Denis Sołodow
Katedra Kryminalistyki i Medycyny Sądowej
Uniwersytetu Warmińsko-Mazurskiego w Olsztynie

O POTRZEBIE ZNAJOMOŚCI KRYMINALISTYKI CYFROWEJ PRZEZ PRZYSZŁYCH PRAWNIKÓW

Educating future lawyers in the field of digital forensics

Kryminalistyka od początku swej historii aktywnie wykorzystuje osiągnięcia innych nauk oraz techniki w celu zwiększenia efektywności ścigania karnego[1]. Jeszcze nie tak dawno o dowodach cyfrowych mówiło się przeważnie w kontekście przestępstw komputerowych[2], a w wielu podręcznikach kryminalistyki wątek nowoczesnych technologii był w ogóle pomijany. W ciągu ostatniej dekady sytuacja zmieniła się radykalnie. Technologie cyfrowe są wszechobecne i szeroko dostępne. Z danych GUS za 2017 r. wynika, że liczba gospodarstw domowych wyposażonych w komputery w Polsce wynosi 81,8% ogółu gospodarstw danej grupy. W 2017 r. z komputerów korzystało 22,0 mln osób, a 20,9 mln Polaków użytkowało komputer regularnie. 81,9% gospodarstw ma dostęp do Internetu[3]. Zgodnie z raportem analitycznym Urzędu Komunikacji Elektronicznej, z telefonów komórkowych korzysta 91,9% Polaków, a większość z nich używa smartfonów[4]. Jak wynika z raportu Związku Praco-

---

1 B. Hołyst, *Kryminalistyka*, LexisNexis, Warszawa, 2013, s. 27; tenże (red.), *Technika kryminalistyczna w pierwszej połowie XXI wieku. Wybrane problemy*, Wydawnictwo Naukowe PWN, Warszawa 2014, s. 9.

2 E. Gruza, M. Goc, J. Moszczyński, *Kryminalistyka – czyli rzecz o metodach śledczych*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008, s. 559–574.

3 Główny Urząd Statystyczny, *Społeczeństwo informacyjne w Polsce. Wyniki badań statystycznych z lat 2013–2017*, http://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-wyniki-badan-statystycznych-z-lat-2013-2017,1,11.html [dostęp: 13.03.2018]. Te dane korespondują ze wzrostem liczby wniosków organów ścigania o ujawnienie danych użytkowników portali społecznościowych, takich jak YouTube, Google+, Gmail czy Facebook (http://prawo.gazetaprawna.pl/galerie/1112478,duze-zdjecie,1,sciaganie-dowodow-w-sledztwach-od-gigantow-internetowych.html [dostęp: 13.03.2018]).

4 Urząd Komunikacji Elektronicznej, *Badanie konsumenckie 2017*, https://www.uke.gov.pl/akt/badanie-konsumenckie-2017,50.html [dostęp: 13.03.2018].

dawców Branży Internetowej IAB Polska, około 40% polskich internautów posiada sprzęty, które mogą funkcjonować w ekosystemie Internet rzeczy (IoT), a kolejne 50% wykorzystywałoby te urządzenia, gdyby miało taką możliwość[5]. W 2014 r. systemy monitoringu wizyjnego funkcjonowały we wszystkich miastach wojewódzkich oraz w ponad 85% miast powiatowych[6]. Maksymalna długość przechowywania nagrań, co jest ważne z punktu widzenia kryminalistyki, wynosiła nawet 90 dni[7]. Z roku na rok rośnie popularność monitoringu prywatnego będącego stosunkowo prostym, a jednocześnie efektywnym środkiem prewencyjnym[8]. Zwiększa się liczba samochodów prywatnych wyposażonych w wideorejestratory. Bardzo często są to urządzenia połączone z odbiornikiem GPS, które mogą wykonywać precyzyjne pomiary prędkości oraz zapisywać bieżącą lokalizację pojazdu. Dostępne na rynku modele zapewniają kąt „widzenia" od 120 stopni i rejestrują obraz w bardzo dobrej jakości nawet przy niedostatecznym oświetleniu. Większość takich kamer ma wbudowane akumulatory, co umożliwia funkcjonowanie w trybie autonomicznym. Zaawansowane wideorejestratory nagrywają również obraz za pojazdem oraz reagują na ruch (np. na parkingu). Niektóre urządzenia oprócz standardowej opcji rozszerzenia pamięci wewnętrznej potrafią zsynchronizować nagranie z „chmurą" czy smartfonem, co pozwala przechowywać znaczne ilości informacji przez praktycznie nieograniczony czas. Wszystko to sprawia, że ślady cyfrowe odgrywają co raz większą rolę[9], stanowiąc na równi z innymi, tradycyjnymi dowodami podstawę wyrokowania również w sprawach o przestępstwa pospolite. Zabezpieczenie nagrań z monitoringu, analiza połączeń z telefonów komórkowych, badanie aktywności w Internecie, treści umieszczonych na portalach społecznościowych – to rutynowe czynności organów ścigania, które bardzo często dostarczają cenne z punktu widzenia wykrycia przestępstwa informacje.

Ewolucji technologii cyfrowych towarzyszy stały przyrost danych pochodzących z niemal wszystkich obszarów życia codziennego, co zdaniem bada-

---

5 Związek Pracodawców Branży Internetowej IAB Polska, Raport *Internet Rzeczy w Polsce*, s. 12, https://iab.org.pl/wp-content/uploads/2015/09/Raport-Internet-Rzeczy-w-Polsce.pdf [dostęp: 13.03.2018].

6 Najwyższa Izba Kontroli, *Funkcjonowanie miejskiego monitoringu wizyjnego*, 2014, https://www.nik.gov.pl/aktualnosci/nik-o-miejskim-monitoringu-wizyjnym.html [dostęp: 13.03.2018].

7 Fundacja Panoptykon, *Monitoring w polskich miastach i w oczach społeczeństwa*, https://panoptykon.org/sites/default/files/publikacje/panoptykon_cctv_seminarium_10-10-2012_2.pdf [dostęp: 13.03.2018].

8 Por. P. Waszkiewicz, *Wielki Brat – rok 2010. Systemy monitoringu wizyjnego – aspekty kryminalistyczne, kryminologiczne i prawne*, Wolters Kluwer Polska, Warszawa 2011, s. 56.

9 Por. W.A. Kasprzak, *Ślady cyfrowe. Studium prawno-kryminalistyczne*, Difin, Warszawa 2015, s. 228.

czy świadczy o nastąpieniu tzw. złotej ery dowodów[10]. Większa część tych danych jednak nigdy nie „wychodzi" poza świat cyfrowy[11]. Z perspektywy kryminalistyki istotne znaczenie ma fakt, że średnio statystyczny użytkownik posiada dość ograniczoną wiedzę w tym zakresie. Procesy, które odbywają się wewnątrz komputera, smartfonu czy tabletu, dla wielu stanowią tajemnicę. Częściowo „winę" za to ponoszą producenci sprzętu cyfrowego, którzy od lat konsekwentnie dążą do stworzenia maksymalnie przyjaznego interfejsu użytkownika. Powoduje to, że skomplikowane procesy wewnętrzne są maksymalnie zautomatyzowane. Nowoczesne urządzenie cyfrowe potrafi nie tylko samodzielnie przeprowadzić diagnostykę w poszukiwaniu ewentualnych błędów, a nawet je naprawić, nie angażując w ten proces użytkownika. Ważne jest to, że współczesne systemy operacyjne i tzw. programy użytkowe przedstawiają sobą wyjątkowo skomplikowany produkt będący wynikiem wieloletniej pracy setek i tysięcy specjalistów. Pełne zrozumienie mechanizmów ich działania wymaga ponadprzeciętnych zdolności technicznych i głębokiej wiedzy informatycznej. Kolejną przeszkodą jest to, że ogólnie dostępna wiedza informatyczna ma charakter ograniczony. Stosowane w systemach operacyjnych i programach technologie bardzo często stanowią know-how producenta, który ze zrozumiałych powodów nie jest szczególnie zainteresowany dzieleniem się tymi informacjami[12].

Niestety ta uwaga dotyczy również przyszłych prawników, którzy w trakcie studiów nie otrzymują pełnych i aktualnych informacji o technologiach cyfrowych oraz możliwościach praktycznego wykorzystania śladów cyfrowych w sprawach karnych i cywilnych[13]. Programy kształcenia prawników nie uwzględniają w wystarczającym stopniu wątku cyfrowego. Na niektórych uczelniach informatyka śledcza jako kierunek pod różnymi nazwami istnieje na poziomie studiów podyplomowych, których audytorium docelowe stanowią informatycy. Studenci prawa uczą się obsługi podstawowych programów do pracy z tekstem, korzystania z prawniczych baz danych, a jednocześnie otrzymują przeważnie fragmentaryczne informacje o współczesnych systemach operacyj-

[10] C. Ball, *What Every Lawyer Should Know About E-Discovery*, http://www.craigball.com/What%20Every%20Lawyer%20Should%20Know%20About%20E-Discovery_FINAL.pdf [dostęp: 13.03.2018].

[11] 93% generowanych informacji cyfrowych istnieje wyłącznie w formie elektronicznej (Digital Evidence & Computer Forensics, David Nardoni CISSP, EnCE, http://wwwscf.usc.edu/~uscsec/images/DigitalEvidence&ComputerForensicsversion1.2USC.pdf [dostęp: 13.03.2018].

[12] Por. A. Loll, *Understanding digital enhancement processes*, „Journal of Forensic Identification" 2016, nr 66 (1), s. 3–4.

[13] Por. M. Szmit (red.), *Elementy informatyki sądowej*, Polskie Towarzystwo Informatyczne, Zarząd Główny, Warszawa 2011, s. 9; G. Oparnica, *Digital evidence and digital forensic education*, „Digital Evidence and Electronic Signature Law Review" 2016, nr 13, s. 143.

nych, możliwościach ekspertyz z zakresu badań śladów cyfrowych, technikach zabezpieczania śladów cyfrowych. Brakującą wiedzę prawnik „uzupełnia" w praktyce, ucząc się od starszych, bardziej doświadczonych kolegów, ale niestety mało pomocnych, jeśli chodzi o przedmiotowy obszar. Możliwości „samokształcenia" w tym zakresie ograniczają brak usystematyzowanej wiedzy podstawowej oraz ogólnie słaba znajomość „technicznego" języka angielskiego. W razie konieczności ograniczony w środkach prawnik sięga po pomoc przysłowiowego „wujka Google'a", ale rezultat końcowy nie zawsze jest zadowalający. Algorytmy wyszukiwania są stale doskonalone, jednak to, co wśród pokazywanych wyników zajmuje pierwsze miejsca (pierwszą stronę), nie zawsze odpowiada rzeczywistym potrzebom użytkownika. Rezultaty podawane przez wyszukiwarki internetowe mogą zawierać zarówno wiarygodne, aktualne, jak i nieprawdziwe lub przestarzałe informacje (z aktualną datą). Niespecjalista może mieć trudności z odróżnieniem jednych od drugich, co w konsekwencji może prowadzić do podjęcia błędnych decyzji, których skutków w dalszym ciągu nie będzie łatwo zneutralizować. Istotne znaczenie ma i to, że świat technologii cyfrowych stale się zmienia. To, co jeszcze wczoraj wydawało się rozwiązaniem całkowicie słusznym, jutro może okazać się nieaktualne. Nowe technologie mogą wymagać gruntownej rewizji dotychczasowych zasad postępowania. Charakterystycznym przykładem są dyski SSD, które do przechowywania informacji wykorzystują pamięć *flash* typu NAND. W przypadku klasycznych dysków wyposażonych w obracające się talerze magnetyczne nie zaleca się nagłego odłączenia zasilania, ponieważ ruchoma głowica odczytująco-zapisująca może nieodwracalnie uszkodzić powierzchnię talerza magnetycznego, co uniemożliwi późniejszy odczyt zapisanych w tym miejscu danych. Dyski SSD są natomiast wyposażone w zaawansowane kontrolery zarządzające przechowywaniem danych. Procesy wewnątrz takiego dysku odbywają się bez wiedzy i udziału użytkownika, a nawet niezależnie od działania systemu operacyjnego. Pozostawienie takiego dysku podpiętego do zasilania zmniejsza szansę na odzyskanie usuniętych danych (odtworzenie stanu pierwotnego zmodyfikowanych)[14]. W odróżnieniu od laptopów czy komputerów stacjonarnych, w odniesieniu do których wciąż istnieją skuteczne metody pozwalające na odtworzenie usuniętych (zmodyfikowanych) danych, w przypadku urządzeń mobilnych (smartfonów, tabletów) taka możliwość za sprawą no-

[14] Metodologie *garbage collection* firmy Kingston jako sposób na zwiększenie wydajności dysków SSD w przypadku obciążeń klienckich, https://www.kingston.com/pl/ssd/enterprise/technical_brief/garbage_collection [dostęp: 13.03.2018]; Y. Gubanov, O. Afonin, *SSD Forensics 2014. Recovering Evidence from SSD Drives: Understanding TRIM, Garbage Collection and Exclusions*, https://belkasoft.com/download/info/SSD%20Forensics%202014.pdf [dostęp: 13.03.2018].

wych algorytmów szyfrujących oraz innej polityce dostępu obecnie została praktycznie wyeliminowana[15]. Próba zastosowania dotychczasowych metod badawczych do nowych urządzeń cyfrowych bez rozumienia charakteru i zakresu wprowadzonych zmian może prowadzić do nieodwracalnej utraty relewantnych śladów cyfrowych.

Pytania, czy prawnik musi posiadać kompetencje techniczne, a jeśli tak, to w jakim zakresie, należą do dyskusyjnych. W literaturze polskiej można spotkać pogląd, że „zaawansowana wiedzą z zakresu informatyki (…) tak naprawdę prokuratorowi nie jest potrzebna"[16]. Jednocześnie nie można nie zauważyć wzrostu liczby opracowań w tym zakresie tworzonych z myślą o prawnikach i ich potrzebach. Jeśli zwrócimy się do doświadczeń innych krajów, to warto podkreślić, że np. w Stanach Zjednoczonych posiadanie przez prawnika kompetencji technicznych w świetle obowiązujących reguł etycznych jest rzeczą obowiązkową[17]. Z kolei w Wielkiej Brytanii dla funkcjonariuszy policji pracujących na „pierwszej linii" organizowane są specjalne szkolenia w zakresie nowych technologii cyfrowych[18]. Przyjmuje się, że brak elementarnego rozeznania w dziedzinie nowoczesnych technologii informatycznych ogranicza możliwości organów ścigania, jeśli chodzi o skuteczne zapobieganie przestępstwom oraz ich wykrywanie. Prawdopodobieństwo, że na miejscu zdarzenia znajdą się nośniki danych cyfrowych, ocenia się jako wystarczająco wysokie. Ślady, które mogą mieć doniosłe znaczenie wykrywcze i dowodowe, jeśli nie zostaną „rozpoznane" przez osobę dokonującą oględzin czy przeszukania, w najlepszym wypadku pozostaną „rzeczą samą w sobie", a w najgorszym – okażą się niedostępne (nadpisane, zmodyfikowane, usunięte). W jednej ze spraw, w której jako adwokat, a potem obrońca uczestniczył autor, podczas

---

15 C. Ball, *Opportunities and Obstacles: E-Discovery from Mobile Devices*, http://www.craigball.com/ [dostęp: 13.03.2018].

16 J. Kudła, A. Staszak, *Procesowa i operacyjna kontrola korespondencji przechowywanej w tzw. chmurze*, „Prokuratura i Prawo" 2017, nr 7–8, s. 33.

17 A. Perlman, *The twenty-first century lawyer's evolving ethical duty of competence*, „The Professional Lawyer" 2014, t. 22 (4); A.E. Davis, *The ethical obligation to be technologically competent*, „The New York Law Journal", 8 stycznia 2016 r. W 2012 r. odpowiednie zmiany zostały wprowadzone do kodeksu etyki zawodowej prawników amerykańskich – American Bar Association Model Rules of Professional Conduct: „[A] lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation", "[t]o maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology…" (reguła 1.1).

18 IACP TECHNOLOGY POLICY FRAMEWORK, January 2014, http://www.theiacp.org/Portals/0/documents/pdfs/IACP%20Technology%20Policy%20Framework%20January%202014%20Final.pdf [dostęp: 13.03.2018]; A. Hitchcock, R. Holmes, E. Sundorph, *Bobbies on the Net: A Police Workforce for the Digital Age*, http://www.reform.uk/wp-content/uploads/2017/08/Bobbies-on-the-net.pdf dostęp: 13.03.2018].

przeszukania mieszkania w sprawie o pobicie z pobudek ekstremistycznych funkcjonariusze Federalnej Służby Bezpieczeństwa Rosji zabezpieczyli komputer stacjonarny oraz płyty CD i DVD należące do podejrzanego (był nim kierownik lokalnego „oddziału" organizacji neonazistowskiej). Nikt z dokonujących przeszukania nie zwrócił uwagi na leżący na półce tuż obok komputera pendrive. Miał on postać kawałka drewna z przewierconą na końcu dziurką, przez którą przeciągnięto sznurek do zawieszenia na szyi. Zawierał niezaszyfrowane dane o członkach organizacji, zdjęcia i „sprawozdania" z przeprowadzonych akcji, o czym później autorowi powiedział klient. Funkcjonariusz w randze majora wziął co prawda przedmiot do ręki, uważnie go obejrzał, ale po chwili odłożył z powrotem. Można się domyślić, że ta sprawa zakończyła się dla klienta pomyślnie. Oskarżeniu nie udało się udowodnić motywu ekstremistycznego, zmieniono kwalifikację czynu, co otworzyło drogę do umorzenia postępowania za zgodą obu stron.

Jeśli chodzi o niedostateczne kompetencje techniczne prawników, o skali problemu wystarczy się przekonać, zadając studentowi kilka prostych pytań: co można, a czego nie można robić z konkretnym nośnikiem informacji znalezionym na miejscu zdarzenia (na przykład wideorejestratorem zainstalowanym w jednym z aut uczestniczących w wypadku drogowym, smartfonem czy tabletem znalezionym przy zwłokach), w jaki sposób należy taki przedmiot zabezpieczyć, dlaczego zaleca się ten, a nie inny sposób postępowania z daną kategorią urządzeń cyfrowych. Szczególnie znaczenie będzie miała odpowiedź na ostatnie z pytań, ponieważ ten, kto rozumie, dlaczego należy postępować tak, a nie inaczej, raczej nie popełni błędu. Brak świadomości potrzeby działania w określony sposób, stosowania określonej metody czy przestrzegania zalecanej kolejności działań z reguły wynika z braku wystarczającej wiedzy o przedmiocie oraz jego istotnych z punktu widzenia kryminalistyki właściwościach. Rozumienie – chociażby na poziomie podstawowym – natury obiektu jest również warunkiem jego właściwej oceny dowodowej[19]. Podobnie jak prowadzący przesłuchanie świadka musi koniecznie posiadać wiedzę o procesach warunkujących formowanie się zeznań, rozumienie zasad i mechanizmu funkcjonowania sprzętu cyfrowego jest elementem niezbędnym, jeśli chodzi o prawidłową interpretację zebranego materiału dowodowego. Prawnik, który otrzymuje opinię biegłego z zakresu badań śladów cyfrowych, ale nie orientuje się w dzie-

[19] Por. G.C. Kessler, *Judges' Awareness, Understanding, and Application of Digital Evidence*, A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy, Fort Lauderdale, USA, 2010, s. 2, www.garykessler.net/library/kessler_judges &de.pdf [dostęp: 13.03.2018]; L. Daniel, L. Daniel, *Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom*, Syngress–Elsevier, Waltham, MA 2012, s. 55–56.

dzinie, którą biegły reprezentuje, nie jest w stanie dokonać prawidłowej oceny merytorycznej i dowodowej uzyskanych wyników. Co więcej, wiedza informatyczna jest konieczna również przy określaniu zakresu pytań kierowanych do biegłego. W jednej ze spraw, która dotyczyła przestępstwa skarbowego, śledczy podczas przeszukania w siedzibie firmy absolutnie prawidłowo, można powiedzieć książkowo, zabezpieczył komputer księgowej. Był tylko jeden problem, o którym śledczy nie wiedział. Pracownicy ochrony wewnętrznej zabarykadowali drzwi wejściowe, przez co opóźnili całą akcję śledczych, a w tym czasie księgowej udało się usunąć dokument ukazujący realną księgowość firmy. Ta operacja została przeprowadzona w ten sposób, że księgowa usunęła inkryminowany plik do kosza, a następnie z poziomu menu podręcznego wyczyściła jego (kosza) zawartość. Śledczy zlecił badania komputerowo-techniczne zabezpieczonego sprzętu. Sprawie nadano priorytet, opinia biegłych była więc gotowa już po kilku dniach. Biorąc pod uwagę sposób usunięcia pliku, można było przewidzieć, że śledztwo będzie miało niepodważalny dowód popełnienia przestępstwa skarbowego, o czym adwokat od razu poinformował klientów. Później jednak, studiując postanowienie śledczego o powołaniu biegłych, adwokat (księgowa oraz prezes firmy byli wezwani w charakterze świadków, co w świetle obowiązującego prawa procesowego Rosji uprawniało do korzystania z pomocy adwokata) ze zdziwieniem stwierdził, że biegłym nie postawiono pytania dotyczącego obecności na zabezpieczonym nośniku usuniętych plików oraz ich zawartości. W swojej opinii, jak to czasem się zdarza, biegli udzielili odpowiedzi tylko na te pytania, które zostały zawarte w postanowieniu. Po zapoznaniu się z wynikami ekspertyzy adwokat natychmiast złożył wniosek o przekazanie przebadanego komputera z powrotem jego właścicielom, motywując to tym, że firma musi dalej funkcjonować, a wszelkie badania specjalistyczne zatrzymanego sprzętu, które uznano za konieczne, zostały już przeprowadzone. Wniosek (co prawda po kilku godzinach, w ciągu których, jak nietrudno się domyślić, śledczy konsultował decyzję z przełożonym i kolegami) został w pełni uwzględniony. Dalszy los komputera, a w szczególności dysku twardego, nietrudno było przewidzieć. Podobne przypadki świadczą o niedostatecznej wiedzy śledczych w zakresie współczesnych technologii cyfrowych.

Kwestią istotną jest również wybór właściwego biegłego. Wyszukiwarka internetowa na hasło „biegły w zakresie informatyki" pokazuje obecnie ponad setkę wyników. Niestety zdarza się, że osoba podająca się za specjalistę/biegłego tak naprawdę nie jest w stanie przeprowadzić zleconych badań z powodu braku wiedzy czy też niezbędnego sprzętu i oprogramowania. W tej sytuacji badania są podzlecane firmom informatycznym, a co za tym idzie,

osoby, które faktycznie je wykonują, nie ponoszą odpowiedzialności za wynik końcowy. Badania są przeprowadzane w sposób niekontrolowany, nieprzejrzysty, bez przestrzegania zasad informatyki śledczej, co zwiększa ryzyko nieodwracalnej utraty lub modyfikacji materiału dowodowego. Podobnych sytuacji można uniknąć, jeśli prawnik zlecający przeprowadzenie ekspertyzy będzie miał chociażby podstawową wiedzę o mechanizmie powstawania danego rodzaju śladów cyfrowych oraz istniejących metodach ich ujawnienia i odzyskania.

Za koniecznością poszerzenia wiedzy informatycznej prawników oraz funkcjonariuszy organów ścigania przemawia i ten fakt, że w dziedzinie technologii cyfrowych granica między wiedzą powszechną a specjalistyczną zauważalnie się przesunęła. Dzisiaj uczeń szkoły podstawowej potrafi sprawnie wykonać operacje informatyczne, które jeszcze nie tak dawno były poza zasięgiem średnio statystycznego użytkownika (stworzyć kopię binarną pliku, obliczyć i porównać sumy kontrolne, wyostrzyć zdjęcie, odczytać i przeanalizować metadane pliku, nagłówek [*header*] wiadomości emailowej itd.). Jednak w postanowieniach o powołaniu biegłych z zakresu informatyki śledczej wciąż można zobaczyć zlecenie im stosunkowo prostych operacji, które śledczy może wykonać sam, na przykład w ramach oględzin.

Pozostaje pytanie drugie dotyczące zakresu kompetencji technicznych, które powinien posiadać przyszły prawnik. Warto zacząć przede wszystkim od uświadomienia istoty śladu cyfrowego i jego specyfiki. Niestety w wielu podręcznikach z kryminalistyki dla prawników te pojęcia, kluczowe dla właściwego rozumienia przedmiotowej kwestii, są pomijane. Najczęściej znajdziemy w nich informacje o sposobach popełniania przestępstw komputerowych oraz zasadach zabezpieczania komputerów stacjonarnych, które nie zawsze uwzględniają aktualny stan techniki cyfrowej. Prawnikowi, który na co dzień będzie miał do czynienia z cyfrowym materiałem dowodowym, ta wiedza nie wystarczy. W błąd może wprowadzać błędne utożsamianie śladów cyfrowych z tradycyjnymi śladami materialnymi, z którymi łączy je wspólna, materialna forma istnienia oraz jednoznaczny, obiektywny związek przyczynowo-skutkowy z inicjującym powstanie śladu procesem fizycznym (działaniem użytkownika czy zapisanego w pamięci maszyny algorytmu). Jednak na tym podobieństwo się kończy. Ujawnienie i zabezpieczanie śladów cyfrowych wymaga zastosowania innych metod i środków. Ślady cyfrowe w porównaniu ze śladami materialnymi mają szerszy zakres, tj. dotyczą różnych stron życia człowieka, mogą zawierać wrażliwe informacje o charakterze osobistym, wymagają odbycia przez podmiot wykonujący badania odmiennych szkoleń oraz

posiadania odmiennych narzędzi[20]. Ślady cyfrowe, a czasem i same ich nośniki, nie zawsze można zobaczyć w ramach tradycyjnych oględzin (dane przechowywane w „chmurze", na zdalnym serwerze). Ślad cyfrowy może jednocześnie powstawać (znajdować się) w kilku miejscach w pamięci maszyny. Przy kopiowaniu danych cyfrowych powstaje dokładne, binarne odzwierciedlenie oryginału, co raczej jest nieosiągalne w przypadku klasycznych śladów materialnych. Nagranie cyfrowe lub zdjęcie ukazujące to samo zdarzenie mogą być przedstawione w różnych formatach, które z perspektywy informatyki śledczej zasadniczo się różnią. Do cech istotnych śladów cyfrowych należą również obecność tzw. metadanych (danych o charakterze technicznym, które mogą być wykorzystane w celach kryminalistycznych, dowodowych), automatyczne dublowanie danych tworzących ślad cyfrowy przez system operacyjny, niewystępowanie zjawiska starzenia się czy degradacji śladu w ich klasycznej postaci.

Przez ślad cyfrowy w kryminalistyce cyfrowej rozumie się każdą zmianę w kodzie binarnym systemu teleinformatycznego czy urządzenia cyfrowego zdolnego do przetwarzania, wysyłania, gromadzenia pakietów danych, będącą wynikiem procesów zewnętrznych (na przykład wprowadzenie określonych poleceń przez użytkownika) bądź wewnętrznych (samodzielne, niezależne od użytkownika działanie systemu operacyjnego czy programu)[21].

W porównaniu z tradycyjnymi śladami kryminalistycznymi ślady cyfrowe są nadzwyczaj różnorodne. W literaturze za ślad cyfrowy uznaje się książki adresowe i listy kontaktowe, pliki audio, kopie zapasowe tworzone przez programy użytkowe oraz urządzenia mobilne, zakładki (*bookmarks*, *favorites*), historię przeglądarki internetowej, kalendarze cyfrowe, zarchiwizowane dokumenty elektroniczne łącznie z archiwami zaszyfrowanymi, pliki konfiguracji, „ciasteczka" internetowe (*cookies*), bazy danych, dokumenty, pocztę elektroniczną, załączniki do e-listów, wydarzenia programowe (*events*), pliki ukryte oraz systemowe, logi (*log files*), pliki pamięci wirtualnej maszyny (*page files*), pliki powstające podczas przejścia maszyny w stan uśpienia (*hibernation files*), pliki powstające podczas drukowania, obrazki, fotografie cyfrowe, maszyny wirtualne, pliki tymczasowe i inne[22]. Co więcej, ten sam plik cyfrowy, którego zawartość może mieć znaczenie dowodowe, w zależności od rodzaju nośnika

[20] S.E. Goodison, R.C. Davis, B.A. Jacksons, *Digital Evidence and the U.S. Criminal Justice System, Report on behalf of the U.S. Department of Justice, National Institute of Justice (NIJ), the RAND Corporations*, s. 3, https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf [dostęp:13.03.2018].

[21] J. Kasprzak, B. Młodziejowski, W. Kasprzak, *Kryminalistyka. Zarys systemu*, Difin, Warszawa 2015, s. 157; W.A. Kasprzak, op. cit., s. 31.

[22] Y. Gubanov, *Retrieving Digital Evidence: Methods, Techniques and Issues*, Belcasoft, https://belkasoft.com/download/info/Retrieving%20Digital%20Evidence%20-%20Methods,%20Techniques%20and%20Issues.pdf [dostęp: 13.03.2018].

wymaga od badaczy zastosowania odmiennych metod postępowania. Informacje o działaniach, poleceniach użytkownika w zależności od rodzaju zainstalowanego systemu operacyjnego oraz jego konfiguracji mogą znajdować się w różnych miejscach w systemie plików. Nagranie cyfrowe tego samego zdarzenia może występować w różnych formatach, które „decydują" o jego wartości kryminalistycznej i dowodowej. Niemniej jednak mimo różnorodności można wskazać następujące elementy wspólne, które nadają śladom cyfrowym pewną specyfikę:

1) cyfrowe odzwierciedlenie, tworzące podstawę śladu, pozostaje w sztucznym środowisku – systemie komputerowym;
2) w odróżnieniu od procesu powstawania klasycznych śladów materialnych (odzwierciedlenie cech zewnętrznych przedmiotu tworzącego ślad na podłożu) podczas „tworzenia" śladów cyfrowych odzwierciedlają się nie cechy obserwowanego zjawiska lub procesu fizycznego, lecz tylko parametry formalnego, matematycznego modelu, za pomocą którego przedmiotowe zjawisko zostaje zarejestrowane przez urządzenie techniczne;
3) dyskretny sposób rejestracji przedmiotowego zjawiska umożliwia wcześniejszą ocenę możliwości urządzenia rejestrującego (np. znając właściwości techniczne dyktafonu, można wcześniej poddać ocenie wartość dowodową informacji, która będzie za jego pomocą zarejestrowana);
4) ślad cyfrowy nie ma całościowej struktury fizycznej, jest on bowiem sumą wielu elementów, zapisanych na różnych częściach dysku twardego w komputerze;
5) ślad cyfrowy, oprócz informacji sensownej, zawiera znaczną liczbę danych wspomagających, które są niezbędne dla działania systemu komputerowego;
6) ślady cyfrowe są wyjątkowo trwałe z uwagi na to, że w trybie automatycznym powstają kopie zapasowe nowych danych, które są przechowywane w różnych lokalizacjach w pamięci maszyny, a czasem również poza nią, co umożliwia odzyskanie usuniętych danych;
7) znaczenie kryminalistyczne mogą mieć nie tylko zawartość pliku, ale również jego atrybuty – nazwa, rozmiar, data utworzenia;
8) ślady cyfrowe zawierają markery czasowe, co pozwala na dokładne odtworzenie kolejności wydarzeń oraz korelacji między nimi[23].

[23] T. Knutson, *Filesystem Timestamps: What Makes Them Tick?*, https://www.sans.org/reading-room/whitepapers/forensics/filesystem-timestamps-tick-36842 [dostęp: 13.03.2018].

Jeśli chodzi o dowodowe wykorzystywanie śladów cyfrowych, prawnik musi mieć świadomość pewnych ograniczeń. Po pierwsze, nie zawsze da się ustalić bezpośredni związek między konkretną osobą, jej działaniem a śladem cyfrowym rzekomo przez taką osobę pozostawionym. Ślad cyfrowy, z natury swojej będąc tylko formalnym odzwierciedleniem procesów fizycznych w rzeczywistości wirtualnej, nie zawiera w sobie danych, na podstawie których można było by w sposób kategoryczny zidentyfikować jego „twórcę" czy ustalić jego lokalizację fizyczną. W 2016 r. amerykańska Electronic Frontier Foundation opublikowała raport dotyczący niewłaściwej interpretacji adresów IP przez organy ścigania oraz sądy w Stanach Zjednoczonych i innych wybranych krajach. Specjaliści fundacji doszli do wniosku, że w każdym przypadku należy przeprowadzać dodatkową weryfikację lokalizacji fizycznej adresu IP, gdyż ten sam adres IP może być jednocześnie „przypisany" do kilku urządzeń znajdujących się fizycznie w różnych miejscach lub może być „udostępniony" nieograniczonej liczbie osób poprzez publiczną sieć WLAN [24]. Po drugie, ślad cyfrowy bardzo łatwo ulega destrukcji na skutek niewłaściwego postępowania z nośnikiem danych. Niewłaściwe może być też zaniechanie działania w sytuacjach, kiedy jest to konieczne. Po trzecie, metadane jako element składowy pliku same w sobie nie mogą służyć za wiarygodne źródło informacji, jeśli chcemy ustalić miejsce i czas, w którym powstał taki ślad, fakt jego modyfikacji oraz urządzenie – źródło śladu. Metadane (pliku) mogą być stosunkowo łatwo zmodyfikowane lub usunięte w sposób nieodwracalny. Równocześnie brak śladu w sytuacji, kiedy taki ślad musi istnieć, sam w sobie może posłużyć za wskazówkę. To, że przedmiotowy plik nie zawiera standardowych metadanych, może świadczyć o celowej ingerencji człowieka próbującego ukryć określone informacje (aczkolwiek w niektórych przypadkach jest to skutek działania skonfigurowanego w odpowiedni sposób programu). Po czwarte, technologii, dzięki którym powstają ślady cyfrowe, nie tworzy się z myślą o potrzebach kryminalistyków. W rezultacie biegli nie zawsze są w stanie odpowiedzieć na pytania prawnika, a czasem wariantów prawidłowych odpowiedzi może być kilka. W pewnej sprawie, w której m.in. był badany wątek posiadania przez oskarżonego plików wideo o charakterze pornograficznym z udziałem osób nieletnich, biegły zwrócił uwagę sądowi na to, że przy przeglądaniu stron internetowych na dysku twardym w folderach tymczasowych umieszczane są pliki związane z oglądanymi stronami. Ścieżka lokalizacji pliku jest ściśle określona w ustawieniach przeglądarki i systemu operacyjnego. Dysponując danymi o tym, gdzie przechowuje się pliki tymczasowe, można sprawdzić, czy zostały one za-

[24] *Unreliable Informants: IP Addresses, Digital Tips and Police Raids*, https://www.eff.org/pl/node/93067 [dostęp: 13.03.2018].

pisane w trybie automatycznym, czy użytkownik zrobił to celowo. Wyjątek dotyczy sytuacji, gdy plik został odzyskany z danych. Wówczas określenie katalogu, w którym uprzednio się on znajdował, nie jest możliwe, a czasem nie ma również możliwości podania daty powstania pliku[25].

Ryzyko popełnienia błędów przy ujawnieniu, zabezpieczeniu i interpretacji śladów cyfrowych jest zdecydowanie mniejsze, jeśli osoba wykonująca te czynności ma adekwatną i aktualną wiedzę informatyczno-techniczną. Pod tym względem w chwili obecnej za konieczne można uznać kształcenie w następujących zakresach:

- podstawy formowania się śladów cyfrowych najczęściej występujących w sprawach karnych i cywilnych;
- podstawy funkcjonowania powszechnie stosowanych systemów operacyjnych – Windows, Linux – oraz ich modyfikacji mobilnych z perspektywy informatyki śledczej;
- system plików w środowisku Windows i Linux;
- metadane i ich analiza kryminalistyczna;
- podstawy funkcjonowania Internetu;
- zasady i metody dowodowego wykorzystania mediów społecznościowych;
- podstawy technologii przetwarzania danych w „chmurze";
- podstawy funkcjonowania popularnych przeglądarek internetowych, poczty elektronicznej, komunikatorów internetowych;
- technologie bezpieczeństwa w komunikacji cyfrowej (szyfrowanie, tunelowanie danych, Tor);
- podstawy funkcjonowania telefonii komórkowej.

Proces kształcenia musi przewidywać wystarczającą liczbę godzin na zajęcia praktyczne, w ramach których przyszli prawnicy będą mogli zastosować nabytą wiedzę, rozwiązując typowe kazusy czy prowadząc wielowątkowe „śledztwo cyfrowe".

Podsumowując, należy uznać, że ślady i dowody cyfrowe odgrywają szczególną rolę we współczesnym procesie karnym. Ze względu na swoją specyfikę charakteryzują się wyjątkową trwałością, mają obiektywny charakter, są wszechobecne, a sprawcy przestępstw często nie wiedzą o ich istnieniu. To sprawia, że w każdej sprawie karnej istnieje duża szansa na odnalezienie czy odzyskanie relewantnych śladów cyfrowych. Czy ten cel zostanie w pełni osiągnięty – zależy od wiedzy i umiejętności osób prowadzących postępowanie. Nie mniej istotna jest kwestia właściwej interpretacji zabezpieczonego cyfro-

[25] Wyrok Sądu Apelacyjnego we Wrocławiu, II Wydział Karny, z dnia 27.09.2012, Sygn. akt II AKa 171/12.

wego materiału dowodowego. Przyszli prawnicy muszą zatem dysponować adekwatną i aktualną wiedzą o najczęściej występujących śladach cyfrowych, mechanizmach ich powstania oraz właściwych technikach zabezpieczania.

Streszczenie

Wszechobecność i szeroka dostępność technologii informatycznych sprawiają, że ślady i dowody cyfrowe odgrywają coraz większą rolę w postępowaniu karnym. Ze względu na to, że są one obiektywne, precyzyjne, wyjątkowo trwałe i różnorodne, stanowią istotny element pracy wykrywczej nie tylko w śledztwach o przestępstwa komputerowe. W odróżnieniu od tradycyjnych śladów kryminalistycznych sprawca nie zawsze jest świadom samego faktu istnienia śladu cyfrowego, a próby usunięcia bądź celowej modyfikacji takiego śladu przy braku odpowiednich umiejętności i wiedzy z reguły kończą się względnym niepowodzeniem, co zwiększa szansę na ich znalezienie i odzyskanie. Wiedza o śladach cyfrowych, ich właściwościach i mechanizmach powstania jest zatem niezbędnym elementem w arsenale współczesnego prawnika.

Słowa kluczowe: proces karny, kryminalistyka cyfrowa, ślad cyfrowy, dowód cyfrowy, ekspertyza, opinia biegłego

Abstract

Digital traces play an important role in the crime detection and the process of proof. In contrast to traditional types of forensic traces, in the case of digital traces, the perpetrator is not always aware of the fact of leaving them, and attempts to remove or deliberately modify such traces in the absence of adequate knowledge and relevant skills often end in relative failure. This causes that in almost every case there is a good chance to find (retrieve) relevant digital evidence. The article raises issues related to the training of future lawyers in the field of modern digital technologies, the possibility of evidence-based use of digital traces, their proper protection and interpretation.

Keywords: criminal process, digital forensics, digital traces, evidence, expertise, expert opinion

Bibliografia

Literatura

Daniel L., Daniel L., *Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom*, Syngress–Elsevier, Waltham, MA 2012.

Davis A.E., *The ethical obligation to be technologically competent*, „The New York Law Journal", 8 stycznia 2016 r.

Gruza E., Goc M., Moszczyński J., *Kryminalistyka – czyli rzecz o metodach śledczych*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008.

Hołyst B. (red.), *Technika kryminalistyczna w pierwszej połowie XXI wieku. Wybrane problemy*, Wydawnictwo Naukowe PWN, Warszawa 2014.

Hołyst B., *Kryminalistyka*, LexisNexis, Warszawa 2013.

Kasprzak J., Młodziejowski B., Kasprzak W., *Kryminalistyka. Zarys systemu*, Difin, Warszawa 2015.

Kasprzak W.A., *Ślady cyfrowe. Studium prawno-kryminalistyczne*, Difin, Warszawa 2015.

Kudła J., Staszak A., *Procesowa i operacyjna kontrola korespondencji przechowywanej w tzw. chmurze*, „Prokuratura i Prawo" 2017, nr 7–8.

Loll A., *Understanding digital enhancement processes*, „Journal of Forensic Identification" 2016, nr 66 (1).

Oparnica G., *Digital evidence and digital forensic education*, „Digital Evidence and Electronic Signature Law Review" 2016, nr 13.

Perlman A., *The twenty-first century lawyer's evolving ethical duty of competence*, „The Professional Lawyer" 2014, t. 22 (4).

Szmit M. (red.), *Elementy informatyki sądowej*, Polskie Towarzystwo Informatyczne, Zarząd Główny, Warszawa 2011.

Waszkiewicz P., *Wielki Brat – rok 2010. Systemy monitoringu wizyjnego – aspekty kryminalistyczne, kryminologiczne i prawne*, Wolters Kluwer Polska, Warszawa 2011.

Źródła

Wyrok Sądu Apelacyjnego we Wrocławiu, II Wydział Karny z dnia 27.09.2012, Sygn. akt II AKa 171/12.

Internet

Ball C., *Opportunities and Obstacles: E-Discovery from Mobile Devices*, http://www.craigball.com/ [dostęp: 13.03.2018].

Ball C., *What Every Lawyer Should Know About E-Discovery*, http://www.craigball.com/What%20Every%20Lawyer%20Should%20Know%20About%20E-Discovery_FINAL.pdf [dostęp: 13.03.2018].

Digital Evidence & Computer Forensics, David Nardoni CISSP, EnCE, http://wwwscf.usc.edu/~uscsec/images/DigitalEvidence&ComputerForensicsversion1.2USC.pdf [dostęp: 13.03.2018].

Fundacja Panoptykon, *Monitoring w polskich miastach i w oczach społeczeństwa*, https://panoptykon.org/sites/default/files/publikacje/panoptykon_cctv_seminarium_10-10-2012_2.pdf [dostęp: 13.03.2018].

http://prawo.gazetaprawna.pl/galerie/1112478,duze-zdjecie,1,sciaganie-dowodow-w-sledztwach-od-gigantow-internetowych.html [dostęp: 13.03.2018].

Główny Urząd Statystyczny, *Społeczeństwo informacyjne w Polsce. Wyniki badań statystycznych z lat 2013–2017*, http://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-

informacyjne/spoleczenstwo-informacyjne-w-polsce-wyniki-badan-statystycznych-z-lat-2013-2017,1,11.html [dostęp: 13.03.2018].

Goodison S.E., Davis R.C., Jacksons B.A., *Digital Evidence and the U. S. Criminal Justice System, Report on behalf of the U.S. Department of Justice, National Institute of Justice (NIJ), the RAND Corporations*, https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf [dostęp: 13.03.2018].

Gubanov Y., *Retrieving Digital Evidence: Methods, Techniques and Issues*, Belcasoft, https://belkasoft.com/download/info/Retrieving%20Digital%20Evidence%20-%20Methods,%20Techniques%20and%20Issues.pdf [dostęp: 13.03.2018].

Gubanov Y., Afonin O., *SSD Forensics 2014. Recovering Evidence from SSD Drives: Understanding TRIM, Garbage Collection and Exclusions*, https://belkasoft.com/download/info/SSD%20Forensics%202014.pdf [dostęp: 13.03.2018].

Hitchcock A., Holmes R., Sundorph E., *Bobbies on the Net: A Police Workforce for the Digital Age*, http://www.reform.uk/wp-content/uploads/2017/08/Bobbies-on-the-net.pdf [dostęp: 13.03.2018].

IACP TECHNOLOGY POLICY FRAMEWORK, January 2014, http://www.theiacp.org/Portals/0/documents/pdfs/IACP%20Technology%20Policy%20Framework%20January%202014%20Final.pdf [dostęp: 13.03.2018].

Kessler G.C., *Judges' Awareness, Understanding, and Application of Digital Evidence*, A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy, Fort Lauderdale, USA, 2010, www.garykessler.net/library/kessler_judges&de.pdf [dostęp: 13.03.2018].

Knutson T., *Filesystem Timestamps: What Makes Them Tick?*, https://www.sans.org/reading-room/whitepapers/forensics/filesystem-timestamps-tick-36842 [dostęp: 13.03.2018].

Najwyższa Izba Kontroli, *Funkcjonowanie miejskiego monitoringu wizyjnego*, 2014, https://www.nik.gov.pl/aktualnosci/nik-o-miejskim-monitoringu-wizyjnym.html [dostęp: 13.03.2018].

Unreliable Informants: IP Addresses, Digital Tips and Police Raids, https://www.eff.org/pl/node/93067 [dostęp: 13.03.2018].

Urząd Komunikacji Elektronicznej, *Badanie konsumenckie 2017*, https://www.uke.gov.pl/akt/badanie-konsumenckie-2017,50.html [dostęp: 13.03.2018].

Związek Pracodawców Branży Internetowej IAB Polska, Raport *Internet Rzeczy w Polsce*, https://iab.org.pl/wp-content/uploads/2015/09/Raport-Internet-Rzeczy-w-Polsce.pdf [dostęp: 13.03.2018].