CBKE
e-BIULETYN

Wykrywanie przestępstw popełnianych w bankowości elektronicznej (problematyka dowodowa)

Prof. dr hab. Ryszard Jaworski

Uniwersytet Wrocławski, Wydział Prawa, Administracji i Ekonomii, Katedra Kryminalistyki

Elektroniczny przekaz oświadczeń woli, będący sposobem dokonywania operacji bankowych, stwarza zupełnie nowe problemy wykrywcze i dowodowe, typowe dla tzw. „przestępstw komputerowych".

Tradycyjny sposób realizowania operacji bankowych pozostawiał wiele klasycznych śladów, będących podstawą działań wykrywczych, a ponadto stanowiących później rzeczowe środki dowodowe w procesie. Poddawały się one percepcji wzrokowej, a tylko niekiedy wymagały udziału biegłych do zbadania ich szczególnych właściwości. Klient banku ręcznie wpisywał różne dane, podobnie jak i pracownicy banku. Na poszczególnych etapach operacji dokument bywał także opatrywany indywidualnymi pieczęciami pracowników banku. Gdy powstawały wątpliwości, rekonstruowano obieg dokumentu oraz identyfikowano pracowników dokonujących poszczególnych operacji, poprzez analizę porównywanie pieczęci i podpisów, a w razie konieczności – ich kryminalistyczne badania identyfikacyjne. Podstawą identyfikacji było założenie, że w piśmie ręcznym i podpisach występują liczne cechy (budowa liter i cyfr, wiązania międzyliterowe, naciskowość itd.) mające walor cech indywidualnych człowieka, dzięki czemu ich badanie pozwala ustalić, czy istnieje związek tych elementów dokumentu z ich wykonawcą (klient, pracownicy banku). Dużą liczbę cech indywidualnych posiadają również stemple. Udowodnienie istnienia lub braku związku fizycznego człowieka z dokumentem stwarzało domniemanie prawdziwości oświadczenia woli tego właśnie człowieka albo braku oświadczenia pochodzącego od tej osoby.

Elektroniczny zapis i przekaz nie zawiera śladów, na podstawie których zidentyfikowano by osobę dokonującą zapisu: forma zapisu, ani jego treść nie zawierają cech, jakie posiada pismo ręczne, komputer eliminuje też błędy ortograficzne, a nawet językowe. Elektroniczna forma

czynności bankowych utrudni wykrycie sprawcy i udowodnienie mu winy, z tego względu, że można zidentyfikować urządzenie (komputer) użyte do przekazu. Ale czy postawimy komputer przed sądem? Komputer jest ogniwem pośrednim, środkiem, którym posłużył się człowiek. Czy możemy dotrzeć do tego człowieka? „Ślad elektroniczny" ma formę ciągu liczbowego, pozbawiony jest cech indywidualizujących wykonawcę już podczas wprowadzania go do maszyny. Jak udowodnić następne ogniwo: maszyna = człowiek? Innymi słowy, udowodnić możemy związek przyczynowy pomiędzy maszyną użytą do fałszywego przekazu woli (właściciela rachunku itp.) a skutkiem czynu. Podmiotem odpowiedzialności karnej jest natomiast człowiek.

Komputer wprowadza więc anonimowość, autor fałszywego przekazu „chowa się" za maszyną. Uzyskać może znaczne korzyści materialne, równocześnie unikając odpowiedzialności. Co gorsze, czasem przerzucając skutki swego działania na człowieka obsługującego konkretny komputer.

Drugim, całkowicie nowym elementem, ważnym dla wykrycia sprawcy i udowodnienia mu winy, jest oddzielenie miejsca pobytu sprawcy od miejsca wystąpienia skutku. Sprawca może znajdować się nawet na innym kontynencie. Nie wchodzi w kontakt fizyczny z pokrzywdzonym, ten ostatni nie jest więc źródłem dowodowym, tak jak przy wielu klasycznych czynach kryminalnych. Może jedynie zanegować fakt złożenie przez siebie stosowanego oświadczenia woli odnośnie czynności bankowej.

Ponadto pojawia się pytanie, czy – z powodu wspomnianej odległości - uda się obalić alibi sprawcy? Jest to niezbędne z uwagi na przepis kodeksu postępowania karnego, nakładający na oskarżyciela ciężar dowodu.

Problematyka procesowo – kryminalistyczna, powstająca na tle przestępczości elektronicznej, została dostrzeżona już kilkanaście lat temu:

1. Raport OECD z roku 1986 uznał za niezbędne transgraniczne przeszukanie sieci.
2. Raport Wspólnoty Europejskiej z roku 1987 szerzej potraktował problem. Uznano w nim transgraniczne przeszukanie sieci za podstawowe narzędzie ścigania przestępstw komputerowych.
3. Raport Rady Europy z roku 1990 zwrócił uwagę na specyfikę środków dowodowych i środków przymusu, problem dopuszczalności danych komputerowych jako dowodu, uznając dotychczasowe uregulowania prawne za niedostosowane do nowego typu dowodów.
4. Zalecenia XV Międzynarodowego Kongresu Prawa Karnego w Rio de Janeiro z roku 1994 były następujące:
   - przyznać organom ścigania uprawnienia do:

a) prowadzenia przeszukania sieci komputerowych i zatrzymania rzeczy niematerialnych,

b) kontrolowania wiadomości przesłanych wewnątrz systemu komputerowego i między systemami i uzyskiwania w ten sposób dowodów oraz dopuszczenia tych dowodów do wykorzystania w procesie.

c) zobowiązać pokrzywdzonych, świadków i inne osoby (oprócz podejrzanego) do współpracy z organami ścigania.

5. Zalecenie Rady Europy nr 13 z roku 1995 dotyczące zagadnień związanych z technologią informatyczną oraz Załącznik do tego zalecenia potraktował zagadnienia te znacznie obszerniej („Archiwum Kryminologii", tom XXIV, rok 1997-1998, Warszawa.)

Zwraca się w tym dokumencie uwagę, że informacja w postaci danych komputerowych jest nową formą dowodu. Klasyczne rzeczy mogły być odnalezione dzięki swym właściwościom fizycznym, zatrzymane przez organa ścigania i poddane badaniom identyfikacyjnym. Środkiem dowodowym było już samo ich miejsce przechowywania, właściwości rzeczy poddające się postrzeganiu zmysłowemu, następnie zaś wyniki badań identyfikacyjnych. Co do pojedynczego komputera, klasyczne przeszukanie może dostarczyć dowodów (znalezienie w nim danych oraz wykazanie potraktowania ich jako informacji przez użytkownika komputera). Natomiast staje się to prawie niemożliwe, gdy komputer pracuje w sieci.

Dlatego należy przyznać organom ścigania inne możliwości zdobywania dowodów:

- przeszukiwanie systemów komputerowych, nakładając obowiązek pomocy ze strony operatora systemu i administratora danych,
- rozpoczęcie działań (przeszukanie i zatrzymanie) bez wiedzy użytkownika lub administratora danych, bowiem dane w formie elektronicznej są bardzo łatwe do usunięcia,
- wyraźnie dopuszcza się stosowanie działań operacyjnych odnośnie przestępstw informatycznych, postulując poszerzenie uprawnień organów ścigania co do czynności operacyjnych na tę kategorię zdarzeń (dotychczas czynności operacyjne były dopuszczalne tylko przy najpoważniejszych przestępstwach). Uzasadnia się to tym, że nie można akceptować sytuacji, gdy organa ścigania nie mogłyby wykonać swych obowiązków w odniesieniu do wymiaru sprawiedliwości i społeczeństwa,
- stosowanie kontroli przepływu danych. Uzyskane w wyniku tego informacje mogą być podstawą do wszczęcia dochodzenia. Jest to przełom w dotychczasowym traktowaniu czynności operacyjnych przez naukę prawa, zdecydowanie negatywnym.

Wskazuje to uświadomienie sobie przez teorię procesu specyfiki „śladu elektronicznego" i wynikających z niej trudności dowodowych,

- z uwagi na nielimitowany granicami państwowymi przepływ danych, szczególnego znaczenia nabiera współpraca organów ścigania różnych krajów. Pojawia się problem przeszukiwania transgranicznego, a na tym tle konfliktu interesów i wartości: szybkość działania a zagadnienie suwerenności państwowej,
- stosowanie szyfrowania do przekazu danych może być stosowane również przez przestępców. Przeciwdziałać temu można ograniczając dostęp do systemów szyfrujących lub zobowiązując operatorów do udostępnienia organom ścigania odpowiednich algorytmów.

Inny, ważny problem, podniesiony w tym dokumencie to zagadnienie wiarygodności dowodów elektronicznych. Jak wykazać, że dowód dostarczony do sądu dotarł w formie niezmienionej i kompletnej, w takiej jak go znaleziono?

Proponuje się rozwiązania polegające na tym, że:

- prokurator musi odtworzyć kompletny łańcuch posiadaczy danych od momentu ich znalezienia,
- do zabezpieczania znalezionych danych używany jest podpis elektroniczny.

W dokumencie tym uznaje się za niezbędne szkolenie prokuratorów i sędziów w zakresie „dowodów elektronicznych", gdyż zasadna jest obawa, że konserwatywne podejście skutkować może uniewinnianiem przestępców. Przeciętny prawnik, zatrudniony w prokuraturze, może mieć trudności w ustaleniem łańcucha działań (serwery, połączenia i ich kolejność), będzie zmuszony do korzystania z pomocy specjalistów już od etapu poszukiwania maszyny zastosowanej do fałszywej operacji.

Postulat ten jest jak najbardziej uzasadniony, powinien być wzięty pod uwagę na etapie nauczanie prawa, jak i doskonalenia umiejętności zawodowych prawników – praktyków. Można się bowiem spodziewać, że udowodnienie sprawstwa nastąpi przeważnie z jakimś stopniem prawdopodobieństwa. Czy to wystarczy sądowi do uznania sprawstwa, zwłaszcza wobec normy prawnej nakazującej rozstrzygać na korzyść oskarżonego nie dające się usunąć wątpliwości. W jakiej sytuacji należy uznać, że prawdopodobieństwo, iż to ktoś inny niż oskarżony dokonał czynu, jest tak małe, że praktycznie oznacza wykluczenie takiej możliwości? Czy prawnicy potrafią prawidłowo obliczyć prawdopodobieństwo? Obserwacje wykazują, że mają z tym problem, gdyż tylko znikoma część prawników, nawet studentów (ponieważ aktualnie studenci prawa w programie nauczania szkoły średniej mieli rachunek prawdopodobieństwa), potrafi obliczyć prawdopodobieństwo dwóch zdarzeń przypadkowych[1].

Wyżej zasygnalizowane problemy znalazły bardziej konkretny charakter, w formie norm prawnych, w Europejskiej Konwencji w Sprawie Cyberprzestępczości, z dnia 23.XI.2001 roku.

Również organa ścigania, w krajach o najbardziej zaawansowanej technologii elektronicznej, dostrzegały problemy dowodowe :

- Interpol już w 1990 roku opracował informacje odnośnie utrwalania i przesyłania dowodów elektronicznych.
- W USA Departament Sprawiedliwości opracował w roku 1989 podobne wytyczne dla prokuratorów i policjantów, a w roku 1994 wydano w tym przedmiocie wytyczne federalne.

Niektóre przestępstwa w bankowości elektronicznej pozostawiają po sobie również klasyczne ślady, na tyle liczne i zróżnicowane, że nie powinno być większych trudności z ustaleniem sprawstwa. Wymienić tu można:

- fałszowanie kart płatniczych (magnetycznych) lub ich podrabianie,
- fizyczną kradzież kart płatniczych, odkodowanie numeru PIN i wybranie pieniędzy.

Bardziej złożone pod względem śladów są takie zdarzenia, jak:

- podrabianie internetowych stron bankowych i przekierowywanie przelewów lub wpłat na inne konta,
- przychwytywanie danych odnośnie konta bankowego i jego parametrów podczas sesji połączeniowych: przelewy, zakupy internetowe (e- commerce).

Należy się liczyć także z sytuacją, gdy sprawca fałszywej dyspozycji będzie pracownikiem banku. Dynamiczny rozwój bankowości zmusił do zatrudniania nowych pracowników, a nie wszyscy zdążyli sobie przyswoić swoisty etos pracy w tych instytucjach, co było zresztą zawsze procesem trwającym kilka lat. Stały kontakt z pieniędzmi pobudza wyobraźnię takich osób w niewłaściwym kierunku, szukają oni wówczas sposobności, analizują szansę zdemaskowania, możliwość „podszycia" się pod kogoś. Zabezpieczenia utrudniają wprawdzie popełnianie nadużyć w obrocie bankowym, ale nie dają gwarancji ich uniknięcia.

Już klasyczna kradzież zaistniała w banku jest nietypowa. Nie sprawdza się w jej przypadku klasyczne typowanie kryminalistyczne, oparte na motywie materialnym. Impulsem kradzieży, bo tak należałoby powiedzieć, może być niezwykła okazja, sytuacja nieprzewidziana i nieplanowana, dająca zarazem gwarancję, że podejrzenie padnie na zupełnie inną osobę, a nie na rzeczywistego sprawcę.

Chociaż są różne sposoby zapobiegania potencjalnym nadużyciom, takie jak hasła dostępu i częsta ich zmiana (nie zawsze wymóg ten był i jest respektowany), magnetyczne lub elektroniczne karty dostępu, rejestracja operacji (czas dokonania, stanowisko, treść operacji) itp., to praktyka wykazuje, że nie zawsze są one wystarczające.

Komputer ułatwia sprawcy maskowanie działań, można bowiem korzystać z komputera kolegi (gdy komputer pozostaje nie wyłączony) lub podpatrzonego czy odkodowanego hasła dostępu.

Sprawstwo przypisywane jest prawie automatycznie użytkownikowi komputera wykorzystanego do fałszywej operacji. Człowiek taki jest „karany" wielostronnie, bo oprócz konsekwencji karno – prawnych i cywilno - prawnych ponosi straty moralne. W opinii dotychczasowych kolegów uchodzi nie tylko za przestępcę, ale i za osobę, która sprzeniewierzyła się zasadom zawodowym, naruszyła reputację zespołu pracowniczego oraz instytucji, dla której uczciwość jest fundamentem funkcjonowania. Nie koniec na tym. Zwolnienie tego pracownika nie zawsze oznacza wykrycie sprawcy i rozwiązanie problemu, sprawca być może nadal pozostaje w zespole. Ponieważ wszyscy mają tego świadomość, zdezorganizowana jest praca instytucji. Traci zespół pracowniczy: sprawca działa przeciwko kolegom, wszyscy wiedzą, że ktoś spośród nich złamał jedną z podstawowych zasad pracy w banku – wzajemnego zaufania. Wyjaśnienie tej sytuacji ma nie tylko znaczenie prawne, ale także moralne i czysto ekonomiczne. Kryminalistyka dysponuje w tym zakresie pewnymi możliwościami[2].

Trudno oszacować liczbę przestępstw popełnianych w bankowości elektronicznej, ponieważ są ukrywane przez banki obawiające się o swoją reputację. Jest jednak prawdopodobne, że różne formy nadużyć w elektronicznym obrocie bankowym zdarzać się będą częściej. Składają się na tę prognozę następujące obserwacje:

I. Wprawdzie zabezpieczenia elektronicznych czynności bankowych są ciągle doskonalone, to z drugiej strony rozpowszechnia się umiejętność korzystania z komputerów i znajomość ich programowania, a wielu „hakerów" poszukuje sposobów „obejścia" lub „złamania" zabezpieczeń. Niektórzy traktują to jako źródło dochodów, inni jako „hobby" czy nawet swego rodzaju intelektualną rywalizację. Co istotne dla działań wykrywczych, to fakt, że są to osoby o specyficznej motywacji, nieznanej przy „klasycznych przestępstwach", nie mieszczącej się w dotychczasowych klasyfikacjach, a o tyle niebezpiecznej, że jest ona bardzo silna, niekiedy trudno zrozumiała dla postronnego obserwatora. Wpływać to musi na typowanie możliwych sprawców, bo udana próba zrodzić może pokusę przekroczenia granic zabawy. Wymaga to zatem innego podejścia do budowania wersji śledczych i innych metod ich sprawdzania.

II. Już obecnie następuje „przeorientowanie" klasycznych włamywaczy, rozbójników i złodziei na wyłudzenia kredytów i towarów (mniejsze zagrożenie karne, mniejsza szansa wykrycia, mniejszy nakład pracy, bardziej oczywisty „zysk"). Za klika lat, po upowszechnieniu się umiejętności obsługi komputerów i znajomości ich programowania, zainteresują się oni zapewne wykorzystaniem bankowości elektronicznej do celów przestępczych.

[1] Swoistym sprawdzianem polskiego wymiaru sprawiedliwości w zakresie oceny dowodów elektronicznych będzie zapewne tzw. „Warez City", ujawniona i wykryta w lecie roku 2004 przez policję gorzowską. W sprawie tej działania przestępców skierowane były na kradzież intelektualna (filmy, utwory muzyczne, gry i programy komputerowe) i niszczenie danych. Działania operacyjne podjęte były w październiku 2003r. i obejmowały początkowo miejscowych hakerów („Gazeta Wyborcza" nr 198/2004, z dnia 24 sierpnia 2004r.).

[2] Por.: R. Jaworski, Nadużycia w elektronicznym obrocie bankowym i ich wyjaśnianie poprzez badanie śladów pamięciowych człowieka, „Bank i Kredyt" 2003, nr 7, s. 66-71.