Ars Iuridica 2023, Vol. 23, nr 1
DOI: 10.17951/szn.2023.23.1.65-76

Izabella Grens-Trykoszko
Uniwersytet w Białymstoku
iza.grens@gmail.com
ORCID: 0000-0002-7857-2100

Rola biegłego w czynności przeszukania pomieszczeń. Uwagi w kontekście informatyki śledczej

The role of an expert in searching premises. Comments in the context of computer forensics

ABSTRACT

The article is an attempt to prove the importance of the role of an IT expert as a consultant in the search of premises. The author proposes using the expert knowledge of the expert already at the initial stage of the pre-trial investigation in the course of revealing and securing digital traces. The study briefly characterizes the search institution as a non-repeatable evidence gathering step in the context of the specificity of digital traces as future electronic evidence. The main aspects of law enforcement cooperation with the expert in the field of IT as a consultant were also presented, as well as an attempt to indicate the reasons for the insufficient degree of engaging an expert in the indicated specialty at the initialstage of criminal proceedings.

Keywords: expert, consultant, search, digital traces, computer forensics.

WPROWADZENIE

Problematyka nowoczesnych technologii w procesie karnym nie ma wielu opracowań, jak i obszernego orzecznictwa sądowego. Tymczasem niemal w każdym postępowaniu przygotowawczym mamy do czynienia z dowodami elektronicznymi. Informatyzacja życia codziennego sprzyja przypisaniu tej kategorii dowodów miana istotnych – zawartość nośników elektronicznych może bowiem dostarczyć organom ścigania cennych danych o figurujących w postępowaniu osobach: ich przeszłości, jak i planach, życiu prywatnym, zawodowym, cechach

osobowości czy stanie zdrowia. Bez wątpienia nośniki teleinformatyczne są celem, np. hackingu, narzędziem popełnienia przestępstwa, np. rozpowszechniania pornografii, a także świadkiem, np. kontaktów członków zorganizowanych grup przestępczych. Pozyskiwanie tej kategorii materiałów odbywa się m.in. w toku przeszukania pomieszczeń. O ile standardy zabezpieczenia śladów i dowodów przed ich zniesieniem, zatarciem i zniekształceniem wyznaczają nie normy prawa karnego procesowego, a kryminalistyka, o tyle coraz bardziej aktualny wydaje się postulat angażowania biegłego z zakresu informatyki w czynności zmierzające do ujawnienia i zabezpieczenia przyszłych dowodów elektronicznych. Niniejszy artykuł stanowi przyczynek do rozważań o wykorzystywaniu eksperckiej wiedzy biegłego z zakresu informatyki już na wstępnym etapie postępowania przygotowawczego, kiedy podjęte w ramach czynności niepowtarzalnej działania mają realny wpływ na całokształt ustaleń i podjęcie końcowej decyzji merytorycznej. Z uwagi zaś na analizowany etap postępowania karnego zasadne jest zawężenie opracowania do kryminalistycznej – śledczej sfery informatyki.

ŚLADY CYFROWE JAKO CZYNNIKI IMPLIKUJĄCE CZYNNOŚCI W POSTĘPOWANIU PRZYGOTOWAWCZYM

Każde działanie użytkownika systemu teleinformatycznego pozostawia po sobie ślad, który w kontekście cyberprzestępczości jest śladem cyfrowym, wirtualnym[1]. Takie następstwa działań użytkownika systemu definiowane są jako zmiany w kodzie binarnym systemu teleinformatycznego, a także w urządzeniach cyfrowych zdolnych do przetwarzania, wysyłania, gromadzenia pakietów danych, będących wynikiem ingerencji zewnętrznej (fizycznej) bądź wewnętrznej (zdalnej)[2]. Ślady wytwarzają zatem zarówno legalni użytkownicy systemu, jak i nieuprawnieni do wprowadzania w nim zmian sprawcy przestępstw. Bacząc na potrzebę stworzenia warunków, pozwalających na przeistoczenie śladów w procesowe dowody cyfrowe (elektroniczne), niezbędne jest odpowiednie zabezpieczenie śladów cyfrowych znajdujących się na nośnikach, urządzeniach, sprzęcie technicznym. Specyfika tych przedmiotów powoduje, iż tok ich zabezpieczenia winien odbyć się według ustalonych wcześniej metod i z wykorzystaniem zasad, które umożliwią następnie pozyskanie pożądanych przez organy procesowe treści. Niewątpliwie stanowi to wyzwanie dla organów śledczych, z uwagi na częste pozyskiwanie takich śladów w toku czynności niepowtarzalnej przeszukania pomieszczeń.

[1] Pojęcia te występują jako synonimy m.in. w A. Lach, *Dowody elektroniczne w procesie karnym*, Toruń 2004, W. A. Kasprzak, *Ślady cyfrowe. Studium prawno-kryminalistyczne*, Warszawa 2015.

[2] W. A. Kasprzak, *Ślady cyfrowe. Studium prawno-kryminalistyczne*, Warszawa 2015, s. 25. Por. także. H. Carvey, *Windows Forensic Analysis*, USA 2007, s. 20.

Przeszukanie pomieszczeń, zgodnie z regulacją w rozdziale 25 Kodeksu postępowania karnego[3], odbywa się w celu wykrycia, zatrzymania, znalezienia rzeczy mogących stanowić dowód w sprawie, jeżeli istnieją uzasadnione podstawy do przypuszczenia, że wymienione rzeczy znajdują się w miejscu wskazanym w postanowieniu o przeszukaniu pomieszczeń lub innych miejsc. Ta poszukiwawcza czynność dowodowa jest także środkiem przymusu pozwalającym na zgodne z prawem wkroczenie w sferę konstytucyjnie gwarantowanych praw i wolności osobistych (art. 41 ust. 1 Konstytucji RP) oraz nienaruszalności mieszkania (art. 50 Konstytucji RP)[4]. Uzasadnienia naruszenia konstytucyjnych wolności upatruje się w celu, jaki stawiają podejmowanej czynności organy śledcze, a mianowicie ujawnienia, zabezpieczenia i wprowadzenia do postępowania karnego śladów, które mogą stanowić wartość dowodową w postępowaniu karnym. Czynność przeszukania pomieszczeń stanowi tym samym skumulowanie funkcji wykrywczej, polegającej na bieżącym poszukiwaniu informacji o źródłach dowodowych przez funkcjonariuszy realizujących czynność przeszukania, oraz funkcji dowodowej, dającej podstawy do transformacji procesowej pozyskanych w toku przeszukania materiałów.

Warto przy tym wskazać, iż przeszukanie należy do kategorii czynności niepowtarzalnych, co oznacza, że nie tylko nie będzie jej można powtórzyć na rozprawie, ale nie będzie jej można w ogóle ponownie wykonać. Okoliczność ta rodzi obawę utraty źródła dowodowego albo możliwości jego przekształcenia, np. ze względu na upływ czasu, kiedy istnieje niebezpieczeństwo, że w przyszłości ich przeprowadzenie będzie niemożliwe albo bezcelowe[5]. Nadto istnieje niebezpieczeństwo, że – z uwagi na działania osób zainteresowanych lub czynników od człowieka niezależnych – mogą nastąpić zmiany nieodwracalne, które uczynią późniejszą czynność bezprzedmiotową[6]. Powyższa problematyka aktualizuje się w szczególności, kiedy za cel przeszukania organy śledcze obierają ujawnienie i zabezpieczenie nośników elektronicznych. Materiał ten cechuje bowiem nie tylko specyficzna forma, ale i łatwość modyfikacji poczynionych na nich zapisów. Może dokonać tego sprawca, a także zabezpieczający. Tymczasem warto pamiętać, iż nie samo zabezpieczenie sprzętu posiadającego pożądaną zawartość, a wykonana przez biegłego ekspertyza może nadać mu znaczenie środka dowodowego. Stąd też organy procesowe, realizujące czynność przeszukania, kompletują nośniki zawierające ślady cyfrowe ujawnione na miejscu czynności, celem przekazania do badań specjalistom, ekspertom, jak i biegłym z zakresu informatyki.

---

[3] Ustawa z dnia 6 czerwca 1997 roku Kodeks postępowania karnego, Dz. U. z 2018 roku poz. 1987 t.j.

[4] Konstytucja Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 roku Dz. U. z 1997 roku, nr 78, poz. 16 ze zm.

[5] S. Waltoś, *Istota i zakres uprawnień podejrzanego i pokrzywdzonego oraz ich zastępców w niepowtarzalnych czynnościach śledczych i dochodźczych*, „Palestra" 1969, nr 9, s. 10–11.

[6] T. Grzegorczyk, *Obrońca w postępowaniu przygotowawczym*, Łódź 1988, s. 189–190.

BIEGŁY Z ZAKRESU INFORMATYKI JAKO EKSPERT W POSTĘPOWANIU PRZYGOTOWAWCZYM

O doniosłości opinii biegłego eksperta w postępowaniu karnym napisano już wiele. Za T. Haunaskiem, podkreślającym w definicji wymiar kryminalistyczny tej instytucji, przywołać wypada, iż biegły, spełniając funkcję eksperta (wykonującego ekspertyzę), jest osobnym źródłem dowodowym. Cechuje go pełna samodzielność w doborze metod badawczych, w wykonywaniu czynności wchodzących w skład ekspertyzy, a także w sporządzeniu sprawozdania i wniosków[7]. Złożona do sprawy pisemna opinia biegłego z zakresu informatyki stanowi odkodowaną warstwę informacyjną materiału badawczego – śladu kryminalistycznego zabezpieczonego z wytypowanego nośnika. Dopiero sprowadzony do takiej postaci materiał może być zweryfikowany zgodnie z zasadami prawdy materialnej, obiektywności, bezstronności i uznany jako związany z przedmiotem postępowania przygotowawczego. Czynność ta stanowi niejako moment zwrotny w postępowaniu przygotowawczym, wieńcząc proces wykrywczy, w którym to jedynie uprawdopodobniano sprawstwo podejrzanego o popełnienie zarzucanego mu czynu, i daje podstawy do rozpoczęcia etapu udowadniania winy.

Warto zauważyć, iż w praktyce – począwszy od planowania realizacji czynności niepowtarzalnej do zabezpieczenia nośników – potrzeba powołania biegłego z zakresu informatyki – o ile w ogóle – aktualizuje się dopiero po dokonaniu protokolarnego zabezpieczenia nośników przez organy procesowe. Często też jawi się jako ostateczność.

Na taki stan rzeczy ma wpływ wiele czynników. Jednym z nich jest z pewnością możliwość zbadania nośników we wchodzących w skład Policji laboratoriach kryminalistycznych, które umożliwiają bieżące przejęcie materiałów do opiniowania. Ilość powierzonych tym komórkom ekspertyz i czasochłonność ich wykonania może jednak zachęcać organy do poszukiwania bliższych terminów realizacji opinii. Tym samym, zaangażowanie niezależnego biegłego z zakresu informatyki przyczynia się do uniknięcia długotrwałości postępowania, zapewniając szybsze uzyskanie wyniku analiz nośników. Nie sposób przy tym pominąć także aspektu finansowego wydania opinii przez biegłego z zakresu informatyki, będącego często zaporą dla niewielkich jednostek policji czy prokuratury. Wreszcie, na podjęcie decyzji o zaangażowaniu biegłego w badania nad zabezpieczonymi nośnikami ma wpływ wstępne ich sklasyfikowanie jako wymagających pogłębionej analizy, pracy przy zaawansowanej aparaturze bądź oprogramowaniu, na co składają się okoliczność zniszczenia nośnika, potrzeba odzyskania danych bądź wyodrębnienie określonego zakresu danych.

[7] T. Haunasek, *Kryminalistyka – zarys wykładu*, Kraków 2005, s. 167.

BIEGŁY Z ZAKRESU INFORMATYKI JAKO KONSULTANT W CZYNNOŚCIACH POSTĘPOWANIA PRZYGOTOWAWCZEGO

Szeroki wachlarz możliwych badań zabezpieczonych w toku przeszukania nośników i doniosłość informacji, które mogą ujawnić, potęguje obawy o nieprawidłowe zabezpieczenie sprzętu przez funkcjonariuszy realizujących czynność. Stopień zaawansowania ciągle aktualizującej się wiedzy informatycznej biegłego nie może być bowiem porównywany do zakładanej wiedzy funkcjonariuszy na temat standardów postępowania z dowodami cyfrowymi i dobrych praktyk. O ile zatem nośniki danych mogą być pozyskiwane i analizowane na każdym etapie postępowania w następstwie przyjętej wersji śledczej, o tyle wydaje się, iż warto, by pozyskiwanie materiału cyfrowego w toku czynności przeszukania pomieszczeń odbywało się z udziałem biegłego z zakresu informatyki, a sam tok ich zabezpieczania był z biegłym konsultowany. Należy przyjąć bowiem, iż czynność przeszukania stanowi z jednej strony etap, w którym pozyskuje się przyszłe dowody w postępowaniu karnym, z drugiej wstępną fazę postępowania, w której błędów technicznych można pełnić co niemiara, a możliwości późniejszego ich naprawienia są z reguły znikome lub żadne. Tymczasem stale rosnące znaczenie opinii biegłego z zakresu informatyki zmusza do tego, by materiał uzyskany w toku przeszukania, został zabezpieczony w sposób prawidłowy i umożliwiał jej sporządzenie. Los ujawnionego śladu bezsprzecznie zależy bowiem od jego prawidłowego zabezpieczenia[8].

Dynamiczny charakter czynności przeszukania jest wypadkową zespołu powiązanych działań o charakterze taktycznym, technicznym, procesowym, zmierzających do ujawnienia określonych nośników. Mimo iż przepisy Kodeksu postępowania karnego nie przewidują obowiązku planowania poszczególnych etapów postępowania, wydaje się, że czynności przeszukania winny znajdować odzwierciedlenie w sporządzanych przez funkcjonariuszy policji planach śledztw wieloczynowych o skomplikowanym stanie faktycznym[9]. Doniosłość czynności przeszukania uzasadniona obawą utraty źródła dowodowego sprawia, iż czynność procesowa winna być – w miarę możliwości – dokładnie zaplanowana. Wydaje się, że niezbędne jest odpowiednie rozeznanie, mające na celu wytypowanie używanych przez sprawców nośników, jak i określenie ich lokalizacji, co w toku postępowań z zakresu cyberprzestępczości nie jest zagadnieniem prostym. *Modus operandi* wysoko wykwalifikowanych sprawców polega bowiem przede wszystkim na mani-

[8] J. Jerzewska, *Od oględzin do opinii biegłego. Poradnik dla prowadzących postępowania karne*, wyd. 2, Warszawa 2005, s. 16.

[9] Zarządzenie nr 4 Komendanta Głównego Policji z dnia 9 lutego 2017 roku w sprawie niektórych form organizacji i ewidencji czyn. dochodzeniowo-śledczych Policji oraz przechowywania przez Policję dowodów rzeczowych uzyskanych w postępowaniu karnym, Dz. Urz. Komendy Głównej Policji z dnia 10 lutego 2017 roku, poz. 9.

pulacjach danymi, programem oraz urządzeniami peryferyjno-systemowymi[10]. Jak wskazuje J. Moszczyński, w miarę możliwości ważne jest wcześniejsze ustalenie:

1. informacji na temat sprzętu i środowiska komputerowego, które mają zostać poddane badaniu, tj. rodzaju komputerów, systemów operacyjnych, programów użytkowych, rodzajów pamięci, konfiguracji sieci, haseł dostępu itp.;

2. okoliczności, w jakich sprzęt będzie zabezpieczany podczas przeszukania – w obecności użytkowników sprzętu komputerowego lub pod ich nieobecność, w zależności od tego, czy będą dostępni administratorzy systemu itp.;

3. stanu aktywności systemów komputerowych (np. pracujące, wyłączone, w trakcie wykonywania backupu);

4. możliwość zdalnego usunięcia danych[11].

Trudno nie oprzeć się wrażeniu, iż o powodzeniu zabezpieczenia śladu z wytypowanego i ujawnionego nośnika decyduje szereg okoliczności związanych z technicznym aspektem planowania przeszukania. Bacząc na to, że sposób zabezpieczenia materiału rzutować będzie na możliwości badawcze biegłego z zakresu informatyki w toku sporządzania opinii, zasadna jest współpraca z ekspertem wskazanej specjalności już na etapie planowania przeszukania. Użytek z jego specjalistycznej wiedzy może pozwolić oszacować nie tylko ilość nośników możliwych do zajęcia na miejscu czynności, dostępne łącza, sieci, ale i metodykę przeszukania w zakresie systemów teleinformatycznych, tak by nie zdezorganizować pracy dużych podmiotów takich jak szpitale, urzędy, hotele. Wymiana informacji w powyższym zakresie z biegłym z zakresu informatyki może uchronić w toku czynności przeszukania od błędów, marnotrawstwa środków i czasu na bezcelowe czynności.

Wskazówki co do sposobu przeprowadzenia czynności wpisują się w akt konsultacji, definiowany jako zasięganie opinii u fachowców i specjalistów; udzielanie rad, wskazówek i wyjaśnień przez rzeczoznawców; porada[12]. Postać biegłego – konsultanta w kryminalistyce postrzegana jest jako osoba, biorąca udział w różnych czynnościach procesowych, jedynie w celu służenia radą i pomocą organowi procesowemu przeprowadzającemu te czynności. Podkreśla się, że pomoc taka potrzebna jest wówczas, gdy przeprowadzenie fragmentu tych czynności wymaga wiadomości specjalnych[13]. Biegły z zakresu informatyki może zatem pełnić rolę konsultanta już na etapie planowania realizacji czynności przez organy procesowe, udzielając porad oraz wskazówek co do sposobu realizacji zaplanowanej czynności.

---

[10] K. J. Pawelec, *Proces dowodzenia w postępowaniu karnym*, Warszawa 2010, s. 335.

[11] J. Moszczyński, *Informatyka kryminalistyczna*, [w:] *Kryminalistyka – czyli rzecz o metodach śledczych*, E. Gruza, M. Goc, J. Moszczyński, Warszawa 2008, s. 569–570.

[12] *Słownik języka polskiego*, M. Szymczak (red. nauk.), t. I, Warszawa 1993, s. 996.

[13] T. Hanausek, *Kryminalistyka…*, *op. cit.,* s. 167, por. także R. A. Stefański, [w:] *Kodeks Postępowania Karnego – Komentarz*, red. Z Gostyński, Warszawa 2003, t. I, s. 893.

Niezależnie od stopnia zaawansowania wiedzy realizujących czynność funkcjonariuszy, specyfika śladów cyfrowych potęguje przekonanie, iż sposób ich technicznego zabezpieczenia może rzutować na ograniczenie możliwości badawczych, a nawet uniemożliwić przeprowadzenie badań. Do ich cech szczególnych należą bowiem:

1) specyficzna forma, co implikuje trudności techniczne i prawne w gromadzeniu dowodów elektronicznych;

2) łatwość modyfikacji pojedynczych zapisów, łatwość manipulacji tymi dowodami, zmuszenie do stosowania odpowiednich instrumentów autentyfikacji zapisów. Należy jednak pamiętać, że ślady elektroniczne powstają nieraz równolegle w wielu różnych miejscach, co umożliwia ich weryfikację;

3) łatwość powielania, kopiowania. Właściwość ta uławia pracę organom ścigania i biegłym, którzy mogą tworzyć liczne kopie dowodu oraz badać je bez obawy utraty materiału dowodowego w wyniku pomyłki;

4) łatwość przechowywania;

5) powszechna opinia o ich nietrwałości;

6) potrzeba stosowania szczególnych środków technicznych do ich zabezpieczania i przechowywania[14].

Należy podkreślić, iż konieczność zapewnienia ochrony przed zniszczeniem śladów pojawia się nie od dostarczenia śladów do badań, a od momentu poprzedzającego ich zabezpieczenie. Zasadny zatem wydaje się postulat angażowania biegłego z zakresu informatyki w samą czynność przeszukania, szczególnie w przypadku spraw z zakresu cyberprzestępczości lub postępowań, gdzie ustalono mnogość nośników podlegających zabezpieczeniu. Biegły z zakresu informatyki może zatem pełnić rolę konsultanta, uczestnicząc w czynności przeszukania i dostarczając bieżącego wsparcia merytorycznego funkcjonariuszom realizującym czynności. Mimo otrzymanych wytycznych od biegłego na etapie planowania czynności przeszukania, nie sposób jest przewidzieć zastanych na miejscu realizacji czynności sytuacji. Zabezpieczenie śladów cyfrowych może okazać się nieefektywne, gdy zostaną zabezpieczone nieliczne bądź niewłaściwie. Zapobiec temu miałaby wiedza i doświadczenie obecnego podczas przeszukania biegłego.

Specyfika czynności jako niepowtarzalnej implikuje potrzebę wykorzystania trafnie wytypowanego miejsca realizacji przeszukania, celem nie tylko ujawnienia nośników spełniających kryteria przyjęte w postanowieniu o żądaniu wydania rzeczy i o przeszukaniu, ale także badania tej strefy wszelkimi dostępnymi instrumentami, co często przewyższa stopień zaawansowania wiedzy informatycznej i doświadczenia nadzorujących czynność i podległych im pracowników. Niekiedy także nieodzowna wydaje się być wstępna analiza nośników pod kątem przydatności dla postępowania, takich jak: pozorujące inne przedmioty nośniki pendrive,

[14] A. Lach, *Dowody elektroniczne w procesie karnym*, Toruń 2004, s. 32 i n.

komputery *all in one* czy aparatura do kopania kryptowalut[15]. Decyzja o zabezpieczeniu konkretnych materiałów, jak i selekcja nośników, może zatem często wykraczać poza rutynową wiedzę realizujących czynność funkcjonariuszy.

Tymczasem to właśnie biegły z zakresu informatyki dysponuje niejako wyobrażeniem co do przedmiotów spełniających różne funkcje cyfrowe, a także form przechowywania takich informacji. Jako uczestnik czynności prowadzonej przez organ procesowy, oprócz rad i wskazówek co do sposobu realizacji przeszukania, może na bieżąco interpretować uzyskiwane wyniki, opiniować kompletność nośników lub oceniać bezcelowość zabezpieczenia pewnych przedmiotów, np. tych ciężko uszkodzonych mechanicznie. Profesjonalne pozyskanie materiału przyczynia się także do zachowania łańcucha dowodowego, czyli zabezpieczenia i odzyskania materiału dowodowego tak, by nie wprowadzić zmian na urządzeniu.

Powyższe jest szczególnie istotne w przypadku zastanych na miejscu czynności włączonych nośników w trybie pracy. W tej sytuacji biegły z zakresu informatyki winien dokonać oceny, czy nie jest zainstalowane oprogramowanie szyfrujące, które po wyłączeniu komputera uniemożliwi deszyfryzację bez znajomości hasła. O ile bowiem czynność przeszukania przeprowadzana jest w celu ujawnienia nośników niezwiązanych z osobą podejrzanego, hasła można domagać się w toku czynności od użytkownika nośnika, który w postępowaniu będzie posiadać status świadka. Żądanie zaś podania hasła dostępu do zabezpieczonych w toku czynności nośników od osoby posiadającej status podejrzanego jawi się jako naruszenie zasady *nemo se ipsum accusare tenetur*[16]. Procesowa potrzeba zabezpieczenia nośników teleinformatycznych implikuje zatem swoisty układ współpracy organów ścigania z biegłym z zakresu informatyki.

Nadto od obecnego w toku przeszukania biegłego można oczekiwać znajomości wypracowanych przez środowiska eksperckie z zakresu informatyki dobrych praktyk. Niektóre z nich przewidują, by po odłączeniu jakiegokolwiek urządzenia, zwrócić uwagę, czy nie będzie konieczne zabezpieczenie danych ulotnych (pamięć RAM), np. w przypadkach związanych z infekcjami i kradzieżami z kont internetowych. Pozyskane w ten sposób informacje mogą być bezcenne w dalszym badaniu przez biegłego, gdzie zwyczajne wyłączenie komputera może trwale uniemożliwić

[15] Na dwuetapowy proces selekcji dowodów cyfrowych zwraca uwagę B. Hołyst, wyróżniając etap poznania hardware (komputer, dyski, telefony) oraz etap odróżnienia nieistotnych danych cyfrowych od tych, które mogą zawierać dowód w sprawie, por. B. Hołyst, *Kryminalistyka*, Warszawa 2018, s. 933.

[16] Odmienny pogląd przedstawia B. Hołyst: „Przeprowadzający przeszukanie ma prawo zażądać od dysponenta lub użytkownika urządzenia zawierającego dane informatyczne lub systemu informatycznego ujawnienia hasła lub haseł umożliwiających dostęp do urządzenia lub systemu nawet wówczas, gdy dysponentem lub użytkownikiem jest oskarżony, osoba najbliższa dla oskarżonego czy świadek mający prawo do uchylenia się od odpowiedzi na pytanie", B. Hołyst, *Kryminalistyka*…, *op.cit*., s. 187.

odnalezienie dowodów[17]. Warto przy tym wskazać, iż szczegółowe instrukcje do identyfikacji, gromadzenia, pozyskiwania i zachowania cyfrowych śladów dowodowych określają wytyczne Międzynarodowej Organizacji Normalizacyjnej o numerze PN-EN ISO/IEC 27037:2016-12, obejmujące powszechny standard pracy biegłych.

Należy nadmienić, iż zaangażowanie biegłego – konsultanta w czynności przeszukania nie musi ograniczać się jedynie do instruowania funkcjonariuszy, realizujących zabezpieczenie nośników. Trudno bowiem doszukać się przeszkód prawnych, które uniemożliwiałyby biegłym z zakresu informatyki czynne uczestnictwo w zabezpieczaniu materiału w miejscu przeszukania. Status biegłego determinuje bowiem m.in. dyspozycja aparaturą, przyrządami niezbędnymi do przeprowadzenia badań w ramach nie tylko zleconej mu ekspertyzy, ale i w procesie pozyskania materiałów do jej sporządzenia. Podkreślić jednak należy, iż w toku uczestnictwa biegłego w przeszukaniu, proces decyzyjny co do przebiegu czynności leży wyłącznie w gestii organu procesowego przeprowadzającego czynność. Czynność zabezpieczenia materiału przy wykorzystaniu specjalistycznej wiedzy i aparatury biegłego odbywa się zatem przy jego udziale, nie jest zaś czynnością przez biegłego prowadzoną. Trudno także dopatrzeć się przeszkód (innych niż finansowych) uniemożliwiających magazynowanie przez biegłego – konsultanta zabezpieczonych w toku przeszukania nośników do czasu rozpoczęcia wykonywania przez niego ekspertyzy bądź przez powołanego w tym celu innego biegłego.

DOKUMENTOWANIE UDZIAŁU BIEGŁEGO-KONSULTANTA W CZYNNOŚCIACH POSTĘPOWANIA PRZYGOTOWAWCZEGO

Udział biegłego w czynności przeszukania bądź planowania jej przebiegu należy procesowo udokumentować. Wydaje się, iż na tajnym etapie planowania czynności, niewystarczające będzie udokumentowanie powyższego notatką urzędową sporządzoną przez organ procesowy. Zaangażowanie biegłego z zakresu informatyki w etap konsultacji co do sposobu przeprowadzenia czynności przeszukania pomieszczeń, winno zostać poprzedzone postanowieniem prokuratora, wydanym w oparciu o art. 193§ 1 k.p.k., celem dopuszczenia do udziału w czynności. Taka decyzja procesowa nie tylko nada biegłemu status uczestnika postępowania karnego, ale i pozwoli na ewentualne dyscyplinowanie go poprzez przewidziane w kodeksie postępowania karnego środki przymusu, np. w sytuacji niestawiennictwa biegłego na kolejny etap konsultacji. Wydaje się także, iż wyniki czynności, które toczyły się według porad i wskazówek biegłego w zakresie sposobu przeszukania pomieszczeń,

[17] P. Krejza, *Najlepsze praktyki w poszukiwaniu i zabezpieczaniu dowodów elektronicznych,* [w:] *Elementy informatyki sądowej*, M. Szmit (red.), Warszawa 2011, s. 48.

mogą przyczynić się do dodatkowych ustaleń w postępowaniu, wobec czego może wyniknąć potrzeba przesłuchania go w trybie art. 183 k.p.k.

Udokumentowanie obecności biegłego podczas samej realizacji czynności przeszukania wynika wprost z art. 143§ 1 pkt 6 k.p.k. oraz art. 148§ 1 k.p.k. Obecność ta winna zatem znaleźć odzwierciedlenie w protokole przeszukania, dokumentującym czynność, w którym biegły figuruje jako osoba uczestnicząca w czynności.

PODSUMOWANIE

Rola biegłego z zakresu informatyki w toku czynności postępowania przygotowawczego jawi się jako niezmiernie doniosła. Ma on bowiem szczególną pozycję w procesie ujawnienia okoliczności dokumentujących *modus operandi* sprawców, co przyczynia się do osiągnięcia głównego celu procesu – wykrycia prawdy materialnej. Stąd też ujawnianie, pozyskanie i zabezpieczenie nośników zawierających ślady cyfrowe, jak i planowanie zaawansowanych czynności w tym zakresie, w miarę możliwości, winno odbywać się przy udziale konsultanta – biegłego z zakresu informatyki. Konstatacja ta wynika zarówno ze specyfiki niepowtarzalnej czynności, jaką jest przeszukanie, jak i charakterystyki zastanych na miejscu czynności śladów cyfrowych. Wiedza i doświadczenie biegłego wykorzystane już na wstępnym etapie postępowania przygotowawczego nie tylko zwiększy prawdopodobieństwo należytego zabezpieczenia tychże śladów, ale i przyczyni się do dostarczenia cennego i rzetelnego materiału do późniejszego sporządzenia wartościowej opinii. Zakres informatycznej wiedzy i doświadczenia biegłego może być zatem wykorzystywany przez organy procesowe nie tylko w ekspertyzach i opiniach, ale także w toku ujawniania i pozyskiwania materiału do ich sporządzenia.

Niestety, wydaje się, iż organy ścigania nie zawsze będą mogły z powodzeniem wdrożyć postulat zaangażowania biegłego do realizacji czynności przeszukania bądź konsultacji w tym zakresie.

Decydując na początkowym etapie śledztwa lub dochodzenia o czynnościach realizacyjnych, organy procesowe niekiedy nie mają wyobrażenia o skali bądź rzeczywistym przedmiocie przestępczego procederu. Przyjęte wersje śledcze niekiedy zwyczajnie nie zakładają potrzeby angażu biegłego z zakresu informatyki. Jako przykład posłużyć może treść komunikatów medialnych z września 2018 roku, donosząca o zrealizowaniu przeszukania w fabryce amfetaminy, gdzie organy ścigania jednocześnie ujawniły kopalnię kryptowalut[18]. Odkrycie to z pewnością dostarczyło kolejnych kierunków prowadzenia postępowania, w tym m.in. weryfi-

[18] MaG, *W fabryce amfetaminy policja odkryła „fabrykę bitcoinów"*, https://wiadomosci.radiozet.pl/Polska/Mazowieckie.-Policja-odkryla-fabryke-narkotykow-i-kopalnie-bitcoinow, dostęp:25 lutego 2019.

kacji wątku lokowania środków pochodzących z przestępstwa w waluty wirtualne. Powyższe obrazuje z jednej strony doniosłość śladów cyfrowych i ich wpływu na bieg postępowania, z drugiej zaś nieprzewidywalność współczesnej przestępczości.

Przeszkodą w ścisłej współpracy z biegłym może okazać się także aspekt finansowy. Zważyć należy, iż wynagrodzenie za udział biegłego w czynności bądź konsultacji nie obejmuje przyszłych kosztów udzielenia opinii.

W końcu, w kategorii spraw złożonych podmiotowo, np. z zakresu przestępczości zorganizowanej, czynności przeszukania realizowane są niekiedy w wielu lokalizacjach jednocześnie. Sprostanie wymogowi zapewnienia jednolitości składu zespołu realizującego czynność oraz wzbogacenie go o eksperckie informatyczne wsparcie stanowiłaby nie lada logistyczne wyzwanie dla organów planujących takie przeszukania. Warto wspomnieć także o aspektach finansowych takiego procesowego przedsięwzięcia, bowiem niezależnie od jednostki, która realizuje zlecone przeszukania, koszty udziału biegłego ponosi powołujący go, a zatem jednostka prowadząca postępowanie[19].

BIBLIOGRAFIA

Carvey H., *Windows Forensic Analysis*, USA 2007.
Grzegorczyk T., *Obrońca w postępowaniu przygotowawczym*, Łódź 1988.
Haunasek T., *Kryminalistyka – zarys wykładu*, Kraków 2005.
Hołyst B., *Kryminalistyka*, Warszawa 2018.
Jerzewska J., *Od oględzin do opinii biegłego. Poradnik dla prowadzących postępowania karne*, wyd. 2, Warszawa 2005.
Kasprzak W. A., *Ślady cyfrowe. Studium prawno-kryminalistyczne*, Warszawa 2015.
Krejza P., *Najlepsze praktyki w poszukiwaniu i zabezpieczaniu dowodów elektronicznych*, [w:] *Elementy informatyki sądowej*, M. Szmit (red.), Warszawa 2011.
Konstytucja Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 roku, Dz. U. z 1997 roku, nr 78, poz. 16 ze zm.
Lach A., *Dowody elektroniczne w procesie karnym*, Toruń 2004.
MaG, *W fabryce amfetaminy policja odkryła „fabrykę bitcoinów"*, https://wiadomosci.radiozet.pl/Polska/ Mazowieckie.-Policja-odkryla-fabryke-narkotykow-i-kopalnie-bitcoinow, dostęp: 25 lutego 2019 roku.
Moszczyński J., *Informatyka kryminalistyczna*, [w:] *Kryminalistyka – czyli rzecz o metodach śledczych*, Gruza E., Goc M., Moszczyński J., Warszawa 2008.
Pawelec K. J., *Proces dowodzenia w postępowaniu karnym*, Warszawa 2010.
Porozumienie między Prokuratorem Generalnym, a Komendantem Głównym Policji w sprawie Zasad ponoszenia przez Prokuraturę i Policję wydatków w postępowaniu przygotowawczym z dnia 19 stycznia 2000 roku.

[19] Porozumienie między Prokuratorem Generalnym, a Komendantem Głównym Policji w sprawie Zasad ponoszenia przez Prokuraturę i Policję wydatków w postępowaniu przygotowawczym z dnia 19 stycznia 2000 roku.

Stefański R. A., [w:] *Kodeks Postępowania Karnego. Komentarz*, t. I, red. Z. Gostyński, Warszawa 2003.
Szymczak M. (red. nauk.), *Słownik języka polskiego*, t. I, Warszawa 1993.
Ustawa z dnia 6 czerwca 1997 roku Kodeks postępowania karnego, Dz. U. z 2018 roku, poz. 1987 t.j.
Waltoś S., *Istota i zakres uprawnień podejrzanego i pokrzywdzonego oraz ich zastępców w niepowtarzalnych czynnościach śledczych i dochodźczych*, „Palestra" 1969, nr 9.
Zarządzenie nr 4 Komendanta Głównego Policji z dnia 09 lutego 2017 roku w sprawie niektórych form organizacji i ewidencji czynności dochodzeniowo-śledczych Policji oraz przechowywania przez Policję dowodów rzeczowych uzyskanych w postępowaniu karnym, Dz. Urz. Komendy Głównej Policji z dnia 10 lutego 2017 roku, poz. 9.

ABSTRAKT

Artykuł stanowi próbę wykazania doniosłości roli biegłego z zakresu informatyki jako konsultanta w czynności przeszukania pomieszczeń. Autorka wysuwa postulat wykorzystywania eksperckiej wiedzy biegłego już na wstępnym etapie postępowania przygotowawczego w toku ujawniania i zabezpieczania śladów cyfrowych. W opracowaniu pokrótce scharakteryzowano instytucję przeszukania jako czynności niepowtarzalnej w kontekście specyfiki śladów cyfrowych, będących przyszłymi dowodami elektronicznymi. Przedstawiono także główne aspekty współpracy organów ścigania z biegłym z zakresu informatyki i podjęto próbę wskazania przyczyn niedostatecznego stopnia angażowania biegłego wskazanej specjalności na początkowym etapie postępowania karnego.

Słowa klucze: biegły, konsultant, informatyka śledcza, przeszukanie, ślady cyfrowe.