw na świecie. Dlatego też, mimo iż samo wykrycie sprawstwa popełnienia czynu zabronionego nie jest trudne, to jednak już wyegzekwowanie konsekwencji prawnych wobec osoby popełniającej przestępstwo i doprowadzenie jej przed oblicze sądu okazuje się niezwykle trudne. Wystarczy, że sprawca popełniający przestępstwo kradzieży informacji z polskiej witryny strony internetowej jest mieszkańcem np. regionu Oceanii.

Problematyka, jaką jest badanie śladów cyfrowych jako pozostałości po dokonaniu przestępstwa i znajomość metodyki pracy biegłych z zakresu informa-

[3] http://www.internetworldstats.com/stats.htm.

tyki śledczej, jest stosunkowo słabo znana (*Computer forensic science*)[4] przez prawników i pracowników organów ścigania. Do skutecznego współdziałania kryminalistyki i procesu karnego wymagane jest poznanie podstaw funkcjonowania systemów komputerowych i praw nimi rządzących, a także lepsze zaznajomienie się z przepisami i terminologią prawną przez biegłych informatyków. W trakcie badań i studiowania literatury, zarówno prawniczej, jak i informatycznej, natknięto się na znaczne nieścisłości wynikające z braku zrozumienia przez autorów jednej z w/w dziedzin naukowych. W książkach informatycznych mylenie takich pojęć, jak ślad i dowód czy też stosowanie ich zamiennie w odniesieniu do tego samego elementu, jest nagminne. Z drugiej strony brak jest w polskiej literaturze fachowej pozycji poświęconej prawnym i kryminalistycznym zagadnieniom informatyki śledczej. W większości z badanych opracowań poświęconych kryminalistyce istnieją zapisy dotyczące śladów, jakie powstają przy użytkowaniu komputera i innych urządzeń cyfrowych. Problem jednak powstaje w momencie, gdy uświadamiamy sobie, że wiele z tych pozycji opisuje stan z okresu 2000 roku lub wcześniejszy. W momencie, gdy zwrócimy teraz uwagę na dane statystyczne zamieszczone w tabeli nr 1 opracowania, zobaczymy, jak bardzo rozwinęła się idea cyfryzacji społeczeństwa. Aspekty kryminalistyczne, na które zwracało się uwagę w roku 2000, dziś mogą nie mieć już zupełnie znaczenia. Zaczynamy żyć w czasach, gdzie zwykły telefon komórkowy (*smartfon*) staje się równie szybkim urządzeniem w przeprowadzaniu obliczeń, co komputer domowy. Przykładowo przestępca w dzisiejszych czasach coraz rzadziej będzie montował skaner na czytniku w bankomacie, by uzyskać dane karty magnetycznej, ponieważ będzie starał się przechwycić za pomocą komputera połączenie naszego telefonu komórkowego, łączącego się z bankiem, w celu uzyskania kodów dostępu i innych newralgicznych danych narażających potencjalnego obywatela na straty.

Niezwykle istotnym zabiegiem jest obecnie podniesienie rangi śladu cyfrowego we współczesnej kryminalistyce i postawienie go na równi z innymi rodzajami śladów. Kryminalistyka nie wyróżnia śladów mniej ważnych od tych bardziej ważnych[5], dlatego istotnym faktem jest konieczność poszerzenia i rozwijania naszej wiedzy także w kierunku zagadnień cyfrowych. Kryminalistyka jako nauka interdyscyplinarna potrafi adaptować dla swojej korzyści rozwiązania i metody innych dyscyplin wiedzy[6]. Z ogólnodostępnej literatury wynika, że kryminalistyka jest pojmowana powszechnie przez autorów jako nauka zajmująca się wy-

---

[4] R.C. Newman: *Computer Forensics Evidence Collection and Management*, Auerbach Publication, USA 2007, s. 5.

[5] J. Kasprzak: *Cheiloskopia kryminalistyczna,* Warszawa 1991, s. 6.

[6] E. Gruza, M. Goc, J. Moszczyński: *Kryminalistyka – czyli rzecz o metodach śledczych*, Warszawa 2008, s. 19.

krywaniem przestępstw, ściganiem sprawców i zapobieganiem przestępstwom[7]. Wykorzystywanie takich elementów, jak badania fizyko-chemiczne, balistyczne, fonoskopijne, daktyloskopijne i wiele innych, stawia kryminalistykę jako priorytetową dziedzinę nauk śledczych. Pojmowanie kryminalistyki w jak najszerszym znaczeniu sprzyja jej rozwojowi, ponieważ nauka ta jest dziedziną bardzo wszechstronną i dynamicznie dostosowuje się do coraz to nowszych rodzajów przestępstw. W drodze ewolucji paradygmatu kryminalistyki[8] w celu lepszego zapobiegania i wykrywania przestępstw elektronicznych konieczne jest szersze otwarcie się tej dziedziny na nowe trendy technologiczne i coraz szybszy postęp cyfrowy.

Celem niniejszej pracy jest przedstawienie istoty śladu cyfrowego jako pozostałości po dokonaniu przestępstwa w systemie teleinformatycznym i dodanie do istniejących rodzajów śladów funkcjonujących w kryminalistyce śladu cyfrowego w celu pokazania możliwości zwalczania działalność cyfrowej przestępców, stanowiących istotne zagrożenie dla codziennego życia społecznego. Należy podać charakterystykę i określić rodzaje śladów cyfrowych oraz sklasyfikować je pod kątem przydatności dla pracy śledczej. Każdy funkcjonujący rodzaj śladu w kryminalistyce wymaga odrębnej metody zabezpieczania w celach późniejszej analizy i badań dokonywanych przez biegłego. Nie inaczej jest w przypadku śladów cyfrowych. Praca przedstawia metody ujawniania i zabezpieczania śladów cyfrowych, ze szczególnym uwzględnieniem zasad procesowych zabezpieczania śladu. Z uwagi na bardzo specyficzny charakter śladów cyfrowych wymagana jest zupełnie inna metodyka zabezpieczania i badań zabezpieczonego już śladu cyfrowego. Dlatego w pracy przedstawiono ogólną problematykę poprawnego wykonania ekspertyzy śladów cyfrowych. Materiał dowodowy uzyskany z wyników ekspertyzy śladów cyfrowych bywa niekiedy podważany w trakcie trwania procesu jako ślad niepewny i podatny na zniekształcenie, zniszczenie i zatarcie. Dlatego też stałe tworzenie, uaktualnianie i dokładne trzymanie się w tym zakresie przyjętych procedur wydaje się konieczne.

Zakres pracy obejmuje całokształt ogólnej problematyki kryminalistycznej dotyczącej śladów cyfrowych, przedstawia charakterystykę i istotę tych śladów, sposoby i procedury ich zabezpieczania i badania przez biegłego, a także wykorzysta-

---

[7] P. Horoszowski: *Kryminalistyka*, Warszawa 1958, s. 13; J. Sehn: *Kryminalistyka a prawo procesowe*, „Nowe Prawo", 1958, nr 6; W. Gutekunst: *Kryminalistyka, zarys systematycznego wykładu*, Warszawa 1974, s. 21, Z. Czeczot, M. Czubalski: *Zarys kryminalistyki*, Warszawa 1972, s. 9 i nast., M. Kulicki: *Kryminalistyka, Wybrane zagadnienia teorii i praktyki śledczo-sądowej*, Toruń 1994, s. 41, Z. Czeczot, T. Tomaszewski: *Kryminalistyka ogólna,* Toruń 1996, s. 16., T. Hanausek: *Kryminalistyka, zarys wykładu*, Kraków 1996, s. 14., K. Sławik: *Kryminalistyka. Przegląd zagadnień,* Warszawa 2002, s. 15, red. J. Widacki: *Kryminalistyka*, Warszawa 2008, s. 4 i nast., B. Hołyst: *Kryminalistyka*, Warszawa 2010, s. 41.,

[8] J. Konieczny: *Kryzys czy zmiana paradygmatu kryminalistyki?*, „Państwo i Prawo", Warszawa 2012, nr 1, s. 19.

nia ich w działaniach wykrywczych i w procesie dowodzenia. Przeprowadzenia badań wymagało również określenie, jak sądy odnoszą się do śladów cyfrowych jako materiału dowodowego i prezentowanej przez biegłego opinii w tym zakresie. Oddzielny problem stanowią metody i szczegółowe techniki wykonywania ekspertyz śladów cyfrowych. W tym przypadku stosowana metodyka badawcza jest na poziomie bardzo wysokiej specjalizacji w zakresie informatyki. Autor, będąc prawnikiem i kryminalistykiem, nie jest w stanie przedstawić szczegółowo metod i technik badawczych śladów cyfrowych w ramach ekspertyzy. Wynika to z ogromnej różnorodności badanych śladów cyfrowych, różnorodności badanego sprzętu, a także z różnorodności i technicznej komplikacji stosowanych przez biegłego metod. Kolejną kwestią jest fakt szybkiego i stałego rozwoju stosowanych metod. Każdy rok przynosi w zakresie badań śladów cyfrowych nowe technologie i nowe metody. Autor więc musiał się odnieść przy omawianiu ekspertyzy śladów cyfrowych do zagadnień prawnych (często nieznanych i ignorowanych przez biegłych informatyków, a niezmiernie ważnych dla organu procesowego) oraz do omówienia zakresu ogólnych możliwości badawczych danego rodzaju śladów, wskazując na szczegółową technologię badawczą jedynie przykładowo.

Zadaniem badań naukowych jest ujawnienie nowych prawd i tworzenie nowych teorii naukowych[9]. Wiedza oraz działalność ludzka zawarta w systemie nauki jest złożona, wielostronnie uwarunkowana, dlatego też jedynie świadome i celowo zastosowane procedury badawcze są w stanie zapewnić podstawowe funkcje badań naukowych[10].

Rozróżnienie metod badawczych, technik i narzędzi badawczych ma charakter umowny i jest w nauce w różnorodny sposób interpretowane[11]. Nie wdając się w tym zakresie w szczegółowe rozważania, należy stwierdzić, iż dana metoda badawcza posługuje się określonymi technikami, a do praktycznej realizacji techniki służą dane narzędzia. Te same techniki i narzędzia badawcze mogą być stosowane w różnych metodach[12]. W przedmiotowej pracy wykorzystywano następujące metody badawcze specyficzne dla kryminalistyki[13]:

– badania literatury,
– badania źródeł prawa,
– badania aktowe,

---

9 Por. J. Apanowicz: *Metodologia nauk,* Toruń 2003, a także J. Pieter: *Zarys metodologii pracy naukowej,* Warszawa 1975, T. Pilch: *Zasady badań pedagogicznych,* Warszawa 1995.

10 J. Apanowicz: *Metodologiczne uwarunkowania pracy naukowej,* Warszawa 2005.

11 Por. K. Ajdukiewicz: *Logika pragmatyczna,* Warszawa 1975., J. Antoszkiewicz: *Metody heurystyczne. Twórcze rozwiązywanie,* Warszawa 1990., T. Kotarbiński: *Elementy teorii poznania, logiki formalnej i metodologii nauk,* Warszawa 1986.

12 J. Kasprzak: *Wybrane problemy metodologiczne badań w zakresie procesu karnego i kryminalistyki,* [w:] *Wybrane problemy procesu karnego i kryminalistyki,* red. J. Kasprzak, B. Młodziejowski, Olsztyn 2010, s. 12.

13 J. Kasprzak: op. cit., s. 12.

– badania materiałów statystycznych,
– wywiad, ankieta, rozmowa,
– badania laboratoryjne.

Badania literatury obejmowały studiowanie pozycji z zakresu kryminalistyki, kryminologii, prawa (szczególnie prawa karnego, postępowania karnego, prawa internetowego), a także z zakresu informatyki. Wykorzystywano pozycje w języku polskim, angielskim i rosyjskim. Wiele informacji zaczerpnięto także ze stron internetowych.

Badania źródeł dotyczyły analizy obowiązującego, jak i dawnego prawa karnego, prawa internetowego (w Polsce i za granicą), analizy orzecznictwa sądów, a także wytycznych i Dyrektyw Unii Europejskiej.

Badania aktowe przeprowadzono w Sądzie Okręgowym w Warszawie, Sądzie Okręgowym w Olsztynie, Sądzie Okręgowym w Gdańsku i Sądzie Okręgowym w Łodzi. Badania obejmowały sprawy zakończone prawomocnym wyrokiem w latach 2010–2013. Analiza badanych akt prowadzona była dwutorowo: pierwszą grupę stanowiły przestępstwa „typowo komputerowe" – takich spraw zbadano łącznie 64 (z wymienionych sądów). Drugą grupę badanych akt stanowiły wybrane z repertoriów sprawy z podanych wyżej sądów w badanym okresie (wybierano ze wszystkich prowadzonych spraw). Wybierano losowo po 200 spraw z każdego sądu. W każdej też sprawie ankietyzowano akta. Celem badań pierwszej grupy było określenie *modus operandi* sprawcy, ustalenie rodzaju przestępstwa „komputerowego", sposobu ujawnienia, rodzaju i sposobu zabezpieczenia śladów cyfrowych, wykonywane w sprawie ekspertyzy tych śladów, ich znaczenie dowodowe i wpływ śladów cyfrowych na decyzję procesową sądu, przede wszystkim w postaci wyroku. W drugiej grupie badawczej dobór spraw był losowy (przypadkowy), zbadano z wymienionych sądów łącznie 800 spraw. Sprawy te dotyczyły różnych przestępstw (szczegółowy wykaz w rozdziale VIII). W tak badanych sprawach chodziło o ustalenie, czy w ogóle pojawia się w niej ślad cyfrowy, jakiego rodzaju to ślad, jakie ma znaczenie dla ustalenia faktycznych okoliczności sprawy, jak był ujawniony i zabezpieczony, jakiego rodzaju ekspertyzy były prowadzone. W badanych 800 sprawach występowanie śladów cyfrowych stwierdzono w 564 (co stanowi 70,5% badanych spraw, dokładne dane rozdział VIII). Oceniając reprezentatywność tej próby, można posłużyć się kategoriami przyjętymi w naukach statystycznych. Próbę uznaje się za reprezentatywną, gdy próbka Z1 stanowi reprezentację populacji Z w tym sensie, że częstość występowania w próbce każdego z badanych elementów nie powinna różnić się znacznie od częstości występowania tych elementów w populacji generalnej. W sytuacji, gdy niemożliwe (bądź bardzo kosztowne) byłoby przebadanie wszystkich elementów populacji Z, można przyjąć, że próba jest reprezentatywna, gdy elementy próbki Z1 są wybierane ze zbioru Z w sposób losowy. Innymi słowy, gdy prawdo-

podobieństwo *a priori* wylosowania każdego elementu populacji generalnej przed losowaniem było takie samo[14].

W prowadzonych badaniach analizowano także dane statystyczne dotyczące liczby użytkowników Internetu, dane odnośnie jego funkcjonowania, a także dane dotyczące danego rodzaju przestępstw.

Metodą badawczą pozwalającą uzyskać bardzo cenne informacje był wywiad przeprowadzony przy wykorzystaniu ankiety[15] z 64 sędziami, 113 prokuratorami, 42 adwokatami i 365 funkcjonariuszami policji, dotyczący przede wszystkim ich znajomości problematyki śladów cyfrowych i ich praktycznego wykorzystania.

Wiele cennych informacji uzyskano także podczas licznych rozmów i konsultacji z ekspertami z zakresu badań śladów cyfrowych z Wyższej Szkoły Policji w Szczytnie, z Centralnego Laboratorium Kryminalistycznego Policji w Warszawie oraz z Laboratorium Kryminalistycznego Komendy Wojewódzkiej Policji w Olsztynie, a także z przedstawicielami prywatnych instytucji, które wykonują badania sprzętu łączności i badania sprzętu komputerowego.

Praca zawiera zagadnienia wstępne, dziewięć rozdziałów merytorycznych i wnioski. W rozdziale I przedstawiona została definicja śladu cyfrowego i jego charakter we współczesnym świecie. Nie jest możliwe przedstawienie wyników badań nad tego typu śladem bez dogłębnego przedstawienia jego specyfiki i faktów, które determinują tego rodzaju ślady do rangi bardzo istotnych we współczesnej kryminalistyce. Przedstawiono ewolucję pojęcia śladu w kryminalistyce i klasyfikację śladów. Opisano także proces powstawania śladów kryminalistycznych. W trakcie opisywania śladu cyfrowego zaznaczono istotę i charakter takiego śladu. Każde urządzenie teleinformatyczne jest w stanie pozostawić ślady swojej pracy. Dodatkowo każde działanie człowieka w cyberprzestrzeni pozostawia różnego rodzaju ślady cyfrowe, mogące posłużyć do udowodnienia sprawcy popełnienia przestępstwa lub będące późniejszymi dowodami potwierdzającymi przedstawione alibi przez podejrzanego. Potencjał wykorzystania śladów cyfrowych wydaje się być niezwykle szeroki. We współczesnym systemie pracy policji, gdzie zanikła bariera opóźnienia komunikacyjnego i porównanie wyników badań odbywa się drogą elektroniczną, ślady cyfrowe zaczynają nabierać bardzo istotnych cech wykrywczych. Organy ścigania są w stanie uzyskać informację na

---

[14] W. Krysicki, J. Bartos, W. Dyczka, K. Królikowska, M. Wasilewska: *Rachunek prawdopodobieństwa i statystyka matematyczna w zadaniach,* cz. II, Warszawa 1997, s. 5, por. Z. Hellwig: *Elementy rachunku prawdopodobieństwa i statystyki matematycznej,* Warszawa 1998, s. 188–194, Cz. Nowaczyk: *Podstawy metod statystycznych dla pedagogów,* Warszawa – Poznań 1985, s. 133, P.J. Good: *Applying Statistics in the Courtroom,* New York 2001, s. 17.

[15] Por. K. Lutyńska: *Wywiad kwestionariuszowy. Przygotowanie i sprawdzanie narzędzia badawczego,* Wrocław – Warszawa – Kraków – Gdańsk – Łódź 1984., a także K. Lutyńska, A.B. Wejland: *Wywiad kwestionariuszowy. Analizy teoretyczne i badania empiryczne,* Wrocław – Warszawa – Kraków – Gdańsk – Łódź 1983.

temat miejsca pobytu, działalności, kontaktów i prowadzonej aktywności w Internecie właśnie za pośrednictwem pozostawionych śladów cyfrowych.

W rozdziale II zostało szczegółowo omówione zagadnienie cyberprzestrzeni jako materii, w której dokonywane jest przestępstwo i w której odnajdywane są ślady cyfrowe. W dzisiejszych czasach komputer lub inne urządzenie cyfrowe, np. telefon, może być uznane za potencjalne narzędzie popełnienia przestępstwa w cyberprzestrzeni. Dokładne sklasyfikowanie i podzielenie zakresu cyberprzestrzeni jest wymagane do precyzyjnego zrozumienia całości problematyki nowoczesnych przestępstw komputerowych. Przedstawiona została zatem historia powstania pierwszych sieci komputerowych ARPA-NET i stopniowa ewolucja w kierunku dziś znanego wyglądu sieci nazywanego Internetem. Przestępstwa komputerowe istniały już w przeszłości w fazach, gdy Internet nie wychodził poza granice Stanów Zjednoczonych Ameryki. Niesamowity rozwój technologii i postęp sprawił, że Internet jest najchętniej odwiedzanym miejscem przez społeczeństwo w historii. Dokładnie przedstawiony i przeanalizowany został także stan obecny Internetu, jak i samej cyberprzestrzeni na tle kontroli i funkcjonowania w różnych państwach na świecie. Rozdział zawiera także przewidywania i szacowane kierunki rozwoju Internetu. Przyszły rozwój jest jednym z kluczowych elementów skutecznej walki z cyberprzestępcami, gdyż pozwoli wskazać sektory najbardziej narażone na atak i te kierunki działań o cechach przestępczych, które mogą w znaczącym stopniu zaburzyć poprawne funkcjonowanie wielu jednostek w społeczeństwie. Na koniec omówione zostały istniejące patologie w cyberprzestrzeni, głównie w Internecie. Jednymi z największych zagrożeń w dzisiejszych czasach są problemy z kwestiami terroryzmu, pedofilii, pornografii, oszustw bankowych, kradzieży w Internecie, nękania, łamania praw autorskich, pułapek finansowych i wielu innych obszarów patologii, z jakimi walczą przedstawiciele organów ścigania.

W rozdziale III przedstawione i przeanalizowane zostały akty prawa krajowego dotyczące kontroli cyberprzestrzeni. Poza aktami odnoszącymi się bezpośrednio do tematyki Internetu, omówione zostały również przepisy kodeksu karnego penalizujące zachowania przestępcze w Internecie. Dużym problemem w dzisiejszym prawie polskim jest brak ujednoliconych przepisów dotyczących narastającego problemu rosnącej przestępczości w Internecie. Największymi problemami, z którymi boryka się ustawodawstwo, są zagadnienia łamania praw autorskich i obecność tak zwanej szarej strefy użytku komercyjnego. Drugim rodzajem działalności przestępczej sprawiającej organom ścigania duże problemy jest piractwo komputerowe. Szacuje się, że blisko 50% oprogramowania obecnego w komputerach domowych i innych urządzeniach cyfrowych wyposażonych w systemy operacyjne (nowoczesne telefony, tablety) pochodzi z nielegalnego źródła. W polskim systemie państwowym brak jest wyspecjalizowanej komórki do zwalczania stron, za pośrednictwem których rozpowszechniane są pirackie wersje oprogra-

mowania, filmy, gry i muzyka. Główną przyczyną takiego stanu rzeczy, który został w rozdziale dogłębnie opisany, jest fakt rejestrowania działalności takich nielegalnych stron na serwerach poza granicami naszego państwa. Dzięki takiemu zabiegowi można ominąć częściowo obowiązujące przepisy prawa polskiego. Trzecim i potencjalnie najbardziej niebezpiecznym są oszustwa międzynarodowe, gdzie za pośrednictwem Internetu obywatele są „naciągani" na metodę tzw. „wnuczka" z dalekiego kraju, który znalazł się w potrzebie, pozostawienia dużego spadku przez dalekiego wujka w kraju trzeciego świata i poniesienie „drobnych" kosztów manipulacyjnych w celu odebrania spadku. W rozdziale poza omówieniem sytuacji prawnej na terenie Polski, przebadano i przeanalizowano również ustawodawstwo i regulacje obowiązujące w wybranych krajach należących do Unii Europejskiej. Zagadnienie kontroli i regulacji prawnych cyberprzestrzeni, a w szczególności Internetu, jest inne w każdym z omawianych w rozdziale państw. Pokazany jest więc główny problem współczesnego świata walczącego z plagą przestępstw komputerowych, ponieważ brakuje wydajnych i skutecznych metod przeciwdziałania. Dysproporcje ustawodawstwa w poszczególnych krajach są na tyle duże, że często zdarza się, iż prowadzona sprawa trwa miesiącami lub latami, głównie przez różnice w interpretacji obowiązujących przepisów na terenie wybranych krajów. W rozdziale znalazło się również obmówienie wybranych krajów i ich regulacji prawnych spoza rejonu Unii Europejskiej, takich jak Stany Zjednoczone Ameryki, Rosja i Chiny.

W rozdziale IV został dokładnie przedstawiony i omówiony mechanizm powstawania śladów cyfrowych. Specyfika pracy przy komputerze i użytkowania innych urządzeń cyfrowych łączy się zawsze z pozostawieniem śladów będących rezultatem takiej działalności w systemie i pamięci urządzenia. Śladami cyfrowymi mogą być pliki, zapisy logów komputerowych, adresy IP, daty logowania się urządzenia, bilingi telefoniczne, historia rozmów w komunikatorach internetowych itp. W rozdziale przedstawiono również koncepcje obecności śladów cyfrowych w kontekście *modus operandi* sprawcy czynu zabronionego. Działalność przestępców dokonujących kradzieży i operujących komputerem jako narzędziem popełniania przestępstwa nie różni się wbrew pozorom tak bardzo od klasycznego dokonania kradzieży w rozumieniu kodeksu karnego. W takim przypadku również istnieje pewna grupa cech i czynności, jakie wykonuje sprawca w celu przygotowania się do popełnienia przestępstwa i w momencie samego jego popełnienia. Podjęto się stworzenia spójnych opisów poszczególnych modeli *modus operandi*, w kontekście różnych typów przestępstw, do których dochodzi w cyberprzestrzeni. W rozdziale został opisany także niezwykle istoty aspekt, jakim jest trwałość i podatność na ingerencje zewnętrzne samego śladu cyfrowego. Tak jak w przypadku każdego rodzaju śladów, ślad cyfrowy również możne ulec zniszczeniu. Można zaryzykować nawet stwierdzenie, że ślad cyfrowy należy do grupy śladów niezwykle wrażliwych na wszelkie ingerencje ze-

wnętrzne. Odnosi się to bezpośrednio do stanu śladu cyfrowego przed ujawnieniem, po jego ujawnieniu, w trakcie zabezpieczania i analizie po zabezpieczeniu. Na każdym z wymienionych etapów ślad cyfrowy może zostać zniekształcony nawet do takiego stopnia, że stanie się bezużyteczny dla organu ścigania. Z drugiej jednak strony ślad cyfrowy jako jeden z nielicznych śladów można uznać – paradoksalnie do wcześniejszego opisu – jako ślad trwały. Powodem takiej dysproporcji w opisie jest fakt, że całkowite zatarcie, wymazanie, zniszczenie dowodów naszej działalności w cyberprzestrzeni można uzyskać jedynie przez fizyczne uszkodzenie nośnika danych i całkowite jego zniszczenie mechaniczne. W innym przypadku zawsze w systemie pozostanie informacja o wcześniejszej ingerencji.

W rozdziale V zostały przedstawione metody ujawniania i zabezpieczania śladów cyfrowych. Z uwagi na specyfikę i podatność na zniekształcenia, wymagane było uporządkowanie procedur zabezpieczania śladów cyfrowy opisywanych w literaturze fachowej, przeznaczonej dla informatyków śledczych, w taki sposób, by były one zrozumiałe także dla pracowników organów ścigania i prawników nieposiadających specjalistycznej wiedzy z zakresu informatyki. Zostały przedstawione metody zabezpieczania urządzeń i danych cyfrowych, a także opisane środki techniczne służące skutecznemu odizolowaniu urządzenia cyfrowego od niepożądanych skutków działań czynników zewnętrznych. Najczęściej do uszkodzenia śladu cyfrowego dochodzi w momencie jego zabezpieczania i późniejszej analizy. Utworzenie skutecznej procedury powinno zminimalizować ryzyko wystąpienia błędu. Poza opisem zabezpieczania urządzeń techniczny, zostały także opisane procedury związane z zabezpieczaniem połączeń telefonicznych i internetowych, w ramach których doszło do popełnienia czynu zabronionego lub połączenia takie mogą dostarczyć nowych istotnych źródeł dowodowych dla organów prowadzących postępowanie. Najprościej opisać istotę zabezpieczenia połączenia na przykładzie telefonu komórkowego, gdy poza zabezpieczeniem samego urządzenia, wyłączony zostaje także sam numer. Dzięki temu można gruntownie sprawdzić, z jakimi innymi numerami nawiązywał kontakt zabezpieczony aparat telefoniczny. Innym ciekawym zjawiskiem opisanym w tym rozdziale jest pojęcie „echa cyberprzestrzeni" i „cienia cyberprzestrzeni". Pierwsze z pojęć odnosi się do działalności, po jakiej pozostał ślad, jednak specjaliści z zakresu badań zabezpieczonego urządzenia nie są w stanie podać dokładnych danych. Oznacza to tyle, że coś na danym urządzeniu było robione, jednak nie można kategorycznie stwierdzić, co dokładnie. Drugie pojęcie, czyli „cień cyfrowy", możemy rozumieć jako całość działalności człowieka w cyberprzestrzeni. Poza istotnymi dla sprawy śladami cyfrowymi, w urządzeniu można znaleźć także pozostałości po innych dokonanych przy użyciu takiego urządzenia czynnościach, ale niepowiązanych ze sprawą. Istota poprawnego zabezpieczenia śladów cyfrowych jest podstawą do późniejszego rozpatrywania śladu w ujęciu dowodowym.

W rozdziale VI zostało przedstawione pojęcie „ekspertyzy kryminalistycznej" i istota poprawnego wykonania ekspertyzy śladów cyfrowych. Opisany został również rodzaj i zakres czynności wymaganych przy wykonywaniu ekspertyzy. Przy prowadzeniu badań nad śladem cyfrowym nie można zapominać o fundamentalnej roli biegłych z zakresu badań technik komputerowych, teleinformatycznych, telekomunikacyjnych, ekspertów do spraw analizy treści cyfrowej zawartej na różnego rodzaju nośnikach danych i ekspertów z zakresu analizy fonoskopijnej. Specyfika śladu cyfrowego pozwala na wykorzystanie także wiedzy z innych dziedzin kryminalistyki, np. daktyloskopii, badań pisma, dokumentów. Opisany został również niezwykle istotny, z punktu widzenia poprawnego wykonania ekspertyzy i przyszłego znaczenia w toczącym się postępowaniu, sposób przygotowania do wykonania takiej ekspertyzy śladów cyfrowych. Urządzenia cyfrowe nie można traktować jako jedną istniejącą rodzinę maszyn, z którą procedura postępowania będzie identyczna. Zastosowanie metod analizy w przypadku dysku komputerowego a dysku monitoringu kamer jest tak diametralnie różne, że użycie tej samej metody analizy w obu przypadkach doprowadzi do nieuchronnego utracenia i uszkodzenia przechowywanych danych na takich nośnikach. W rozdziale zostały opisane także wybrane metody badań śladów cyfrowych w odniesieniu do badań komputerów, nośników danych, strumienia danych, serwerów i samej treści informacji cyfrowej. Została również opisana problematyka dojścia od śladu cyfrowego do uzyskania dowodu.

W rozdziale VII opisane zostało wykorzystywanie śladów cyfrowych w pracy wykrywczej. Przedstawione zostały założenia ogólne pracy wykrywczej i ujęcie śladów cyfrowych w analizie kryminalnej. Nie można pominąć również faktu, że przestępstwa z użyciem urządzeń teleinformatycznych w ujęciu definiowanego pojęcia i idei przestępstwa nie różnią się od klasycznych form popełniania czynów zabronionych. W przypadkach przestępstw tzw. „komputerowych" również możemy zaobserwować swoiste *modus operandii* sprawcy i dokonać jego profilowania kryminalistycznego. Sprawcy często posługują się już sprawdzonymi metodami w celu uzyskania nielegalnego dostępu do treści chronionych. W rozdziale opisane zostało również zagadnienia alibi cyfrowego i potencjalnego znaczenia takiego rodzaju alibi dla wymiaru sprawiedliwości. Zaprezentowane zostały hipotetyczne rozważania na temat skuteczności i wiarygodności alibi cyfrowego.

W rozdziale VIII przedstawione zostały wyniki przeprowadzonych badań aktowych w celu uzyskania informacji na temat skuteczności i ilości przeprowadzonych spraw z użyciem śladów cyfrowych. Opisane zostało wykorzystywanie śladów cyfrowych w praktyce śledczej i sądowej i rodzaje przestępstw, w których badano ślady cyfrowe. Opisano także znaczenie takiego śladu cyfrowego w postępowaniu przygotowawczym i sposoby wykorzystania śladu przed sądem. W badaniach wykazano również wpływ przeprowadzonej ekspertyzy śladów cyfrowych na wydany wyrok sądowy. W ostatniej części rozdziału została omówiona ankieta

przeprowadzona wśród pracowników organów ścigania, sędziów, prokuratorów i adwokatów. Sprawdzony został stan obecnej wiedzy o możliwościach wykorzystania śladów cyfrowych przez sędziów i możliwościach przeprowadzenia efektywnej ekspertyzy śladów cyfrowych, a także możliwościach wykorzystania takich śladów przez organy ścigania w celach zapobiegawczych.

W rozdziale IX zostały opisane etyczne problemy wykorzystywania śladów cyfrowych. Możliwość uzyskania śladów cyfrowych wiąże się po części z takimi zagadnieniami, jak posłuch, inwigilacja społeczeństwa i stały monitoring cyberprzestrzeni i życia cyfrowego użytkowników Internetu. Opisana została etyka prowadzenia badań nad śladem cyfrowym w kryminalistyce i granice, w jakich możliwa jest kontrola społeczeństwa.

W tym miejscu pragnę również serdecznie podziękować za pomoc i okazaną ogromną życzliwość prof. dr hab. Denisowi Solodovowi, recenzentom wydawniczym: prof. dr hab. Bronisławowi Młodziejowskiemu i prof. dr hab. Bogusławowi Sygitowi, a także dr Jerzemu Kosińskiemu. Za pomoc i wsparcie dziękuję swoim rodzicom: Annie i Jerzemu Kasprzakom. Jestem bardzo wdzięczny Wydawnictwu za podjęcie się trudu wydania tego opracowania.