CBKE
e-BIULETYN

Dowody cyfrowe w postępowaniu karnym, wybrane zagadnienia praktyczne i teoretyczne

dr Arkadiusz Lach

Katedra Postępowania Karnego UMK w Toruniu

1. Wprowadzenie

Postępująca informatyzacja naszego życia znajduje też odzwierciedlenie w procesie karnym. Z jednej strony umożliwia nam ona przyspieszenie postępowania poprzez użycie np. nowoczesnych technik utrwalania czynności procesowych (np. nagrania przesłuchań) i ich przeprowadzania (np. przesłuchania świadka w drodze videokonferencji), z drugiej jednak przysparza nowych problemów. Jednym z nich jest bez wątpienia zagadnienie wykorzystania elektronicznych śladów przestępstw określanych między innymi mianem dowodów cyfrowych[1].

2. Pojęcie dowodu cyfrowego

Nie wdając się głębiej w kwestie terminologii[2], proponuję w niniejszym opracowaniu oprzeć się o definicję przyjętą przez Międzynarodową Organizację do spraw Dowodów Komputerowych (International Organization on Computer Evidence - IOCE). Zakłada ona, że dowodem takim jest „informacja przechowywana lub transmitowana w formie binarnej, która może mieć znaczenie w postępowaniu sądowym" (*information stored or transmitted in binary form that may be relied upon in court*)[3]. Oczywiście trzeba w tym miejscu zaznaczyć, że dowody cyfrowe będą mogły być wykorzystane równie dobrze na etapie czynności poprzedzających postępowanie sądowe, w tym zwłaszcza w postępowaniu przygotowawczym.

[1] Często też operuje się pojęciem „dowody elektroniczne" czy „dowody komputerowe".
[2] Szerzej na temat A. Lach, *Informacja w formie elektronicznej jako dowód w procesie karnym*, Toruń 2003 (nie publikowana rozprawa doktorska), s. 23 – 25.
[3] Zob. International Organization on Computer Evidence, *G 8 Proposed Principles For The Procedures Relating To Digital Evidence*, www.ioce.org/G8_proposed_principles_for_forensic_evidence.html.

3. Podział dowodów cyfrowych

W literaturze zostało dokonanych wiele prób uszeregowania dowodów cyfrowych. W zależności od systemu prawnego różne kryteria mogą tu mieć kluczowy charakter. Jak się jednak wydaje, zasadniczy podział przedstawia się następująco[4]:

a. dowody uzyskiwane w czasie rzeczywistym i w fazie przechowywania w systemie lub na nośnikach,

b. właściwe (typowe) dowody rzeczowe i dokumenty.

Pierwszy z podziałów wiąże się z metodami uzyskiwania dowodów cyfrowych. Ich uzyskiwanie w czasie rzeczywistym odbywa się drogą podsłuchu lub gromadzenia danych związanych z ruchem (*traffic data*). W tym pierwszym przypadku obostrzenia procesowe co do stosowania środków przymusu procesowego[5] są większe niż podczas uzyskiwania danych, które są przechowywane w systemie lub zostały zapisane na nośniku. Trzeba jednak zasygnalizować, że wielokrotnie określenie, z którą metodą mamy do czynienia może nastręczać trudności. Tak będzie zwłaszcza w przypadku wiadomości *e – mail*. W niektórych systemach ich przesyłanie może być traktowane w sposób zbliżony do rozmowy telefonicznej, w innych zaś do przesyłania tradycyjnej poczty[6]. Pojawi się więc problem, czy w konkretnym przypadku należy stosować podsłuch, czy też np. zażądać wydania przesyłki.

Podział dowodów na rzeczowe i dokumenty ma największe znaczenie w państwach anglosaskich. Zostanie on omówiony w następnym punkcie. W tym miejscu należy jedynie zasygnalizować, że w polskim procesie karnym dokumenty są często uznawane za szczególną formę dowodów rzeczowych, natomiast w krajach anglosaskich *real evidence* i *documentary evidence* są sobie przeciwstawiane.

4. Główne problemy prawne związane z uzyskiwaniem dowodów cyfrowych

Proces uzyskiwania dowodów cyfrowych nasuwa szereg trudności, które różnią się pod względem wagi w poszczególnych systemach prawnych[7]. Należy tu wymienić przede wszystkim:

a. Możliwość i zakres stosowania podsłuchu treści przesyłanej informacji

Zarówno w krajach *common law* jak i *civil law* stosowanie podsłuchu jest zasadniczo dopuszczalne[8]. Odmienności występują tu jednak co do zakresu przedmiotowego, czyli co do jakich

[4] Por. A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 192 oraz A. Lach, *Informacja...*,s. 31 – 32.
[5] Pojęcia środka przymusu nie można utożsamiać ze stosowaniem siły fizycznej do wyegzekwowania obowiązków procesowych. Za środki takie należy uznawać, nieco upraszczając sprawę, przewidziane przez prawo procesowe ograniczenia praw obywatelskich, których niewykonanie może powodować użycie siły fizycznej, sankcji wymuszających (np. areszt) lub nałożenie kary.
[6] Szerzej rozważa ten problem M. C. Berton, *Home Is Where Your Modem Is. An Appropriate Application Of Search And Seizure Law to Electronic Mail*, American Criminal Law Review, vol. 34/1996, s. 182 i nast.
[7] Na temat problemów występujących na gruncie prawa polskiego zob. np. A. Adamski, *Prawo...*, s. 192 – 217 oraz A. Lach, *Gromadzenie dowodów elektronicznych po nowelizacji kodeksu postępowania karnego*, Prokuratura i Prawo, nr 10/2003, s. 16 – 25.

przestępstw podsłuch może być użyty i organu uprawnionego do jego stosowania. Nie negując konieczności ograniczenia przedmiotowego zakresu podsłuchu do przestępstw najpoważniejszych, należy równocześnie zrewidować ich katalog tak, aby zostały uwzględnione niektóre przynajmniej przestępstwa komputerowe. Celowe wydaje się też umieszczenie w regulacjach dotyczących podsłuchu tzw. klauzuli subsydiarności, dopuszczającej stosowanie podsłuchu jedynie wtedy, kiedy uzyskanie dowodów innymi środkami jest niemożliwe lub znacznie utrudnione. Klauzula taka, funkcjonującą np. w polskiej ustawie o Policji (art. 19 ust. 1), czy niemieckim kodeksie postępowania karnego (art. 100c ust. 1) jest, podobnie jak ograniczenia przedmiotowe, przejawem zasady proporcjonalności ingerencji państwa w prawa jednostki. Ze względów gwarancyjnych stosowanie podsłuchu powinno być poddane kontroli sądowej.

Istotnym problemem wiążącym się z podsłuchem jest też kwestia ponoszenia jego kosztów. Niewątpliwie wszystkich wydatków nie powinno się przerzucać jedynie na operatorów[9].

b. Uzyskiwanie danych związanych z ruchem

W niektórych krajach istnieją odrębne procedury uzyskiwania w czasie rzeczywistym danych związanych z ruchem (np. USA, Kanada), w innych może odbywać się to przy wykorzystaniu mechanizmów stworzonych dla podsłuchu treści. Uzyskiwanie danych związanych z ruchem zamiast stosowania podsłuchu treści przekazu pozwala zmniejszyć stopień ingerencji w prawo do prywatności, choć trzeba od razu wskazać na podnoszone w piśmiennictwie wątpliwości, czy w przypadku komunikacji elektronicznej granica nie ulega tu zatarciu[10].

Polski ustawodawca wprowadził, jak należy przypuszczać, możliwość gromadzenia danych związanych z ruchem do k.p.k. nowelą z 18 marca 2004 r.[11] Jest to jednak regulacja budząca wątpliwości interpretacyjne jeśli chodzi o uzyskiwanie tych danych w czasie rzeczywistym. W art. 218 § 1 k.p.k. jest bowiem mowa o wydaniu wykazów połączeń i innych przekazów, a nie np. ich kontroli i utrwalaniu, tak jak w art. 237 k.p.k. czy gromadzeniu. Wola ustawodawcy może być dopiero odczytana z art. 218b przewidującego wydanie rozporządzenia wykonawczego, który wspomina o gromadzeniu danych, jak i samego rozporządzenia. Nie jest to z pewnością uregulowanie najszczęśliwsze. Poza tym uzyskiwanie danych związanych z ruchem w czasie rzeczywistym powinno zostać unormowane w rozdziale 26 k.p.k. traktującym o podsłuchu treści, gdyż są to instrumenty podobne do siebie.

c. Dopuszczalność rozszerzonego przeszukania systemu informatycznego

---

[8] Nie zawsze jednak dowody uzyskane w ten sposób mogą być wykorzystane w procesie bezpośrednio.
[9] Szerzej na ten temat A. Lach, *Obowiązki podmiotów prowadzących działalność telekomunikacyjną w zakresie udzielania pomocy organom wymiaru sprawiedliwości i ścigania*, Materiały z Konferencji Secure 2003, s. 164 – 172.
[10] Zob. A. Adamski, Przestępczość w Cyberprzestrzeni, Toruń 2001, s. 96 – 97. Ilustracją tej tezy może być następujący log z wyszukiwarki internetowej: http://www.google.com/search?hl=en&ie=ISO-8859-1&q=sex+kids&btnG=Google+Search. Jak widać log ten zawiera też informację na temat poszukiwanej treści.
[11] Dz. U. Nr. 69, poz. 626.

Uprawnienie do rozszerzenia przeszukania i uzyskania danych znajdujących się w systemie dostępnym (np. za pomocą Internetu) dla systemu pierwotnie poddanego przeszukaniu w razie obawy utraty tych danych jest zagadnieniem niezwykle kontrowersyjnym. Podnosi się, że przeszukanie takie zagraża zbyt mocno prawu do prywatności uczestników postępowania oraz osób trzecich. Z tego względu procedura powyższa występuje w nielicznych krajach (np. w Belgii). Jak się jednak wydaje, środek ten jest potrzebny przy ściganiu cyberprzestępstw. Pozostaje jednak problem stworzenia odpowiednich zabezpieczeń i gwarancji procesowych, tak aby działania organów ścigania nie przybrały charakteru niekontrolowanego „buszowania w sieci".

d. Uprawnienie do skopiowania danych, wycofania, uczynienia niedostępnymi

Tradycyjne uprawnienia organów procesowych odnoszą się do zatrzymania dowodów rzeczowych o charakterze materialnym, np. nośnika z danymi. Taka procedura nie odpowiada często specyfice dowodów cyfrowych, które mogą być zwielokrotniane bez utraty jakości. Dlatego w procedurach karnych powinny znaleźć się zapisy zezwalające na skopiowanie danych z pozostawieniem nośnika osobie uprawnionej lub, co ważniejsze, obligujące posiadacza danych do ich skopiowania i wydania w odpowiedniej postaci, oczywiście z uwzględnieniem zakazów dowodowych, a zwłaszcza przywileju przeciwko samooskarżaniu. To samo dotyczy obowiązku wycofania danych[12] i uczynienia ich niedostępnymi, np. za pomocą narzędzi kryptograficznych. Procedury te mogą być stosowane zwłaszcza w przypadku, kiedy dane stwarzają zagrożenie (np. wirusy) lub treści zawarte w danych są niedozwolone (np. pornografia dziecięca). Pozbawiają one czasowo posiadacza kontroli nad danymi, lecz równocześnie umożliwiają zwrot danych po zakończeniu postępowania, gdyż nie wiążą się z ich zniszczeniem[13]. Uczynienie niedostępnymi znajduje uzasadnienie szczególnie w sytuacjach, kiedy mamy do czynienia z wielkimi ilościami danych, które nie powinny być dostępne i których wycofanie byłoby kłopotliwe, a jednocześnie nie ma potrzeby zatrzymania fizycznego nośnika.

e. Tymczasowe zabezpieczenie danych

Nietrwałość niektórych rodzajów dowodów cyfrowych sprawia, że muszą one być szybko zabezpieczone i chronione przed utratą bądź modyfikacją. Tradycyjne mechanizmy procesowe nie działają jednak tak szybko i może się okazać, że podczas uzyskiwania nakazu sądowego lub prokuratorskiego przez policję, ślady przestępstwa przestały istnieć lub zmniejszyła się ich wartość dowodowa. Niedogodność tę usuwa wprowadzenie procedury tymczasowego zabezpieczenia danych, która pozwala bez zbędnej zwłoki niejako „zamrozić" dane do czasu zakończenia bardziej

[12] Wycofanie danych oznacza ich zabranie z pozostawieniem nośnika posiadaczowi, czym procedura ta różni się od tradycyjnego zatrzymania, które wiąże się z zajęciem nośnika.
[13] Por. European Committee on Crime Problems, *Draft Convention on Cyber – Crime and Explanatory Memorandum Related Thereto*, Strasbourg, 29 June 2001, par. 197 – 199 of the Draft Explanatory Report.

sformalizowanych kroków. Procedurę taką przewiduje art. 16 i częściowo art. 17 Konwencji Rady Europy o Cyberprzestępczości. Została ona inkorporowana również do prawa polskiego (art. 218a k.p.k.). W myśl tego przepisu sąd lub prokurator może wydać podmiotom wymienionym w art. 218a k.p.k., a więc przede wszystkim podmiotom prowadzącym działalność telekomunikacyjną nakaz zabezpieczenia danych na okres do 90 dni. Konstrukcję tego przepisu należy ocenić sceptycznie. Po pierwsze obowiązek zabezpieczenia danych powinien znaleźć zastosowanie do wszystkich posiadaczy danych (oczywiście z uwzględnieniem zakazów dowodowych), a nie tylko wąskiej ich grupy wymienionej w art. 218a k.p.k., po drugie zaś stosowne uprawnienie, zgodnie z celem instytucji tymczasowego zabezpieczenia danych, powinno zostać przyznane przede wszystkim policji.

f. Wprowadzenie obowiązku zatrzymania danych

Zatrzymanie danych (*data retention*) jest bez wątpienia najbardziej kontrowersyjną metoda zabezpieczenia danych informatycznych dla potrzeb ewentualnych przyszłych postępowań karnych. Wiąże się to z problemami technicznymi (stworzenie odpowiedniej infrastruktury dla przechwytywania, przechowywania i wyszukiwania danych), ekonomicznymi (koszty materiałowe i osobowe przedsięwzięcia) i prawnymi (zachowanie zasady proporcjonalności ingerencji w prawo do poszanowania tajemnicy komunikowania się, zachowanie gwarancji przewidzianych dla przetwarzania danych osobowych). W chwili obecnej procedurę zatrzymania danych przewidują już niektóre państwa UE (Belgia, Zjednoczone Królestwo), które otrzymały na to „zielone światło" w postaci art. 15 dyrektywy UE w sprawie prywatności i komunikacji elektronicznej z 12 lipca 2002 r. (2002/58/EC)[14]. Nie sposób też nie zauważyć, że pewna liberalizacja w tym zakresie nastąpiła po ataku z 11 września 2001 r. na World Trade Center, co trzeba chyba tłumaczyć zbyt bezkrytyczną czasami wiarą w skuteczność gromadzenia danych. W mojej ocenie do przedsięwzięcia tego należy podchodzić sceptycznie, gdyż skala podejmowanych działań, kosztów, ograniczenia prawa do prywatności i innych negatywnych skutków wydaje się przeważać nad ewentualnymi korzyściami[15]. Trudno przy tym zakładać, że dla przestępczości zorganizowanej i terrorystów zatrzymanie danych będzie stanowić jakiś poważny problem.

g. Stosowanie kryptografii

Narzędzia kryptograficzne potrafią znacznie utrudnić, a czasami wręcz uniemożliwić pracę organom ścigania. Z tego względu w prawie krajowym powinny istnieć instrumenty umożliwiające uzyskanie danych w postaci niezaszyfrowanej. Instrumentem takim nie powinien być, jak się wydaje, obowiązek wydania organom ścigania kluczy prywatnych lub „superklucza"

[14] OJ L 201, 31.07.02.
[15] Zob. też opracowanie Article 29 Data Protection Working Party, *Opinion 1/2003 on the storage of traffic data for billing purposes. Adopted on 29 January 2003,* 12054/02/EN, WP 69.

(*key escrow*), o co usilnie zabiega od dłuższego czasu między innymi administracja amerykańska. Wystarczy możliwość wydania podmiotom korzystającym z narzędzi kryptograficznych nakazu dostarczenia danych w postaci niezaszyfrowanej, co jednak też będzie wiązać się ze stworzeniem odpowiedniej infrastruktury i czasami może się okazać znacznie utrudnione lub zgoła niemożliwe ze względów technicznych. Trzeba też zastrzec, że obowiązek deszyfracji powinien ograniczać się do danych zaszyfrowanych przez podmioty zobowiązane do wydania, a nie np. przez użytkowników ich usług.

h. Uprawnienie pracodawców do kontrolowania przekazów informacji dokonywanych przez pracowników

Wiele przestępstw komputerowych popełnianych jest przez pracowników w miejscu pracy, bądź tam znajdują się ślady działalności godzącej w jednostkę zatrudniającą. Działalność taka może wyrządzić pracodawcy bezpośrednią szkodę lub narazić go na roszczenia osób trzecich (poszkodowanych). Dlatego pracodawcy żądają przyznania prawa do kontrolowania poczty elektronicznej pracownika i prowadzonych przez niego rozmów. Powstaje więc problem, czy powinni oni posiadać takie uprawnienia, a jeśli tak, to czy zgromadzone w ten sposób informacje mogą być wykorzystane następnie jako dowody w postępowaniu karnym. Kwestia ta wymaga jasnej regulacji ustawowej, biorącej pod uwagę usprawiedliwione interesy obu stron.

Analiza przedstawionych wyżej zagadnień skłania do postawienia zasadniczego pytania: czy dla potrzeb wykorzystania dowodów cyfrowych powinno się tworzyć nowe środki przymusu procesowego, czy też wystarczające będzie stosowanie *per analogiam* i z uwzględnieniem specyfiki środowiska komputerowego istniejących instytucji karnoprocesowych. Wyrażam tu pogląd o konieczności wprowadzenia niektórych nowych środków[16]. Przemawia za tym szereg argumentów. Po pierwsze, stosowanie tradycyjnych instrumentów wielokrotnie nie zapewnia należytej efektywności i szybkości działania, udaremniając ściganie w cyberprzestrzeni szeregu przestępstw (m. in. rozpowszechniania pornografii dziecięcej). Kolejną okolicznością jest konieczność przestrzegania zasady proporcjonalności ingerencji państwa w prawa jednostki. Koronnym argumentem jest zaś potrzeba istnienia mechanizmu zabezpieczającego przed nadużywaniem uprawnień przez organy ścigania i wyposażenia użytkowników sieci w skuteczne instrumenty prawne służące zaskarżaniu bezprawnych lub niesłusznych czynności procesowych. Trudno sobie wyobrazić, aby środki takie zostały zagwarantowane np. przy „odpowiednim"

[16] Taki punkt widzenia zaprezentował np. holenderski Komitet Doradczy przy Ministrze Sprawiedliwości podczas prac nad nowelizacją przepisów proceduralnych służących ściganiu przestępczości komputerowej. Zob. H. W. Kaspersen, *Computer Crimes and other Crimes against Information Technology in the Netherlands* [w:] U. Sieber, *Information Technology Crime*, Koln – Berlin – Bonn – Munchen 1994, s. 367. Por. też A. Adamski, Prawo..., s. 215 – 216.

stosowaniu przepisów o przeszukaniu pomieszczeń i rzeczy do rozszerzonego przeszukania systemu informatycznego.

5. Status dowodów cyfrowych w prawie dowodowym krajów *common law* i *civil law*

Wykorzystanie dowodów cyfrowych napotyka na zdecydowanie większe trudności w krajach *common law* niż *civil law*. Wiąże się to ze sztywnymi regułami i zakazami dowodowymi funkcjonującymi w systemach posiadających elementy legalnej teorii dowodowej, w tym zwłaszcza zakazem *hearsay* i zasadą *best evidence*[17]. Skutkiem tego jest często niedopuszczalność zgromadzonych legalnie i posiadających dużą wartość informacji. Dlatego w krajach *common law* ogranicza się stopniowo zakaz *hearsay* w drodze ustawowych wyjątków oraz przyjmuje, że dane powstałe w ramach automatycznego działania systemu informatycznego nie stanowią *documentary evidence* lecz *real evidence*[18].

Z powyższymi problemami nie spotykamy się co do zasady w systemach prawnych opartych na zasadzie swobodnej oceny dowodów, np. w Polsce[19]. Próby apriorycznego wartościowania dowodów czy przyjmowanie domniemania ich niewiarygodności są bez wątpienia nie do pogodzenia z tą zasadą.

Niezależnie od przedstawionych wyżej różnic, nie wydaje się, aby w przeciwieństwie do metod uzyskiwania dowodów, musiały zostać wprowadzone do procedur karnych jakieś istotne rozwiązania prawne w zakresie wykorzystania zgromadzonych dowodów cyfrowych w procesie. Jak można przypuszczać, adaptacja tradycyjnych przepisów odnoszących się do typowych dowodów rzeczowych oraz dokumentów jest możliwa i jak najbardziej wskazana. Tezę taką potwierdzają doświadczenia państw, które swojego czasu zdecydowały się na odrębne regulacje, czego znakomitym przykładem jest obowiązujący jeszcze kilka lat temu w prawie angielskim osławiony art. 69 Police and Criminal Evidence Act 1984. Przepis ten przed dopuszczeniem przez sąd dowodów cyfrowych wymagał wykazania co najmniej, że komputer, który je wygenerował działał poprawnie i był prawidłowo użytkowany. Wywoływało to w praktyce duże trudności i prowadziło w następstwie do bezkarności sprawców przestępstw popełnianych przy użyciu komputera. Opracowania, standaryzacji i częściowego skodyfikowania wymagają za to techniczne aspekty postępowania z dowodami cyfrowymi, włącznie z problematyką zapewnienia ich integralności w trakcie procesu i prezentacji.

[17] Na temat tych reguł zob. np. A. Lach, *Dowody w angielskim procesie karnym*, Palestra 1 – 2/2002, s. 150 – 151.
[18] Zob. np. P. Murphy, *Murphy on Evidence*, London 2000, s. 569 – 571.
[19] Zob. art. 7 polskiego k.p.k.

6. Prezentacja dowodów cyfrowych

Aby organ procesowy mógł zapoznać się z zabezpieczonymi dowodami cyfrowymi i właściwie je ocenić, konieczne jest stworzenie należytych mechanizmów prezentacji. Prezentacja taka musi:

a. stwarzać uczestnikom równe szanse zapoznania się z dowodami cyfrowymi, co jest szczególnie ważne w przypadku strony biernej (podejrzanego, oskarżonego), gdyż wiąże się z możliwością wykonywania przez niego prawa do obrony,

b. przystępnie przedstawiać zagadnienia techniczne, z czym wiąże się stosowanie wykresów, schematów połączeń, animacji, itp.,

c. umożliwiać weryfikację autentyczności przedstawionego materiału dowodowego oraz zapewniać integralność danych w czasie samej prezentacji,

d. uwzględniać zasadę szybkości postępowania i ekonomiki procesowej.

Obecnie istnieje na rynku wiele wyspecjalizowanych narzędzi służących do prezentacji dowodów cyfrowych. Przykładowo można wymienić tu system DEPS (Digital Evidence Presentation System). Trzeba jednak też brać pod uwagę realia wymiaru sprawiedliwości, gdzie niekiedy bariery techniczne spowodowane opóźnieniami w zakresie informatyzacji mogą zmuszać do posługiwania się jedynie wydrukami czy innymi tradycyjnymi metodami prezentacji danych, czyniąc tym samym wizję „cybersądu”[20] dość odległą. Opóźnienia te uniemożliwiają też korzystanie z nowoczesnych metod prezentacji danych, jakimi są np. animacje i symulacje komputerowe.

7. Podsumowanie

Współczesne prawo dowodowe wciąż napotyka na nowe metody dochodzenia do prawdy. Dowody cyfrowe stanowią kolejną propozycję, której odrzucić po prostu nie można. Być może ich wykorzystanie wydaje się skomplikowane, metody gromadzenia kontrowersyjne a rezultat niepewny, lecz czyż tak samo nie jest np. z dowodem z badań DNA, wariografem czy śladami osmologicznymi? Chciałbym tu podkreślić stanowczo, że dowodów tych nie można traktować jako drugorzędnych informacji przydatnych tylko do działań operacyjnych lub poszukiwania innych, „pewniejszych” środków dowodowych. Nie stanowią one też zupełnie nowej grupy dowodów, lecz jedynie proces ich gromadzenia ze wskazanych wyżej względów wymaga pewnej modyfikacji niektórych istniejących środków przymusu i w miarę potrzeby wprowadzenia nowych. *Last but not*

[20] Istnieje obecnie wiele projektów wcielających w życie wizję sądu działającego w oparciu o nowoczesne technologie przetwarzania informacji. Zob. np. www.courtroom21.net.

least konieczna jest też standaryzacja metodyki postępowania z dowodami cyfrowymi i szkolenie w tej dziedzinie funkcjonariuszy organów ścigania i wymiaru sprawiedliwości oraz biegłych.