

Dr Arkadiusz Lach

Katedra Postępowania Karnego UMK

Dowody elektroniczne w postępowaniu karnym; zasady ich uzyskiwania i wykorzystywania

Program szkolenia

1. Pojęcie dowodu elektronicznego

Informacja w formie elektronicznej (przesyłana lub przechowywana), mogąca mieć znaczenie dowodowe.

2. Rodzaje dowodów elektronicznych.

Dowody elektroniczne możemy dzielić według różnych kryteriów:

- a. w zależności od rodzaju nośnika: przechowywane (np. dokumenty elektroniczne) lub przesyłane (np. czat, rozmowa telefoniczna),
- b. w zależności od treści: zawierające tekst, obraz, dźwięk i inne,
- c. w zależności od rodzaju zapisu: analogowe i cyfrowe (w tym zdigitalizowane, a więc takie w których wersje tradycyjną przekształcono w cyfrową),
- d. w zależności od źródła dowodu: dowody rzeczowe *sensu stricte* i dokumenty.

Konwencja Rady Europy w sprawie Cyberprzestępczości wyszczególnia treść, dane związane z ruchem i dane dotyczące abonenta.

Dane związane z ruchem (*traffic data*): dowolne dane informatyczne odnoszące się do komunikowania się za pomocą systemu informatycznego, wygenerowane przez system informatyczny, który utworzył część w łańcuchu komunikacyjnym, wskazując swoje pochodzenie, przeznaczenie, ścieżkę, czas, datę rozmiar, czas trwania lub rodzaj danej usługi (art. 1d Konwencji o Cyberprzestępczości).

Dane dotyczące abonenta w Konwencji o Cyberprzestępczości: Wszelkie informacje w postaci danych informatycznych lub w dowolnej innej postaci, znajdujące się w posiadaniu dostawcy usług i odnoszące się do użytkowników tych usług, inne niż dane dotyczące ruchu i treści, które pozwalają na ustalenie:

- rodzaju usług komunikacyjnych z jakich korzysta użytkownik, zastosowanych w związku z tym rozwiązań technicznych oraz okresu usługi

- tożsamości użytkownika, adresu pocztowego lub geograficznego, numeru telefonu lub innego dostępu, wykazu połączeń i informacji o płatnościach dostępnych na podstawie umowy lub ustaleń dotyczących usługi
- wszelkich innych informacji związanych z miejscem zainstalowania sprzętu komunikacyjnego dostępnych na podstawie umowy lub ustaleń dotyczących usługi

Rodzaje danych na gruncie prawa polskiego:

Art. 159 Prawa telekomunikacyjnego: Tajemnica komunikowania się w sieciach telekomunikacyjnych, zwana dalej "tajemnicą telekomunikacyjną", obejmuje:

- 1) dane dotyczące użytkownika;
- 2) treść indywidualnych komunikatów;
- 3) dane transmisyjne, które oznaczają dane przetwarzane dla celów przekazywania komunikatów w sieciach telekomunikacyjnych lub naliczania opłat za usługi telekomunikacyjne, w tym dane lokalizacyjne, które oznaczają wszelkie dane przetwarzane w sieci telekomunikacyjnej wskazujące położenie geograficzne urządzenia końcowego użytkownika publicznie dostępnych usług telekomunikacyjnych;
- 4) dane o lokalizacji, które oznaczają dane lokalizacyjne wykraczające poza dane niezbędne do transmisji komunikatu lub wystawienia rachunku;
- 5) dane o próbach uzyskania połączenia między określonymi zakończeniami sieci telekomunikacyjnej.

3. Regulacje służące gromadzeniu dowodów elektronicznych

- a. W czasie rzeczywistym: rozdział 26 k.p.k. i art. 19 ustawy o Policji
- b. Danych przechowywanych: rozdział 25 k.p.k., art. 20c ustawy o Policji, ustawa o świadczeniu usług drogą elektroniczną
- c. Tymczasowe zabezpieczenie danych: art. 218a k.p.k.
- d. Tzw. dowody prywatne.

4. Zatrzymanie danych (data retention)

Operator publicznej sieci telekomunikacyjnej lub dostawca publicznie dostępnych usług telekomunikacyjnych przetwarzający dane transmisyjne dotyczące abonentów i użytkowników końcowych jest obowiązany, z uwagi na realizację przez uprawnione organy zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, dane te przechowywać przez okres 2 lat. Obowiązek uważa się za wykonany w przypadku gdy zaprzestający działalności operator publicznej sieci telekomunikacyjnej lub dostawca publicznie dostępnych usług telekomunikacyjnych przekaże do przechowywania dane transmisyjne innemu

operatorowi publicznej sieci telekomunikacyjnej lub dostawcy publicznie dostępnych usług telekomunikacyjnych. Po upływie tego okresu, dane transmisyjne są usuwane lub anonimizowane przez operatora publicznej sieci telekomunikacyjnej lub dostawcę publicznie dostępnych usług telekomunikacyjnych, którzy je przechowują. Operator publicznej sieci telekomunikacyjnej lub dostawca publicznie dostępnych usług telekomunikacyjnych przechowujący dane transmisyjne jest obowiązany dołożyć szczególnej staranności w celu ochrony

5. Przydatność dowodów elektronicznych dla dokonywania ustaleń faktycznych

a. poszlakowy charakter, np. użycie hasła identyfikuje wiedzę sprawcy, a nie jego tożsamość, podpis pod dokumentem elektronicznym nie wskazuje nam jego autora, dane nadawcy w nagłówku nie oznaczają, że wiadomość została wysłana akurat przez tę osobę, dane identyfikujące zakończenie sieci nie wskazują osoby, która to urządzenie użytkowała w określonym przedziale czasowym, itp.

b. duplikat a kopia,

Kopiowanie przenosi tylko dane, klonowanie bit po bicie odwzorowuje nośnik (idealnie lub bez zachowania identycznego układu danych), a więc także dane ukryte i usunięte.

c. szczególne właściwości:

- trudność zniszczenia

Można powiedzieć, że dowody elektroniczne łatwo jest usunąć lub przenieść w inne miejsce, natomiast trudno je zniszczyć definitywnie.

- łatwość kopiowania

Właściwość ta pozwala tworzyć kilka kopii danych w celu ich przeanalizowania, co niewątpliwie ułatwia prace organom procesowym i biegłym.

- łatwość modyfikacji

Dane informatyczne łatwo jest zmodyfikować usuwając część danych czy wprowadzając nowe.

6. Rola biegłego i specjalisty

Art. 207 par. 2: jeżeli przedmiot może ulec przy badaniu zniszczeniu lub zniekształceniu, część tego przedmiotu należy zachować w stanie nie zmienionym lub gdy nie jest to możliwe stan ten utrwalić w inny sposób.

Biegły (np. odzyskanie danych, złamanie ochrony) a specjalista (np. fotografia i demontaż systemu)

7. Tryb prywatnoskargowy

a. pokrzywdzony nie ma odpowiednich możliwości dowodowych,

b. objęcie ściganiem czynu przez prokuratora.

8. Współpraca międzynarodowa

Wybrane orzecznictwo:

wyrok SN z 13.11.2002, I CKN 1150/00, LEX nr 75292

Przepisy regulujące podsłuch procesowy i podsłuch operacyjny, uznawane powszechnie za okoliczności wyłączające bezprawność podsłuchu, należy traktować jako istotną wskazówkę przy ocenie wyłączenia bezprawności w innych wypadkach podsłuchu, ponieważ świadczą one o tym, w jakich sytuacjach sam ustawodawca dopuszcza możliwość wyłączenia tajemnicy komunikowania się.

postanowienie SN z 26.04.2007, I KZP 6/07, OSNKW 2007, nr 5, poz. 37

1. "Uzyskane dowody pozwalające na wszczęcie postępowania karnego lub mające znaczenie dla toczącego się postępowania karnego" (art. 19 ust. 15 ustawy z dnia 6 kwietnia 1990 r. o Policji, Dz.U. z 2007 r. Nr 43, poz. 277 ze zm.) to dowody popełnienia przestępstw określonych w art. 19 ust. 1 tej ustawy.

2. Uzyskane w czasie kontroli operacyjnej dowody popełnienia przestępstw - określonych w art. 19 ust. 1 ustawy o Policji - przez osobę inną niż objęta postanowieniem wydanym na podstawie art. 19 ust. 2 tej ustawy albo popełnionych wprawdzie przez osobę nim objętą, ale dotyczące przestępstw innych niż wskazane w tym postanowieniu, mogą być wykorzystane w postępowaniu przed sądem (art. 393 § 1 zd. 1 k.p.k., stosowany odpowiednio), pod warunkiem, że w tym zakresie zostanie wyrażona następcza zgoda sądu na przeprowadzenie kontroli operacyjnej (art. 19 ust. 3 ustawy o Policji, stosowany odpowiednio).

Postanowienie SN z 14.11.2006, V KK 52/06, LEX nr 202271

Nagranie przez Marka P. treści dwóch prywatnych rozmów w których zawarto propozycję korupcyjną, nie odbywało się w trybie przepisów rozdziału 26 k.p.k., wobec czego nie było poprzedzone procedurą przewidzianą w art. 237 i następnych tego Kodeksu. Stąd też mowy być nie może o naruszeniu art. 241 k.p.k. Nagrania te nie były objęte żadnym z zakazów dowodowych przewidzianych w k.p.k. Uznanie, że funkcjonariusz ABW, zapewniając sprzęt

do nagrania tych rozmów, postąpił wbrew regulacjom prawnym go obowiązującym, daje jedynie podstawy do odpowiedzialności np. dyscyplinarnej tego funkcjonariusza, ale nie eliminuje przecież uzyskanego z jego pomocą dowodu spośród materiału mogącego być wykorzystanym w postępowaniu karnym. Obowiązująca procedura karna nie wprowadza żadnego zamkniętego katalogu dowodów, uznając za takie w zasadzie wszystko, co może przyczynić się do wyjaśnienia prawdy, o ile nie jest objęte ściśle określonym zakazem dowodowym. Nieznany jest też tej procedurze zakaz wykorzystania dowodów określanych w literaturze procesowej jako "owoce z zatrutego drzewa".