Krzysztof Krassowski

Kilka uwag o kryminalistyce w świecie informacji cyfrowej oraz stojących przed nią wyzwaniach

Studia Prawnoustrojowe nr 27, 153-163

2015

Krzysztof Krassowski
Katedra Kryminalistyki i Medycyny Sądowej
Wydział Prawa i Administracji UWM

Kilka uwag o kryminalistyce w świecie informacji cyfrowej oraz stojących przed nią wyzwaniach

Wprowadzenie

Od jej początków w XIX wieku losy nowoczesnej kryminalistyki związane są dosyć ściśle z najszerzej ujmowanym postępem cywilizacyjnym i wszelkimi jego przejawami. Wszak sama kryminalistyka powstała jako naturalna odpowiedź na nowe potrzeby organów ścigania i konieczność zapewniania bezpieczeństwa publicznego w obliczu przemian społecznych i gospodarczych zapoczątkowanych rewolucją przemysłową w Anglii i Szkocji jeszcze w XVIII wieku. Rozwój cywilizacji, pociągający za sobą różnego rodzaju skutki, stał się zatem jakby katalizatorem wytwarzania skorelowanych z postępem w zakresie nauk przyrodniczych i technicznych metod oraz badań kryminalistycznych, znajdujących swe zastosowanie przede wszystkim w sferze zainteresowania organów ścigania oraz wymiaru sprawiedliwości.

W opisanym powyżej związku kryminalistyki z postępem wyraża się najpełniej eklektyczność oraz kompleksowość tej pierwszej – cecha podkreślana zgodnie przez doktrynę, mimo utrzymujących się różnic w definiowaniu ogólnego zakresu oraz przedmiotu współczesnej kryminalistyki[1]. Nie zaskakuje zatem będący przedmiotem niniejszego opracowania szybki rozwój metod i badań kryminalistycznych w sferze technologii cyfrowego przetwarzania, przekazywania oraz przechowywania informacji, bez których trudno nawet wyobrazić sobie zarówno funkcjonowanie społeczeństwa informacyjnego XXI wieku, jak i skuteczne zwalczanie narastającej przestępczości teleinformatycznej. Warto przy tym rozważyć w szczególności dalsze perspektywy kryminalistyki w świecie cyfrowym oraz możliwe sfery zastosowań osiągnięć tej nauki, kreujące się obok oczywistego i dominującego aspektu karnoprocesowego. Rozważania podjęte w niniejszym opracowaniu mają charakter generalny – koncentrują się bardziej na kwestiach systemowych niż na partykularnych rozwiązaniach przyjętych na ich podstawie w poszczególnych krajach świata.

[1] E. Gruza, M. Goc, J. Moszczyński, *Kryminalistyka – czyli rzecz o metodach śledczych*, Warszawa 2008, s. 19–22.

Społeczeństwo informacyjne – nowe rodzaje zagrożeń

Społeczeństwo informacyjne to takie, które (wobec mnogości istniejących definicji) można syntetycznie określić jako oparte na szczególnym, wysoko cenionym i wymiennym dobrze niematerialnym – informacji, funkcjonujące w oparciu o jej przetwarzanie, przesyłanie oraz przechowywanie. Jest to więc społeczeństwo zależne w wysokim stopniu od nieustannego rozwoju i zapewniania prawidłowego, bezpiecznego funkcjonowania technologii, które umożliwiają wymagany obieg oraz dostępność niezbędnych informacji. Sama zaś informacja – będąc najcenniejszym dobrem, jak też podstawowym towarem w społeczeństwie informacyjnym – jest z jednej strony zagrożona nowymi rodzajami przestępczości, zaś z drugiej możliwa do zastosowania lub wykorzystania jako narzędzie przestępstwa o charakterze tak lokalnym, jak globalnym.

Rozwijająca się gwałtownie przestępczość w świecie cyfrowym (ang. *cyber crime*), określana także tradycyjnie jako przestępczość komputerowa, podlega nieustannej ewolucji, eksplorując coraz to nowe obszary i możliwości działań przestępczych – wynikające choćby z globalnego upowszechniania się dostępu do sieci Internet oraz rewolucji w dziedzinie technologii mobilnych w XXI wieku. Nie wchodząc zatem w zbędne rozważania teoretyczne czy semantyczne, wypada skonstatować, iż w pojęciu tym mieszczą się zarówno przestępstwa skierowane przeciwko wszelkim urządzeniom komputerowym czy dostępowym, umożliwiającym akces do cyberprzestrzeni (np. smartfonom), jak i te popełniane przy wykorzystaniu takich urządzeń czy oferowanych przez nie funkcjonalności (np. mobilnego dostępu do mediów społecznościowych). Co istotne, działalność taka jest coraz częściej domeną zorganizowanych grup przestępczych, także o charakterze międzynarodowym[2]. Warto odnotować, iż w wielu przypadkach mowa nie tyle o nowych rodzajach przestępczości jako takich, a o efektywnym wykorzystywaniu możliwości oferowanych przez cyfrowy świat i stosowane w nim powszechnie narzędzia przetwarzania, przesyłu i przechowywania informacji do popełniania czynów znanych kryminalistyce od dawna – np. kradzieży, oszustw, aktów terroru czy też obcowania płciowego z małoletnim albo złożenia propozycji takiego obcowania (przy nawiązaniu kontaktu za pomocą systemu teleinformatycznego – art. 200a k.k.[3]).

Wszystko to stanowi niewątpliwe wyzwanie dla współczesnej kryminalistyki, która powinna zapewniać ciągłe wypracowywanie narzędzi, metod oraz wyspecjalizowanych badań umożliwiających nie tylko przeciwdziałanie zaistnieniu w świecie cyfrowym zdarzeń o charakterze przestępczym, ale również skuteczne dochodzenie przestępstw już zaistniałych oraz ustalanie ich sprawców – podobnie jak dzieje się to w każdej innej sferze życia czy funkcjonowania społeczeństwa, w której mogą

[2] Źródło i więcej na ten temat [online] <www.interpol.int/Crime-areas/Cybercrime> (dostęp: 30.06.2014).

[3] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. nr 88, poz. 553 z poźn. zm.).

występować takie zjawiska. Co ciekawe, ze względu na wieloaspektowość i kompleksowość głównego dobra, a jednocześnie towaru, jakim jest informacja, wypracowywane metody i narzędzia pierwotnie kryminalistyczne mają w świecie cyfrowym także realną szansę na naturalne znalezienie zastosowań innych niż objęte bezpośrednim zainteresowaniem organów ścigania – i to nie tylko w sferze komercyjnej, ale również prywatnej (np. lokalizacja osoby w sieci mobilnej jako aplikacja usługowa).

Kryminalistyka w świecie informacji cyfrowej

Kryminalistyka w świecie cyfrowym ma stosunkowo niedługą, aczkolwiek znaczącą historię. Jest oczywiście związana z rozwojem technologii komputerowych oraz sieciowych i coraz powszechniejszym ich stosowaniem w coraz większej liczbie sfer życia publicznego oraz prywatnego. W praktyce należy odnotować przełom lat 70. i 80. XX wieku jako czas boomu komputerowego, początek lat 90. jako czas rozpowszechniania dostępu do sieci Internet i przełom XX oraz XXI wieku jako okres technologicznej rewolucji mobilnej – trzy kamienie milowe w rozwoju technologicznym, mające zasadnicze znaczenie dla rozwoju społeczeństwa informacyjnego oraz możliwości wykorzystania jego osiągnięć także w celach niezgodnych z obowiązującym prawem. Zaistniały zatem jednocześnie nowe możliwości i wyzwania dla przestępców, organów ścigania, rządów, obywateli czy wreszcie biznesu i nauki[4].

Należy zauważyć, że próba ujęcia całości aktywności o charakterze kryminalistycznym bądź związanych z kryminalistyką w świecie cyfrowym napotyka na utrzymujące się trudności o charakterze terminologicznym. Jest to związane z wieloaspektowością informacji w postaci cyfrowej, która może być w istocie aplikowana, wykorzystywana czy też badana jednocześnie w wielu różnych celach – w tym zgodnych i sprzecznych z prawem. W literaturze anglojęzycznej stosowanych jest równocześnie kilka pojęć, których zakresy przedmiotowe są uznawane przez niektórych autorów za pokrywające się, zaś przez innych za odrębne[5]. Tradycyjnie najwcześniej zaistniało pojęcie *computer forensics* – popularnie, aczkolwiek może nie do końca trafnie, określane mianem informatyki śledczej, z czasem ewoluujące w stronę coraz powszechniej stosowanych terminów: *digital forensics* lub *digital forensic science*. Dodatkową trudność sprawia tu kwestia różnych kręgów kulturowych, gdyż samo *forensics* lub *forensic science* z kręgu anglosaskiego odpowiada raczej węziej pojmowanej ekspertyzie kryminalistycznej niż ogólnej nauce krymina-

[4] M. Caloyannindes, N. Memon, W. Venema, *Digital Forensics – Guest Editor Introduction*, "IEEE Computer", marzec-kwiecień 2009, s. 16.

[5] M. Kohn, J.H.P. Eloff, M.S. Olivier, *Framework for a Digital Forensic Investigation*, [w:] H.S. Venter, J.H.P. Eloff, M.M. Labushagne (red.), *Proceedings of the ISSA 2006 from Insight to Foresight Conference*, Sandton (RPA), lipiec 2006, s. 2, [online] <www.mo.co.za> (dostęp: 28.06.2014).

listyki w krajach Europy Środkowej i Wschodniej, w tym i w Polsce. Stąd też zaproponowane tu pojęcie „kryminalistyka cyfrowa" należy interpretować wyłącznie funkcjonalnie, nie skupiając się na kwestii semantycznej.

Wśród wielu konkurujących ze sobą definicji warto przywołać następującą: kryminalistyka cyfrowa to stosowanie ugruntowanych metod naukowych w celu zachowania, zbierania, walidacji, identyfikacji, analizowania, interpretacji, dokumentowania oraz prezentacji dowodów cyfrowych otrzymanych ze źródeł cyfrowych w celu umożliwienia lub ułatwienia rekonstrukcji zdarzeń o charakterze kryminalnym albo też pomocy w przewidywaniu nieautoryzowanych akcji mogących zakłócać planowane działania[6]. Podkreśla się przy tym często, że jakkolwiek podstawowym celem kryminalistyki cyfrowej jest przedstawienie środków dowodowych akceptowalnych przez wymiar sprawiedliwości w ramach procedury karnej oraz coraz częściej cywilnej, to efekty jej zastosowań oraz rezultaty przeprowadzonych badań mają praktyczne odzwierciedlenie – o czym wspomniano już wcześniej – także w sferach gospodarczej (korporacyjnej) oraz prywatnej. Trzeba w tym kontekście odnotować, że stosowanie metod badawczych kryminalistyki cyfrowej w celach ściśle dowodowych wymaga ich odróżnienia od aplikacji w sferze pozaprocesowej (czy szerzej: leżącej poza zakresem zainteresowania organów ścigania), pomimo – co może być mylące – wykorzystywania tych samych narzędzi i zasobu wiedzy specjalistycznej[7], np. w celach zapewniania ogólnego bezpieczeństwa funkcjonującego systemu teleinformatycznego. Podstawowe różnice przedstawia syntetycznie poniższe zestawienie:

Różnice w zastosowaniach metod kryminalistyki cyfrowej według celu

Zapewnianie bezpieczeństwa	Przedstawianie środka dowodowego
Zabezpiecza system przed atakiem	Nie zabezpiecza systemu przed atakiem
Działa zwykle w czasie rzeczywistym	Jest dokonywane po fakcie – po zaistnieniu zdarzenia kryminalnego
Jest wykonywane przez specjalistów z branży technologii informacyjnych	Może być wykonywane przez specjalistów z branży technologii informacyjnych, ale nie jest to obowiązkowe (ekspertyza kryminalistyczna)
Ograniczona prezentacja problemów i nowych rozwiązań w świecie zewnętrznym	Osiągnięty środek dowodowy jest co do zasady prezentowany poza ograniczonym kręgiem personelu IT
Może być ominięte przez zaufanych użytkowników	Integralność środka dowodowego jest najwyższym priorytetem

Źródło: G. Ruibin, M. Gaertner, *Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework*, "International Journal of Computer Evidence" 2005, t. 4(1), s. 4.

[6] G. Ruibin, M. Gaertner, *Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework*, "International Journal of Computer Evidence" 2005, t. 4(1), s. 1.

[7] R.J. Walls, B.N. Levine, M. Liberatore, C. Shields, *Effective Digital Forensics Research is Investigator-Centric*, Georgetown University, Washington D.C. 2011, s. 1, [online] <www.static.usenix.org> (dostęp: 10.06.2014).

Z czysto utylitarnego, pragmatycznego punktu widzenia należy się także zgodzić z ogólniejszym stanowiskiem, iż o tym, czy dany proces badawczy (wykonywana ekspertyza) przeprowadzony z wykorzystaniem ustalonej metodologii, a dotyczący informacji w postaci cyfrowej można określić jako kryminalistyczny *sensu stricto* czy też nie, decydować będzie ostatecznie możliwość wykorzystania jego rezultatów jako środka dowodowego w sądzie[8].

Powyższe rozważania uprawniają do postawienia pytań o charakterze zasadniczym: czy w takim stanie rzeczy kryminalistyka cyfrowa może być uznawana za odrębny dział kryminalistyki oraz czy jej produkty, które dla potrzeb tego opracowania możemy nazwać dowodami cyfrowymi, spełniają konsekwentnie wymagania stawiane dowodom naukowym przy aktualnym stanie wiedzy.

Na wstępie warto wziąć pod uwagę sposób, w jaki powstała i rozwinęła się informatyka śledcza i dalej kryminalistyka cyfrowa. Co interesujące, dyscyplina ta nie została wypracowana w laboratoriach kryminalistycznych, a powstała niejako oddolnie, motywowana potrzebami funkcjonariuszy dochodzeniowo-śledczych, którzy wraz z upowszechnieniem się komputerów i urządzeń zawierających dane cyfrowe zaczęli samodzielnie pozyskiwać informacje przydatne do prowadzonych postępowań, badając zabezpieczony sprzęt komputerowy, do którego mieli fizyczny dostęp[9]. Z czasem, dostrzegając ważkość problemu i potencjalne możliwości związane z dowodami cyfrowymi, podjęto próby skoordynowania działań organów ścigania oraz określenia zasad i procesów badań zabezpieczonych źródeł dowodowych – w czym prym wiodły rozwinięte technologicznie Stany Zjednoczone. Początki takich działań miały miejsce już w połowie lat 80. XX wieku – wówczas powstały programy, których celem było określenie zasad badania komputerów jako źródeł dowodowych (m.in. Federalne Biuro Śledcze w 1984). Niedługo później, w odpowiedzi na lawinowo rosnące zapotrzebowanie w zakresie takich badań, powołano do życia stały zespół ds. analiz komputerowych FBI (CART), którego struktura i metodyka działań została z sukcesem skopiowana w wielu innych agencjach federalnych. Z czasem badania tego typu przesunięto do struktur laboratoriów kryminalistycznych, co stało się standardowym rozwiązaniem organizacyjnym pod koniec XX wieku, obok rozwijającej się współpracy międzyagencyjnej, a z czasem i międzynarodowej na forum tworzonych grup roboczych, najpierw o charakterze czysto technicznym, a z czasem również naukowo-badawczym. Można tu choćby przywołać działalność Technicznej Grupy Roboczej ds. Dowodów Cyfrowych (TWGDE) istniejącej od początku lat 90. czy powołanie pod koniec tej dekady Międzynarodowej Organizacji ds. Dowodów Komputerowych (IOCE)[10]. Procesy takie zachodziły nie

[8] B.D. Carrier, E.H. Spafford, *An Event-Based Digital Forensic Investigation Framework*, Digital Forensic Research Workshop 2004, Baltimore, 11–13 sierpnia 2014, s. 3, [online] <www.digital-evidence.org> (dostęp: 11.06.2014).

[9] E. Casey, *Handbook on Digital Forensics and Investigation*, Elsevier Inc. 2010, s. 2.

[10] C.M. Whitcomb, *An Historical Perspective on Digital Evidence: A Forensic Scientist's View*, "International Journal of Digital Evidence" 2002, t. 1(1), s. 1–2.

tylko w USA, ale także w Europie, głównie pod egidą Europejskiej Sieci Instytutów Nauk Sądowych (ENFSI), gdzie od początku bieżącego stulecia prowadzone są w przedmiotowym zakresie intensywne prace na forum Grupy Roboczej ds. Technologii Informacyjnych w Kryminalistyce (WG FIT)[11] . Można zatem skonstatować, że rozwój kryminalistyki cyfrowej jako odrębnej dyscypliny czy gałęzi kryminalistyki ma u swoich podstaw potrzebę znalezienia w stworzonych strukturach kooperacji technicznych rozwiązań problemów o charakterze prawnym – karnym oraz cywilnym – gdzie od samego początku rozważano priorytetowo kwestię dopuszczalności uzyskanych środków dowodowych w postępowaniach sądowych[12].

Jak się zatem wydaje, z czysto instytucjonalnego punktu widzenia – istnienia wyodrębnionych struktur, dedykowanych tej dziedzinie w laboratoriach kryminalistycznych, w tym policyjnych, a także wyspecjalizowanych organizacji współpracy o charakterze regionalnym i międzynarodowym – są podstawy do uznania kryminalistyki cyfrowej za samoistną gałąź badań i rozważań kryminalistycznych. Należy jednak rozważyć dodatkowo bardzo specyficzny aspekt związany z ogólnymi prawami, jakie rządzą materiałem (śladami) będącym przedmiotem poszczególnymi rodzajów wykonywanych badań. O ile bowiem w klasycznych, wyodrębnionych badaniach kryminalistycznych, np. śladów mechanoskopijnych czy też najbardziej rozpowszechnionych aktualnie śladów biologicznych, mamy do czynienia z ustanowionym i niezmiennym zestawem ogólnych praw będących fundamentem i punktem odniesienia w naukowo ugruntowanych procesach badawczych dotyczących śladów, tak jak prawa fizyki w zastosowaniu do mechanoskopii, albo też zestawem praw głęboko zrozumianych naukowo i trwale przewidywalnych jak prawa ewolucji w odniesieniu do biologii, o tyle w przypadku świata informacji cyfrowej sytuacja jest całkowicie odmienna. Trzeba sobie bowiem uświadomić, że mamy tu do czynienia z sytuacją, gdy eksperci (powoływani biegli sądowi) mogą być w każdej chwili skonfrontowani z materiałem pochodzącym z zupełnie nowej, rządzącej się własnymi prawami rzeczywistości cyfrowej, której kształt i zasady uzależnione są wyłącznie od ludzkiej pomysłowości[13]. Mając na uwadze, że tempo rozwoju technologicznego w świecie cyfrowym jest generalnie nadal zgodne z zasadą sformułowaną w prawie Moore'a[14], gdzie każda nowa generacja technologii zastępuje poprzednią w interwale około 2 lat, jesteśmy konfrontowani z sytuacją ciągłej i bardzo szybkiej ewolucji praw i zasad rządzących dziedziną, w której celem jest przeprowadzenie uznaną metodologią badań materiału cyfrowego i osiągnięcie na tej podstawie dowodu naukowego akceptowalnego przez sąd w postępowaniach karnych oraz cywilnych.

---

[11] Statute of ENFSI Forensic Information Technology Working Group (FIT-WG) [online] <www.enfsi.eu> (dostęp: 16.06.2014).

[12] R. McKemmish, *When is Digital Evidence Sound?*, [w:] R. Indrajit, S. Sujeet (red.), *Advances in Digital Forensics IV*, International Federation for Information Processing 2008, t. 285, s. 4.

[13] A.M. Marshall, *Digital Forensics: Digital Evidence in Criminal Investigation*, John Wiley & Sons Ltd. 2008, s. 1.

[14] Więcej o prawie Moore'a: G.E. Moore, *Cramming More Components onto Integrated Circuits*, "Electronics Magazine" kwiecień 1965, nr 38 (8).

Powyższe nie czyni, rzecz jasna, łatwiejszym spełnienia ogólnie akceptowanych w świecie współczesnej kryminalistyki wymagań stawianych dowodom naukowym – czyli zarówno kryterium powszechnej akceptacji Frye'a, zgodnie z którym źródło dowodów naukowych stanowić mogą jedynie takie metody i aparatura badawcza, które zostały zaaprobowane przez ogół ekspertów z danej dziedziny, jak też standardu Dauberta, określającego następujące kryteria oceny dowodów naukowych:

- falsyfikacji – czy zastosowana przez eksperta teoria i technika była sprawdzana (poddana kontroli)?
- publikacji oraz recenzji – czy dana teoria lub technika była przedmiotem publikacji w literaturze fachowej, a także czy była ona przedmiotem naukowej recenzji?
- wartości diagnostycznej i standaryzacji – czy jest znana lub możliwa do przewidzenia stopa błędów występujących w zastosowanej technice badawczej?
- powszechnej akceptacji – czy zastosowana przez eksperta teoria i technika zyskały sobie powszechną akceptację?[15]

Dowody cyfrowe przeszły wszakże na przestrzeni ostatnich dwóch dekad proces istotnego rozwoju, zaś źródła ich słabości w kontekście naukowym zostały głęboko zrozumiane i dobrze opisane – dzięki czemu podjęto globalnie stosowne działania zaradcze. Słabości te wynikają generalnie z trzech rozpoznanych przyczyn:

- braku w miarę jednolitego, powszechnie akceptowanego systemu certyfikacji czy listy niezbędnych kwalifikacji, jakimi mieliby się legitymować eksperci (biegli) z tej dziedziny;
- braku istnienia w miarę koherentnego systemu edukacji, nabywania doświadczenia oraz szkoleń, któremu mieliby podlegać eksperci badający dowody cyfrowe;
- ciągle istniejącej tendencji do traktowania przez niektóre instytucje i agencje rządowe informacji cyfrowych raczej w kontekście źródeł informacji o charakterze operacyjnym niż potencjalnie dowodowym[16].

Remedium na opisane problemy wydaje się być przede wszystkim wyjątkowo ścisła współpraca regionalna oraz międzynarodowa, której celem jest unifikacja stosowanych metod oraz procesów badawczych w zakresie dowodów cyfrowych, dokonywana intensywnie na kilku płaszczyznach, w tym z udziałem Interpolu prowadzącego szeroko zakrojone programy m.in. koordynacji regionalnej dla poszczególnych kontynentów, a także wsparcia działań narodowych w ramach tzw. laboratorium cyfrowego (Digital Forensic Laboratory). Na naszym kontynencie ma to przede wszystkim miejsce na forum wspomnianej już wcześniej Europejskiej Sieci Instytutów Nauk Sądowych. Efektem tych działań jest wspieranie standaryzacji metod oraz narzędzi badawczych stosowanych w laboratoriach kryminalistycznych i dotyczących dowodów cyfrowych (obok innych dziedzin, gdzie procesy takie są już bardzo zaawansowane – np. badań DNA czy badań daktyloskopijnych), a także zapewnia-

[15] D.J. Ryan, G. Shpantzer, *Legal Aspects of Digital Forensics*, George Washington University, Washington 2005, s. 2 [online] <www.ebooksmagz.com> (dostęp: 18.06.2014).

[16] E. Casey, *Handbook of Digital Forensics*..., s. 2.

nia ich należytej wiarygodności w ramach wdrażania systemu jakości w oparciu o normę ISO/IEC 170025 i przewodnik ILAC G-19:2002. W wymiarze praktycznym efektem prac ENFSI jest wydany po raz pierwszy w roku 2005 i wielokrotnie aktualizowany poradnik w zakresie najlepszych praktyk w kryminalistycznych badaniach technologii cyfrowych[17]. Podobne publikacje są także tworzone od początku XXI wieku na poziomie narodowym – warto tu wspomnieć przede wszystkim o amerykańskiej publikacji pt. „Dowody cyfrowe – standardy i zasady", wydanej pod auspicjami Naukowej Grupy Roboczej ds. Dowodów Cyfrowych[18], jak też o brytyjskim poradniku Związku Szefów Funkcjonariuszy Policji (ACPO) w sprawie dobrych praktyk dotyczących dowodów cyfrowych, opublikowanego po raz pierwszy w 2007 r.[19] Wszystkie one przedstawiają szeroko akceptowane zasady postępowania z materiałem cyfrowym oraz uznaną metodologię jego badań, dążąc tym samym do osiągnięcia standaryzacji i zapewnienia odpowiedniej jakości dowodów cyfrowych w celu ich ostatecznej dopuszczalności przed sądem. Kolejnym elementem, na który zwraca się uwagę, jest zapewnienie odpowiedniej edukacji przyszłych ekspertów z zakresu kryminalistyki cyfrowej, co w niektórych najbardziej rozwiniętych krajach znajduje wyraz we wdrożeniu wyspecjalizowanych programów nauczania na poziomie pomaturalnym, kształcących specjalistów w tej dziedzinie – niektóre z nich zostały uruchomione już kilkanaście lat temu (od 2003)[20].

Mając powyższe na uwadze, wydaje się, że na aktualnym etapie rozwoju kryminalistyka w świecie cyfrowym jest już niewątpliwie nową, wydzieloną gałęzią tej dyscypliny naukowej. Pomimo dodatkowych problemów w zakresie ekspertyzy kryminalistycznej, wynikających z samej natury świata cyfrowego i rządzących nim nieustannie zmiennych praw, działania podjęte w ramach współpracy międzynarodowej, standaryzacji oraz edukacji, umożliwiają aktualnie przedstawianie wiarygodnych środków dowodowych dopuszczanych w ramach praktyki wymiaru sprawiedliwości. O usamodzielnieniu się kryminalistyki cyfrowej może również świadczyć fakt, iż prestiżowa i powszechnie szanowana w świecie nauki organizacja, jaką jest Amerykańska Akademia Nauk Sądowych (American Academy of Forensic Sciences), w 2008 r. wyodrębniła w swych ramach – po raz pierwszy od 28 lat – nową sekcję w zakresie nauk cyfrowych i multimedialnych (Digital and Multimedia Sciences)[21].

Dla uzupełnienia wszystkich powyższych rozważań wypada zauważyć, że koncentrowały się one na problemach ogólnych, systemowych w zakresie dominujące-

[17] Dokument ENFSI "Guideliness for Best Practice in the Forensic Examination of Digital Technology" (FIT-2005-001 Issue 6), [online] <www.enfsi.org> (dostęp: 7.06.2014).

[18] Dokument Digital Evidence "Standards and Principles, Scientific Working Group on Digital Evidence", październik 1999 [online] <www.fbi.gov> (dostęp: 7.06.2014).

[19] Dokument ACPO "Good Practice Guide for Digital Evidence" v. 5, ACPO 2007–2012, [online] <www.acpo.police.uk> (dostęp: 7.06.2014).

[20] Kessler G.C., Schirling M.E., The Design of an Undergraduate Degree Program in Computer & Digital Forensics, "Journal of Digital Forensics, Security And Law" 2006, t. 1(3), s. 37–38.

[21] E. Casey, *Digital Evidence and Computer Crime: Forensic Science*, Computers and the Internet, 3rd ed., Elsevier Inc. 2011, s. 10

go, eksperckiego oraz dowodowego zastosowania kryminalistyki w świecie informacji cyfrowej. Trzeba przy tym zaznaczyć, że w związku z rosnącym znaczeniem prewencyjnej funkcji kryminalistyki w dzisiejszym świecie globalnych zagrożeń (w tym terroryzmem) potencjał wykorzystania osiągnięć tej nauki nie ogranicza się w rzeczywistości cyfrowej wyłącznie do ekspertyzy kryminalistycznej. Jest w nim bowiem przestrzeń do realizacji wielu wyrafinowanych technologicznie przedsięwzięć mających na celu bądź to ogólne zapobieganie przestępczości, bądź też umożliwiających unikanie najgorszych skutków określonych kategorii czynów i zdarzeń (np. programy zapobiegania uprowadzeniom nieletnich typu Amber Gold). Jednakże ze względu na rozległość i kompleksowość tej problematyki, powinna być ona przedmiotem pogłębionej refleksji w odrębnych opracowaniach.

Perspektywy i wyzwania kryminalistyki w świecie cyfrowym

Rosnące uzależnienie społeczeństwa informacyjnego od narzędzi technologicznych sprawia, że zakres zainteresowania organów ścigania światem cyfrowym stale się poszerza – będąc efektem narastającej i coraz bardziej wyrafinowanej przestępczości w tej sferze. Można więc bez ryzyka większego błędu założyć, że zapotrzebowanie na kryminalistykę w ogólności, a na ekspertyzę kryminalistyczną w szczególności będzie mogło tu jedynie z czasem wzrastać. Warto poczynić zatem ogólne obserwacje co do możliwych trendów rozwojowych oraz wyzwań rysujących się w nieodległej przyszłości przed kryminalistyką cyfrową.

Trzeba przed wszystkim zauważyć, że trendy rozwojowe w zakresie kryminalistyki będą wyznaczane przez kierunki rozwoju technologii. Już dzisiaj da się zauważyć przenoszenie środka ciężkości technologii w stronę rozwiązań mobilnych, oferujących nieograniczony w czasie i przestrzeni dostęp do globalnej sieci Internet. Stąd też zasadne wydaje się stanowisko, że w najbliższej przyszłości szybko ewoluujące urządzenia dostępowe do sieci mobilnych – znane obecnie jako smartfony – będą z jednej strony elementem najbardziej narażonym na nowe zagrożenia, zaś z drugiej najbardziej powszechnym narzędziem wykorzystywanym do popełniania przestępstw[22]. Drugim szczególnie szybko rozwijającym się obszarem technologii, w zakresie którego niezbędne jest w najbliższej przyszłości szczególne skupienie uwagi ekspertów kryminalistyki, jest „chmura obliczeniowa" (*cloud computing*), a więc wyniesienie na zewnątrz oraz witrualizacja zasobów obliczeniowych wykorzystywanych przez użytkowników na zasadzie usługi dostarczanej przez podmioty zewnętrzne, bez potrzeby posiadania własnej infrastruktury. „Chmura obliczeniowa" zasadniczo zmieniła sposób, w jaki tworzone, dostarczane, udostępniane oraz zarzą-

[22] A. Rizwan, R.V. Dharaskar, *Mobile Forensics: an Overview, Tools, Future Trends and Challenges from Law Enforcement Perspective*, [w:] *Sixth International Conference of E-governance (ICEG 08)*, IIT and NSIT, New Delhi 2008, s. 321.

dzane są usługi informacyjne, stworzyła także model globalnej replikacji danych w niej przechowywanych. Jest to zjawisko wielowymiarowe, a nie tylko technologiczne, zmusza bowiem do rozważenia np. kwestii różnych jurysdykcji dotyczących miejsc, w których przechowywane są dane w „chmurze", czy ogólnej ilości danych niezbędnych do przeanalizowania w procesach badawczych związanych z ekspertyzą kryminalistyczną[23]. Oceniając rzecz całą z nieco ogólniejszej perspektywy, głównym wyzwaniem kryminalistyki cyfrowej jest z pewnością nadążanie metod i procesów badawczych za niezwykle szybką ewolucją świata cyfrowego, którego kierunek rozwoju jest na dodatek mało przewidywalny.

Nie brakuje też idących dalej opinii, że po okresie „złotej ery"' kryminalistyki cyfrowej z czasów pierwszej dekady bieżącego wieku, gdzie odgrywała ona rolę swoistego magicznego instrumentu pozwalającego zobaczyć przeszłość za pomocą odtworzenia skasowanych danych oraz wejść w umysł przestępcy poprzez odzyskanie jego poczty elektronicznej czy wiadomości typu SMS, dziedzina ta stoi w obliczu fundamentalnego kryzysu spowodowanego opisanym już wcześniej tempem oraz ciągłą ewolucją postępu technologicznego. Wśród jego symptomów wymieniane są zarówno kwestie nadmiaru urządzeń oraz danych wymagających jednocześnie badań oraz analizy, coraz większej mobilności czy przenośności urządzeń służących do ich przechowywania (np. pamięci typu pendrive), wzrastającej różnorodności systemów operacyjnych oraz rodzajów plików, coraz bardziej zaawansowanego zabezpieczania informacji za pomocą mechanizmów kryptograficznych, rozproszenia badanych danych w „chmurze obliczeniowej" oraz problematyka rozwiązań natury legislacyjnej, ograniczających swobodę prowadzonych badań i analiz kryminalistycznych[24]. To, w jaki sposób i czy w ogóle kryminalistyka cyfrowa poradzi sobie ze stojącymi przed nią wyzwaniami, będzie tak krytyczne dla możliwości skutecznego ścigania przestępstw w świecie informacji cyfrowej, jak interesujące do obserwacji i analizy na gruncie nauki kryminalistyki.

[23] K. Ruan, J. Carthy, T. Kechadi, M. Crosbie, *Cloud Forensics*, [w:] G. Peterson, S. Shenoi (red.), *Advances in Digital Forensics VII*, IFIP AICT 361, International Federation for Information Processing 2011, s. 35-36.

[24] S.L. Garfinkel, *Digital Forensics Research: The Next 10 Years*, "Digital Investigation" 2010, nr 7, s. 66.

Summary

Few remarks concerning forensic science in digital information world as well as challenges it is facing

Key words: digital forensics, forensic research, forensic examination, cyber crime, scientific evidence.

The present paper discusses general issues of the digital forensics and the challenges this discipline is facing in the foreseeable future. It provides short description of modern information society and the problems it is experiencing due to increasing dependency on technology. It concentrates on the history of development and the most important issues of digital forensics of today, including – but not limited to – the everchanging nature of digital world impacting ways and means of forensic expertise in this field, as well as fundamental problems of provision of digitial evidence. It gives an insight on how law enforcement and forensic communities try to accomodate to evolving circumstances in order to secure admissibility of the digital evidence at the courts of law. Finally the future challenges and development trends of digital forensics are presented for consideration.