Wojciech Sobala

Informatyczne dowody rzeczowe w postępowaniach karnych

Palestra 48/5-6(545-546), 48-54

2003

Wojciech Sobala

INFORMATYCZNE DOWODY RZECZOWE W POSTĘPOWANIACH KARNYCH

Następuje obecnie gwałtowny rozwój informatyzacji naszego życia. Z dnia na dzień wzrasta ilość sprzętu komputerowego zarówno w firmach, urzędach, uczelniach, szkołach i w domach u osób prywatnych. Użytkujemy coraz szybsze komputery, powszechnie korzystamy z poczty elektronicznej i przeglądamy światowe zasoby stron WWW, coraz częściej w sklepach płacimy kartami płatniczymi, a życzenia imieninowe zamiast na kartkach pocztowych składamy wysyłając sms'y. Skutkiem tych zmian jest również dynamiczny rozwój sieci teleinformatycznych.

Wraz z erą komputeryzacji systemy informatyczne i sprzęt służący przetwarzaniu danych stają się coraz częściej zarówno przedmiotem jak i narzędziem działań przestępczych. Komputer może być przedmiotem przestępstwa np. kradzieży, ale również może służyć jako narzędzie dla sprawców czynów zabronionych do fałszowania dokumentów czy środków płatniczych, piractwa programów komputerowych, stosowania groźby karalnej, zniesławienia, szpiegostwa, propagowania faszyzmu, rozpowszechniania pornografii z udziałem nieletnich, sprowadzenia niebezpieczeństwa powszechnego, sabotażu komputerowego itp.

W celu zobrazowania skali zagrożeń przestępstw z użyciem komputerów można wskazać za literaturą przedmiotu następujące dane FBI, zgodnie z którymi w USA „tradycyjny" napad na bank powoduje średnie straty około 8 tys. USD, podczas gdy przeciętna kradzież informacji (np. numerów kart kredytowych) z bankowego systemu komputerowego już 100 tys. USD, natomiast oszustwo komputerowe aż 500 tys. USD.

Uwzględniając powyższe informacje należy stwierdzić, iż dla organów ścigania coraz większego znaczenia nabierać będą w najbliższym czasie dowody działalności przestępczej, które można ujawnić i następnie zabezpieczyć w systemach teleinformatycznych oraz wszelkich innych urządzeniach służących przetwarzaniu danych.

Dowód w postępowaniu karnym to każdy dopuszczalny przez prawo środek służący dokonaniu określonych ustaleń, czyli służący ustaleniu okoliczności mających znaczenie dla rozstrzygnięcia. Obowiązujący obecnie z 1997 roku kodeks postępowania karnego przez określenie „dowód" rozumie zarówno wyjaśnienia oskarżonego, zeznania świadków, samą osobę świadka i biegłego, otwarcie zwłok, oględzi-

ny, czynność przesłuchania, ciało ludzkie, jak również okazanie i konfrontację. Zawsze jest to jednak środek służący dokonaniu prawdziwych ustaleń faktycznych[1]. Mówiąc o informatycznych dowodach rzeczowych należy wspomnieć treść art. 115 § 14 kodeksu karnego, zgodnie z którym dokumentem jest nie tylko każdy przedmiot, ale również zapis na komputerowym nośniku informacji, z którym jest związane określone prawo, albo który ze względu na zawartą w nim treść stanowi dowód prawa, stosunku prawnego lub okoliczności mającej znaczenie prawne.

Dowodami rzeczowymi znajdującymi się w systemach informatycznych oraz w urządzeniach służących przetwarzaniu danych, stanowiącymi źródło wiedzy w zakresie rozstrzygnięcia postępowania karnego, mogą być:

- dokumenty elektroniczne,
- poczta elektroniczna,
- logi systemowe,
- informacje identyfikujące komputer,
- dane bilingowe,
- system kontroli dostępu,
- system telewizji użytkowej CCTV,
- elektroniczne systemy alarmowe.

Dowodami rzeczowymi mogą być znajdujące się w systemach informatycznych lub przechowywane na nośnikach magnetycznych **dokumenty elektroniczne**. Dokumentem elektronicznym jest informacja zapisana na nośniku elektronicznym (np. dyskietce, dysku twardym, krążku CD-ROM, karcie elektronicznej, taśmie magnetycznej itp.), który umożliwia jej zapis, przechowywanie oraz odczyt przy zastosowaniu technologii informatycznych. Dokumentami są efekty pracy programów jak na przykład materiały stworzone w edytorze tekstu czy pliki tabulogramów. Wszystkie one mogą być źródłem określonych informacji. Należy ich szukać nie tylko w określonych plikach, ale także w ich poprzednich wersjach, plikach tymczasowych, ukrytych i skasowanych. W tym miejscu należy wspomnieć, iż zgodnie z informacjami podawanymi przez firmy zajmujące się odzyskiwaniem utraconych danych informacje można odzyskać w około 90% w przypadku awarii elektroniki i około 63% w przypadku uszkodzenia fizycznego nośnika. Należy mieć zatem świadomość, że zarówno plik wyglądający początkowo jako uszkodzony, lub niezawierający zapisanych żadnych danych nośnik może stać się źródłem niezastąpionych wiadomości. Dokumentów elektronicznych należy również poszukiwać w kopiach archiwalnych, które wykonywane są przez administratorów na wypadek wszelkich nieprzewidzianych okoliczności jakie mogą się pojawić, tj. awarii sprzętu, błędów oprogramowania czy użytkowników, włamania do systemu, pożaru, zalania wodą, kradzieży serwera, eksplozji ładunku wybuchowego, ataku terrorystycznego itp. Celem wykonywania archiwizacji jest zabezpieczenie danych i przy-

[1] T. Grzegorczyk, *Dowody w procesie karnym*, Warszawa 1998, s. 3.

wrócenie pracy systemu. Ze względów bezpieczeństwa kopie zapasowe przechowywane są z reguły daleko od miejsc przetwarzania, często w specjalnych szafach na nośniki magnetyczne, które odporne są na bardzo wysoką temperaturę, zalanie wodą, reakcję związków chemicznych oraz zabezpieczają je przed dostępem osób niepowołanych. Z tego powodu zarchiwizowane dane mogą posłużyć porównaniom aktualnego stanu systemu z zapisaną wcześniej kopią, odnalezieniu poprzednich wersji dokumentów sporządzonych przez użytkowników czy poczty elektronicznej znajdującej się na serwerze pocztowym w określonym przez nas dniu.

Poczta elektroniczna to forma przekazu umożliwiająca przesyłanie informacji w postaci listów elektronicznych, które można zobaczyć na ekranie komputera lub wydrukować. Poczta internetowa jest chyba najczęściej używaną usługą wśród użytkowników Globalnej Sieci Informatycznej (Internetu) i jest podstawowym sposobem wymiany informacji w sieciach komputerowych. Oprócz przekazywania tekstu może służyć do przesyłania załączników. Załącznikami listów mogą być pliki o dowolnej treści, np. dokumenty edytorów tekstu i arkuszy kalkulacyjnych, pliki graficzne, muzyczne, video itp. Listów elektronicznych należy szukać w programach pocztowych komputerów użytkowników lub na serwerach pocztowych, na których listy e-mail znajdują się do czasu ich odebrania przez adresata. W określonych sytuacjach także adres poczty elektronicznej może stanowić źródło wiedzy dla prowadzonego przez organy ścigania postępowania przyczyniające się identyfikacji nadawcy lub odbiorcy. Należy jednak wspomnieć, iż możliwe jest podszywanie się osób trzecich pod użytkownika elektronicznego przekazu wiadomości.

Logi systemowe to najczęściej pliki tekstowe, w których zapisywane są wiersz po wierszu przez system operacyjny określone wydarzenia. Tworzą one historię pracy systemu. Mogą stanowić źródło informacji o pomyślnych i nieudanych próbach wejścia do systemu, zalogowanych użytkownikach z adresem ich komputera i przebiegiem oraz czasem ich pracy, przeprowadzonych połączeniach modemowych, uruchomionych programach, dostępie użytkowników do poszczególnych katalogów i plików itp. Z plików rejestrujących możemy dowiedzieć się również o stronach WWW na jakie zaglądali użytkownicy, jakie pliki ściągali i wysyłali. Interpretacja informacji zawartych w logach ma na celu nie tylko uzyskanie wiedzy na temat nieupoważnionych użytkowników, ale także służy do identyfikacji występujących błędów oraz monitorowania pracy systemu. Połączenie informacji z różnych plików rejestrów jest z pewnością dobrym źródłem wiedzy o pracy systemu. Pamiętać jednak należy, że logi systemowe podatne są na zmiany, podmianę oraz skasowanie. Analizując je należy zwrócić zatem szczególną uwagę na to czy są spójne, czy nie ma w nich „dziur czasowych" oraz innych symptomów mogących wskazywać na ich nieautoryzowaną modyfikację. Jednym z najprostszych i zarazem najbardziej skutecznych mechanizmów zabezpieczających omawiane pliki jest ich dodatkowa archiwizacja na innym serwerze. Sprawdzić

należy zatem, czy taki sposób zabezpieczenia logów był stosowany i ewentualnie poddać go również analizie.

Identyfikacja komputera. Każdy komputer w sieci Internet ma przypisany niepowtarzalny, w danej chwili, adres IP (ang. Internet Protocol address) w postaci czterech 8-bitowych liczb przybierających wartość od 0 do 255 oddzielonych kropkami. Przykładowo 193.59.104.11 jest adresem strony głównej Sejmu RP. Należy traktować taki adres jak numer telefonu, którego znajomość pozwala na nawiązanie połączenia z innym komputerem i wymianę danych.

Każdy z czterech członów adresu IP oznacza co innego i pozwala na zakreślenie coraz to mniejszego obszaru w którym można poszukiwać danego urządzenia. Poprzez jeden człon odnajdziemy określoną sieć, poprzez następny odnajdziemy mniejszą sieć i tak do konkretnego komputera. Pulę (zakresy) adresów IP tworzą tzw. klasy, które są przydzielane firmom będącym dostarczycielami połączeń internetowych. Ze względu na swą unikalność – adres IP w połączeniu z dokładnym określeniem czasu – jednoznacznie identyfikuje urządzenie w sieci Internet oraz firmę, z której puli pochodzi. Określenie czasu jest szczególnie istotne tam, gdzie dany użytkownik łączy się z Internetem za pomocą modemu telefonicznego lub otrzymuje dynamiczny adres IP, tzn. pierwszy wolny w danej chwili z określonego zakresu. Przy połączeniach modemowych sygnał z informacjami przesyłany jest, z grubsza biorąc, za pomocą tych samych urządzeń co rozmowa telefoniczna. Za każdym razem gdy posiadacz modemu chce połączyć się z Internetem, operator sieci telefonicznej przydziela mu numer IP. Jest to numer który nie jest przypisany raz na zawsze jakiemuś użytkownikowi, tylko jak np. samochód z wypożyczalni, oddawany jest danej osobie na czas bytności w sieci. W takiej sytuacji, aby określić jaki komputer korzystał z danego adresu IP, należy sprecyzować datę i godzinę. Tym samym wszelka aktywność danego komputera w sieci, będzie związana z jego adresem IP. Dokonuje się tego za pomocą *bilingu*, wykazującego jaki numer i kiedy łączył się z numerem umożliwiającym wejście do Internetu[2]. W Internecie dostępnych jest jednak wiele publikacji poświęconych podszywaniu opartym na fałszowaniu adresu IP.

Dane bilingowe zawierają informacje o numerze stacji abonenta, adresie abonenta, liczbie jednostek taryfikacyjnych zaliczonych na rzecz danej stacji w przyjętym okresie rozliczeniowym, numerach z którymi abonent uzyskał połączenie, dacie uzyskania i czasie trwania połączenia oraz o jego rodzaju (międzynarodowe, krajowe, lokalne, Internet). Operator jest zobowiązany do rejestracji danych o wykonanych usługach telekomunikacyjnych, w zakresie umożliwiającym ustalenie należności za wykonanie tych usług oraz rozpatrzenie reklamacji i przechowywania

[2] M. Kliś, A. Stella-Sawicki: http://www.vagla.pl/skrypts/dowody_cyfrowe.htm, Listopad 2001.

ich przez okres co najmniej 12 miesięcy, a w przypadku wniesienia reklamacji przez okres niezbędny do rozstrzygnięcia sporu[3].

Systemy kontroli dostępu do pomieszczeń to wyspecjalizowane urządzenia identyfikująco-sterujące, współpracujące z różnego rodzaju urządzeniami identyfikacyjnymi (np. manipulatorami szyfrowymi, czytnikami kart magnetycznych, zbliżeniowych, punktów siatkówki oka, odcisku palca czy dłoni, porównujące cechy głosu) oraz urządzeniami wykonawczymi (np. blokadami magnetycznymi, ryglami i zworami umożliwiającymi otwarcie drzwi, urządzeniami ograniczającymi dostęp do określonych urządzeń i elementów takich jak komputery, drukarki przemysłowe, kserokopiarki, specjalistyczne oprogramowanie). Systemy kontroli dostępu pozwalają na ograniczanie i kontrolowanie dostępu do całych obiektów, stref, poszczególnych pomieszczeń oraz zasobów. W zależności od rodzaju urządzeń identyfikacyjnych system kontroli dostępu może dostarczać nam różne informacje. W przypadku użytkowania czytników bazujących na porównywaniu punktów siatkówki oka (obraz źrenicy oka stabilizuje się w około 3 roku życia i jest niezmienny do około 10 sekund po ustaniu czynności życiowych), lub odcisków linii papilarnych identyfikacja taka będzie niezaprzeczalna. W sytuacjach stosowania na przykład czytników kart zbliżeniowych uzyskamy informacje o numerach użytych kart, które posłużyły do pokonania blokady w interesującym nas przedziale czasowym. Omawiając informacje rejestrowane przez systemy kontroli dostępu wspomnieć należy o dostępnych na naszym rynku zamkach elektronicznych. Zamki tego typu posiadają wbudowaną pamięć rejestrującą datę, czas i identyfikator zdefiniowanego użytkownika, który dokonuje otwarcia lub zamknięcia zamka. Posiadają one swoje źródło zasilania i mogą posiadać informacje do kilku tysięcy otwarć i zamknięć zamka.

Systemy telewizji użytkowej CCTV służą do obserwacji oraz rejestracji wybranych stref chronionego obiektu oraz często jego otoczenia. Dynamiczny rozwój technik przetwarzania i przekazu obrazu sprawia, iż cyfrowe systemy telewizji użytkowej wypierają urządzenia analogowe. Spotykamy się obecnie również z systemami, które łączą w sobie zapis cyfrowy i analogiczny. W systemach tego typu bieżący obraz rejestrowany jest na kasetach analogowych, jednak w przypadku wystąpienia jakiegokolwiek sygnału alarmowego aktualny obraz w postaci cyfrowej wraz z kilkuminutową „historią" poprzedzającą wystąpienia sygnału alarmowego wysyłany jest na przykład do centrum monitoringu i tam również zapisywany. Materiał rejestrowany systemami nadzoru telewizyjnego ma duże znaczenie jako materiał dokumetnacyjny nie tylko dla użytkowników, ale również może być wykorzystywany przez organy ścigania.

[3] A. Lach, *Dowody elektroniczne. Pojęcia i klasyfikacja*, Security Magazine nr 4 (kwiecień 2001), s. 24.

Elektroniczne systemy alarmowe to urządzenia służące sygnalizacji zagrożenia chronionych dóbr czyli osób (bezpieczeństwo życia, zdrowia i nietykalności osobistej), lub mienia (działania zapobiegające powstaniu szkody wskutek przestępstw i wykroczeń przeciwko mieniu), ewentualnie jednocześnie osób i mienia. Urządzenia rejestrujące systemów alarmowych służą do zapisu zdarzeń związanych z pracą systemu alarmowego z podaniem daty i czasu, tj. alarmu, awarii oraz okresowych wyłączeń systemu. Występujące zdarzenia mogą być uwidaczniane na bieżąco na ekranie monitora, tablicach, sygnalizatorach i manipulatorach, ale równocześnie zapisywane są na wydruku lub w pamięci komputera. Podobnie jak obraz z systemu telewizji cyfrowej informacje zapisywane przez systemy alarmowe mogą być przesyłane w inne miejsce i tam również archiwizowane.

Przedstawiając źródła informacji, które mogą być wykorzystane w postępowaniach karnych nie możemy zapomnieć o samym miejscu, gdzie użytkowany jest sprzęt informatyczny lub urządzenia przetwarzające dane, a służące do dokonywania przestępstw. Wartość dowodową może mieć coś, co akurat znajduje się na monitorze komputera i co w celu udokumentowania należy sfilmować lub sfotografować. Okazać może się również iż wartość dowodową mają książki, papiery i notatki, instrukcje obsługi sprzętu oraz programów, zapisane gdzieś na kartkach hasła znajdujące się pod biurkami, stołami, krzesłami, wewnątrz instrukcji i książek, lub informacje zapisane w pamięci telefonów, faksów i modemów itp.

Omawiając przykładowe źródła informacji, które mogą być wykorzystane jako dowody w prowadzonych postępowaniach należy zwrócić szczególną uwagę, iż są to jedynie elektroniczne zapisy informacji. Uwzględniając zatem łatwą możliwość zmian i zniszczenia zapisów w pamięci komputera czy na nośnikach magnetycznych należy przy badaniu informatycznych materiałów dowodowych przyjąć zasadę „po pierwsze nie szkodzić". Zgodnie z tą zasadą:

- nigdy nie należy robić czegoś, co mogłoby spowodować usunięcie lub zapisanie innych danych na nośniku,
- zawsze dokumentować wykonywane czynności,
- zawsze pracować przy badaniu materiału źródłowego na kopii.

Przyjęcie takich zasad postępowania powinno zapewnić wiarygodność oraz autentyczność zabezpieczonych dowodów, a także zagwarantować bezpieczeństwo przed ich uszkodzeniem lub utratą. Ujawniając i zabezpieczając elektroniczne dowody rzeczowe należy zwrócić wyjątkową uwagę na sposób oraz okoliczności w jakich zostały one stworzone, przechowywane, ujawnione, a następnie zabezpieczone. Należy bowiem w trakcie prowadzonych czynności jednoznacznie wykluczyć sytuację, że zostały one zmienione lub podmienione.

Mówiąc o dokumentach elektronicznych i informatycznych dowodach rzeczowych należy wspomnieć, że elektroniczny zapis informacji nie jest rzeczą i nie posiada atrybutu przedmiotu. Jednak w przypadku przechowywania w systemie lub

na nośniku magnetycznym jest on z takim przedmiotem (nośnikiem danych) nierozerwalnie związany. Ze względu na cel czynności procesowych nośniki danych będące przedmiotem czynności powinny być poddane oględzinom, w szczególności pod kątem wartości dowodowej utrwalonego zapisu. Z procesowego punktu widzenia informacja zapisana tuszem na papierze nie różni się niczym od zapisu elektromagnetycznego na nośniku. Przyjmuje się zatem, że do elektronicznego zapisu informacji mają zastosowanie w drodze analogii przepisy o przeszukaniu i zatrzymaniu pism, dokumentów, notatek itp.[4].

Reasumując stwierdzić należy, iż rozwój technologii komputerowej coraz częściej wymuszać będzie po sięganie przez organy ścigania do dowodów rzeczowych znajdujących się w systemach informatycznych oraz urządzeniach służących przetwarzaniu danych. Jednocześnie pamiętać należy, że sprzęt informatyczny oraz tworzone systemy stają się coraz bardziej skomplikowane i zawierają coraz więcej informacji, które mogą zostać wykorzystane nie tylko przez organy ścigania, ale także przez osoby zajmujące się bezpieczeństwem informatycznym.

[4] A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 199.