

Przeszukanie i zatrzymanie sprzętu komputerowego jako procesowa forma uzyskiwania materiału dowodowego

mgr Andrzej Nowak

Uniwersytet Wrocławski

Część I.

Zarówno zatrzymanie, jak i przeszukanie są czynnościami procesowymi zmierzającymi do uzyskania dowodów w prowadzonym postępowaniu przygotowawczym. Działania te realizowane przez organy ścigania odnoszą się do miejsc, pomieszczeń, budynków czy też rzeczy, w których będą znajdować się informacje potwierdzające lub wykluczające popełnienie czynów karalnych. Uzyskane w toku zatrzymania lub przeszukania przedmioty po ich uznaniu przez organ prowadzący postępowanie będą stanowiły rzeczowe środki dowodowe niezbędne do prawidłowego osądzenia danych okoliczności.

Zarówno zatrzymanie rzeczy, jak i ich poszukiwanie w toku przeszukania zawierają się w pewnych ramach wyznaczonych nie tylko przez przepisy prawa, lecz również przez praktykę kryminalistyczną. W trochę inny sposób czynności te będą realizowane w odniesieniu do poszukiwania rzeczy - klasycznych przedmiotów przestępstwa, a inaczej będą wyglądały w odniesieniu do środowiska komputerowego, które niejednokrotnie może okazać się bardzo istotnym źródłem informacji procesowej.

Według S. Waltosia¹ w literaturze istnieje podstawowy podział dowodów z uwagi na sposób percepcji a tym samym zakres informacji, jaki dostarczają organowi procesowemu, co jednocześnie determinuje sposób uzyskiwania tych dowodów. Klasyfikacja ta wskazuje na istnienie dowodów zmysłowych, to znaczy takich, w których na dalszy plan odsunięta jest wartość intelektualna, a podstawą stają się spostrzeżenia zmysłowe właściwości miejsca lub rzeczy. Z kolei

¹ Stanisław Waltoś - "Proces karny - zarys systemu" - Warszawa 1995 , str.332.

dowody pojęciowe to takie dowody, które posiadają treść intelektualną, a ich badanie zmysłowe odsunięte jest na dalszy plan. Takimi dowodami będą niewątpliwie treści dokumentów w tym dokumentów elektronicznych², zeznania świadka czy też opinia biegłego. W tym schemacie klasyfikacja dowodów uzyskiwanych w wyniku czynności odnoszonych do sprzętu komputerowego będzie zdecydowanie plasowała się w kategorii dowodów intelektualnych. Bynajmniej niekiedy uzyskanie dowodów z urządzeń informatycznych może wiązać się z badaniami zmysłowymi (przy wskazaniu np. drukarki na której wytwarzane były fałszywe dokumenty).

Sprzęt komputerowy w obecnych czasach jest narzędziem spełniającym doniosłą rolę w procesie komunikacji międzyludzkiej, jak również w obrocie gospodarczym i prawnym.

Środowisko komputerowe rozwinęło się i obecnie pozwala kilkunastu milionom użytkowników na błyskawiczną wymianę informacji drogą elektroniczną. Pozwala ono również na zawieranie transakcji finansowych czy też handlowych między osobami fizycznymi i prawnymi. Komputeryzacja powoli zaczyna obejmować administrację państwową i samorządową, a jednym z postulatów na najbliższe lata jest umożliwienie załatwiania spraw urzędowych drogą elektroniczną bez zbędnych uciążliwości. Najbardziej wiarygodnym dowodem tych przemian może być chociażby wprowadzenie do obrotu prawnego podpisu elektronicznego i zrównanie jego znaczenia z podpisem własnoręcznym.

Można wspomnieć o nieocenionej roli komputerów przy kierowaniu funkcjonowaniem przedsiębiorstw niemal w każdej branży. Szereg programów umożliwia nie tylko prowadzenie biura, księgowości ale i również pozwala rozwiązywać wiele istotnych problemów związanych z daną gałęzią gospodarki. Można również wskazać na nieocenioną rolę globalnej sieci komputerowej - internetu jako narzędzia służącego do wymiany informacji, korespondencji, śledzenia bieżących wydarzeń, czy też kontaktów z osobami posiadającymi dostęp do komputera w różnych miejscach na całym świecie. Także nauka i realizowane w jej ramach różne projekty badawcze w obecnym czasie nie są zdolne uzyskać wiarygodnych i dokładnych wyników bez udziału tych maszyn.

Sytuacja, jaka się wytworzyła na przestrzeni ostatnich kilku lat nie mogła się ustrzec przed negatywnymi zjawiskami, które ugruntowały w praktyce organów wymiaru sprawiedliwości pojęcie przestępczości komputerowej oraz zakwalifikowały komputer jako narzędzie wykorzystywane do popełniania czynów karalnych.

² Art. 115 §14 kodeksu karnego: "Dokumentem jest każdy przedmiot lub 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.

W tym miejscu należy wskazać, iż według K. J. Jakubskiego³, przestępczość komputerowa obejmuje wszelkie zachowania przestępne związane z funkcjonowaniem elektronicznego przetwarzania danych, polegające zarówno na naruszaniu uprawnień do programu komputerowego, jak i godzące bezpośrednio w przetwarzaną informację,

Komputer obecnie stał się miejscem i środkiem wykorzystywanym do popełnienia szeregu przestępstw. W oparciu o technologię XXI wieku wytworzyły się nowe formy działań niezgodnych z prawem jak: hacking, cracking, phreaking, carding⁴, które funkcjonują w oparciu o opisywane środowisko. Komputer nie powinien być jednak kojarzony tylko i wyłącznie z przestępstwami komputerowymi sensu stricto. Należy podkreślić, iż obecnie "technologia układów scalonych" stanowi obecnie doskonałe narzędzie służące do popełniania szeregu przestępstw pospolitych jak np. oszustw, paserstwa, fałszerstw, gróźb karalnych, publikacji materiałów o treściach rasistowskich czy faszystowskich, pornografii, stręczycielstwa itp.

Szerokie, jeśli nie wręcz uniwersalne zastosowanie posiada środowisko komputerowe przy popełnianiu szeregu najpoważniejszych przestępstw gospodarczych, jak chociażby prania brudnych pieniędzy, czy nielegalnego transferowania środków płatniczych poza granice. Doskonałe warunki do przeprowadzania takich transakcji stwarza e-banking, czyli sieć usług bankowych realizowanych za pośrednictwem internetu. Zaletą komputerów w tym przypadku jest to, że za ich pomocą można dosłownie w ciągu kilkunastu sekund dokonać nielegalnych działań, które w normalnych okolicznościach wymagałyby nakładu czasu i odpowiednich środków (wystarczy porównać np. elektroniczny przelew bankowy z fizycznym przewozem pieniędzy w określone miejsce).

Wobec zaistniałych zagrożeń potrzeba usankcjonowania wiedzy prawniczej i kryminalistycznej w odniesieniu do czynności procesowych takich jak przeszukanie i zatrzymanie w odniesieniu do sprzętu komputerowego oraz danych w postaci elektronicznej. Należy więc odpowiedzieć na pytanie: Jak skutecznie przeprowadzić wskazane czynności procesowe, aby uzyskany w ich toku materiał został właściwie wykorzystany w toku prowadzonego postępowania karnego.

Zatrzymanie i przeszukanie w ujęciu karnoprosesowym.

W toku prowadzenia czynności procesowych zatrzymania i przeszukania obiektem zainteresowania ich realizatorów jest narzędzie, którym dopuszczono się przestępstwa, a także wszelkie informacje mogące uwiarygodnić zaistnienie okoliczności mogących mieć wpływ na

³ K. J. Jakubski "Przestępczość komputerowa - podział i definicja" - "Problemy kryminalistyki" 1997 nr 217, str. 31.

⁴ Nazwy te stosowane są w slangu informatycznym i potocznie określają: włamanie do systemów komputerowych (hacking), łamanie kodów chroniących oryginalne oprogramowanie przed nielegalnym kopiowaniem (cracking), oszustwa telekomunikacyjne z wykorzystaniem urządzeń elektronicznych (phreaking) oraz przestępstwa związane z wykorzystaniem kart kredytowych (carding).

przebieg postępowania karnego. Przeważnie w sprawach o przestępstwa popełniane przy użyciu komputera takim obiektem zainteresowania będzie sam komputer, choć niejednokrotnie okoliczności, jakie towarzyszą popełnieniu czynów, do których udowodnienia się zmierza, mogą determinować zainteresowanie elementami wyposażenia komputera - takimi jak: drukarka, skaner, nagrywarka płyt CD. Sprzęt taki po jego zatrzymaniu może zostać poddany badaniom na potrzeby procesowe. Przykładowo w odniesieniu do komputerowych drukarek atramentowych i laserowych istnieje metoda identyfikacji kryminalistycznej na podstawie cech znajdujących się na wydrukach⁵. Zatrzymanie drukarki może się okazać pomocne np. przy udowodnieniu fałszerstwa dokumentów. Istotne znaczenie procesowe będą mogły mieć ujawnione w toku czynności elektromagnetyczne nośniki w postaci: dysków twardych, płyt CD, dyskietek, taśm magnetycznych itp. Na ww. nośnikach będzie można odnaleźć dane lub dokumenty potwierdzające prowadzenie nielegalnej działalności. Ponadto źródłem informacji procesowej może stać się poczta elektroniczna, której zasoby niejednokrotnie ujawniają korespondencję istotną z punktu widzenia prowadzonego postępowania karnego.

Wiarygodnym materiałem dowodowym będzie w wielu przypadkach sprzęt komputerowy oraz nośniki komputerowe, które po ujawnieniu i zabezpieczeniu zostaną poddane szczegółowym oględzinom zmierzającym do ujawnienia znajdujących się na nich informacji. Jak słusznie wskazuje

A. Adamski⁶, sytuacja będzie jasna i klarowna w momencie wykonywania ww. czynności wobec jednego komputera lub kilku nośników ujawnionych w danym miejscu. Wtedy zasadnym będzie ich zatrzymanie i zabranie celem poddania szczegółowym badaniom przez biegłych lub specjalistów. Inaczej jednak wyglądać będzie sytuacja w odniesieniu do informatycznych systemów sieciowych, które łączą po kilkanaście lub kilkadziesiąt komputerów. W takim wypadku zatrzymywanie wszystkich urządzeń mogłoby naruszać zasadę proporcjonalności z art. 227 kpk. Dlatego też nowela do kodeksu postępowania karnego wprowadziła zapis 236a, który pozwala czynność zatrzymania

i przeszukania rozciągnąć również na środowisko komputerowe. Przedmiotem ww. czynności w takim przypadku będą dane w postaci elektronicznej niezależnie od miejsca ich przechowywania, przetwarzania, udostępniania lub przesyłania.

Niezależnie od sposobu prowadzenia ww. czynności niezbędną jest wiedza - czyli znajomość przepisów regulujących prowadzenie czynności zatrzymania i przeszukania

⁵ Tematykę tą szeroko opisuje Z. Laszczak "Identyfikacja komputerowych drukarek atramentowych", "Problemy Kryminalistyki 1995 nr 210 lub też M. Hryciuk, "Kryminalistyczna identyfikacja wybranych urządzeń kopiujących tj. komputerowych drukarek laserowych oraz kserokopiarek", "Problemy Kryminalistyki 1995 nr 208.

⁶ A. Adamski - "Prawo karne komputerowe" Warszawa 2000, str. 208.

Zasady ogólne prowadzenia zatrzymania i przeszukania.

Zarówno czynność procesowa zatrzymania jak i przeszukania charakteryzuje wiele czynników określających różne sposoby praktycznej realizacji tych działań. Niemniej jednak istnieje kilka cech wspólnych dla obu czynności, które można określić mianem ogólnych zasad, według których realizowane powinno być uzyskiwanie materiałów dowodowych.

Pierwsza z zasad wynika z art. 235 kpk, który wskazuje na jakim etapie postępowania karnego, które organy mają prawo czynności te inicjować. Wskazuje on w szczególności, iż inicjowanie czynności procesowych zatrzymania i przeszukania na etapie postępowania przygotowawczego należeć powinno do prokuratora, natomiast w postępowaniu sądowym do właściwego sądu o ile przepisy nie będą stanowiły inaczej. Ww. zasada rozgraniczenia kompetencji nie określa bynajmniej ostatecznych granic dla działań prokuratora i sądu, ale jak to wskazuje W. Grzeszczyk⁷ wskazuje w jakim stadium procesu karnego jaki organ ma prawo te czynności podejmować.

Z kolei art. 227 kpk wyraża kolejną zasadę, z której wynika, iż czynność przeszukania i zatrzymania powinny być dokonywane w możliwie jak najmniej szkodliwy i dolegliwy sposób a także z poszanowaniem godności osób, których te czynności będą dotyczyły. Zasada ta - nazywana zasadą zachowania umiaru - jest odzwierciedleniem konstytucyjnej normy z art. 30, dotyczącej poszanowania godności człowieka, art. 47 dotyczącego ochrony życia prywatnego i art. 40 zakazującego niehumanitarnego lub poniżającego traktowania⁸. Przepis art. 227 kpk nakreśla pewne ramy prowadzenia czynności procesowych, które sprowadzają zbieranie materiału procesowego do działań stricte podporządkowanych toczącemu się postępowaniu i nie wykraczających poza podstawowe cele, jakie zamierza się w nim osiągnąć.

Również jako zasadę można uznać obowiązek każdorazowego dokumentowania przeprowadzonej czynności w formie protokołu. Dokument taki sporządza się zarówno po przeprowadzeniu zatrzymania rzeczy lub też przeszukania i zawierać on powinien podstawowe dane związane z prowadzoną czynnością. Wyjątkiem od tej zasady jest przepis art. 217 par 3, który wskazuje, że jeśli rzecz zabezpieczona w toku zatrzymania załączona zostanie do akt sprawy, wówczas protokołu można nie sporządzać. W takim wypadku jedynym dokumentem będzie pokwitowanie zatrzymania rzeczy (art. 228 kpk).

Zasadą jest również prawo do wniesienia zażalenia przez osobę, która była stroną wykonywanej przez uprawnione organy czynności procesowej. Podmiot taki w świetle art. 236 ma

⁷ W. Grzeszczyk - Organy uprawnione do podejmowania decyzji w przedmiocie dowodów rzeczowych w postępowaniu przygotowawczym - "Prokuratura i Prawo" 2001/2/163.

⁸ P. Hofmański, E. Sadzik, K. Zgrzyk - "Kodeks postępowania karnego - Komentarz" - Tom I, Warszawa 1999;

prawo do wniesienia zażalenia na wykonywaną czynność (termin 7 dni) jeżeli uzna, że w toku jej wykonywania zostały naruszone prawa, w tym prawo określone w art. 227 kpk.

Zatrzymanie.

Kodeks postępowania karnego zatrzymanie sprzętu komputerowego, czy też danych w postaci elektronicznej (w aspekcie art. 236a kpk) traktuje tak samo jak zatrzymanie każdej rzeczy mogącej stanowić dowód w toczącym się postępowaniu. Art. 217 kpk wskazuje na podstawę zatrzymania, którą będzie żądanie sądu, prokuratora, a w wypadkach nie cierpiących zwłoki - żądanie Policji lub innych uprawnionych organów. W przypadku, kiedy organy realizujące czynność zatrzymania działają w warunkach nie cierpiących zwłoki, wówczas osoba wydająca rzecz, lub osoba której rzecz jest odbierana musi zostać pouczone o prawie złożenia w trybie niezwłocznym wniosku o zatwierdzenie tej czynności przez sąd lub prokuraturę. W przypadku złożenia takiego wniosku organ prowadzący postępowanie związany jest 14 dniowym terminem wydania i doręczenia ww. osobie wniosku o zatwierdzenie zatrzymania rzeczy.

Zatrzymanie rzeczy dotyczy każdej osoby we władztwie której żądane przedmioty się znajdują. Nie będzie w tym przypadku znaczenia miała okoliczność, że dana osoba fizyczna czy prawna nie jest właścicielem tej rzeczy, czy też posiada ją nielegalnie. Nie będzie także znaczenia miał stosunek podmiotu do stron postępowania.

Istotnym elementem procedury zatrzymania jest zakomunikowanie żądania wydania rzeczy osobie, co do której zachodzi przypuszczenie iż może ona być w posiadaniu szukanych przedmiotów. W przypadku, kiedy organ prowadzący czynność spotka się z odmową wydania rzeczy, może wówczas na podstawie art. 217 par. 5 przeprowadzić ich odebranie. Czynność procesowa w takiej sytuacji może (ale nie musi) być poprzedzona przeszukaniem. Konsekwencje w stosunku do osób, które odmawiają wydania rzeczy mogą polegać na zastosowaniu w trybie art. 287 kpk kary pieniężnej lub też kary 30 - dniowego aresztu. Sankcje te nie będą mogły znaleźć zastosowania w stosunku do stron postępowania, ich obrońców, pełnomocników oraz podmiotów, które z mocy prawa posiadają możliwość uchylenia się od składania zeznań (np. osoby bliskie w stosunku do podejrzanego).

Czynność zatrzymania rzeczy wymaga stosownego odzwierciedlenia w aktach sprawy. Formalnym dokumentem potwierdzającym przeprowadzenie zatrzymania lub też odebrania przedmiotów jest protokół. Protokół powinien przede wszystkim zawierać oznaczenie sprawy, dane osób biorących udział w czynności oraz czas rozpoczęcia i zakończenia czynności. Wskazana również powinna być podstawa przeprowadzenia zatrzymania. Wyjątkiem od tej reguły jest art. 217 par 3 w myśl którego wymóg sporządzenia protokołu może nie dotyczyć sytuacji, w której

zatrzymane rzeczy zostaną dołączone do akt sprawy. W takim przypadku jednak należy wydać osobie zainteresowanej pokwitowanie.

Sposób postępowania z danymi oraz sprzętem komputerowym określony został przez przepis art. 228, który w jednakowy sposób reguluje ww. zagadnienie przy zatrzymaniu jak i przeszukaniu. Dlatego też zostanie on omówiony w części poświęconej czynności przeszukania.

Przeszukanie.

Przeszukanie jest czynnością procesową, która zmierza do odnalezienia rzeczy mogących stanowić dowód w sprawie, lub rzeczy podlegających zajęciu w toku prowadzonego postępowania. Przeszukanie może być również przeprowadzone w celu odnalezienia, zatrzymania i doprowadzenia osoby podejrzaney. Mając na uwadze tematykę opracowania chodzić będzie przede wszystkim o przeszukanie zmierzające do ujawnienia i zabezpieczenia sprzętu komputerowego oraz danych w postaci elektronicznej dla potrzeb toczącego się postępowania. Biorąc pod uwagę możliwości lokalizacji sprzętu oraz danych informatycznych można mówić o poszukiwaniu materiału dowodowego znajdującego się w pomieszczeniach, przy osobach (np. dyskiety) bądź w systemach informatycznych komputerów.

Realizatorem ww. czynności może być prokurator, sąd bądź na polecenie ww. Policja lub inny organ ścigania. Tak jak przy zatrzymaniu rzeczy, można w wypadkach wymagających niezwłocznego działania przystąpić do wykonania tej czynności bez stosownego postanowienia, jednakże po uprzednim okazaniu nakazu kierownika jednostki lub legitymacji służbowej. Po zakończeniu czynności procesowej organ musi się zwrócić do sądu lub prokuratora o jej zatwierdzenie. W przypadku nie dochowania tego obowiązku wszystkie przedmioty zatrzymane w toku przeszukania będą podlegały zwrotowi osobom, u których zostały ujawnione. Ponadto na żądanie osoby, u której dokonywane było przeszukanie w terminie 7 dni należy doręczyć postanowienie o zatwierdzeniu czynności przez instytucję prowadzącą postępowanie.

W odniesieniu do przeszukania pomieszczeń zamieszkałych przepis art. 221 kpk określa ramy czasowe dla prowadzenia tej czynności. Przeszukania nie można dokonywać w tych pomieszczeniach w godz. od 22:00 do 6:00. Ograniczenie to nie dotyczy lokali, miejsc dostępnych dla nieokreślonej liczby osób oraz pomieszczeń służących wyłącznie do przechowywania rzeczy. Przed przystąpieniem do przeszukania należy zakomunikować osobom u których ma być dokonane przeszukanie o celu czynności a następnie wezwać do wydania poszukiwanych rzeczy. W przeszukaniu powinna czynny udział brać osoba u której jest ono dokonywane. Ewentualnie w czynności procesowej może brać udział osoba przybrana przez przeszukującego lub też osoba przybrana przez przeszukiwanego. Jeżeli w lokalu nie ma jego gospodarza, należy wezwać

do obecności przy przeszukaniu dorosłego domownika, a w przypadku braku takiego - osobę zamieszkujejącą w sąsiedztwie. W przypadku przeszukania prowadzonego na terenie instytucji publicznej organ prowadzący czynność ma obowiązek zawiadomienia kierownika tej jednostki, a w przypadku jego braku zastępcy bądź przedstawiciela organu nadrzędnego a następnie dopuścić te osoby do udziału przy przeszukaniu. W odniesieniu do przeszukania na terenie jednostek wojskowych organ procesowy jest zobligowany do zawiadomienia i dopuszczenia do udziału w procedurze dowódców tych jednostek.

Czynność procesowa przeszukania za każdym razem musi być udokumentowana w formie protokołu. W sporządzanym protokole należy oznaczyć przede wszystkim numer sprawy, godziny rozpoczęcia i zakończenia czynności, podstawę przeszukania oraz spis i w miarę dokładny opis rzeczy zatrzymanych w trakcie przeszukania. W przypadku gdy wspomnianą czynność prowadzi się w warunkach nie cierpiących zwłoki, w protokole powinna zostać ujęta wzmianka odnośnie pouczenia strony o prawie zażądania pisemnej informacji odnośnie doręczenia postanowienia o zatwierdzeniu czynności przeszukania przez właściwy organ procesowy.

Po sporządzeniu protokołu prowadzący czynność musi zdecydować o sposobie postąpienia z ujawnionymi przedmiotami. Wiązać się to będzie z ich zabranieniem lub pozostawieniem na przechowanie osobie godnej zaufania za pokwitowaniem. Przedtem jednak wskazane przez przepis art. 228 jest dokonanie spisu lub opisu ujawnionych rzeczy oraz ewentualnych ich oględzin.

Specyficzny sposób postępowania z dokumentacją objętą tajemnicą określa przepis art. 225 kpk, który określa sposób zabezpieczania dokumentacji o szczególnym znaczeniu. Przepis ten należy odnosić również do dokumentów elektronicznych, gdyż one w szczególnych sytuacjach, wskazanych w przepisach też będą musiały zostać w odpowiedni sposób zabezpieczone. Przepis ten wskazuje, że jeśli w trakcie zatrzymania lub przeszukania osoby u których są one przeprowadzane oświadczą, że dane dokumenty zawierają tajemnicę państwową, służbową, zawodową, czy też ma charakter osobisty, wówczas prowadzący przeszukanie powinni taki dokument zabezpieczyć w opieczętowanym opakowaniu i bez zapoznawania się z jego treścią przekazuje organowi prowadzącemu postępowanie. Taki sam sposób postępowania dotyczy ujawnionej w trakcie czynności dokumentacji psychiatrycznej. Wyjątkiem od tej normy będą sytuacje w których posiadaczem dokumentów oklauzulowanych jako tajemnica zawodowa, służbowa lub inna chroniona ustawą jest osoba podejrzewana o popełnienie przestępstwa. Podobnie będzie sytuacja wyglądała w odniesieniu do dokumentacji osobistej podejrzanego. Przepis art. 225 kpk reguluje także sytuacje, kiedy w toku wykonywania czynności znaleziona zostanie dokumentacja związana z wykonywaniem funkcji obrońcy w procesie karnym. Podstawą do uznania takiej dokumentacji za

związaną z obroną jest oświadczenie złożone wobec organu prowadzącego czynność przez obrońcę, lub osobę wobec u której dokumenty zostały znalezione. Natomiast w przypadku kiedy istnieją jakiegokolwiek wątpliwości co do oświadczenia osoby innej niż obrońca, wówczas dokumenty te się zabezpiecza oraz przekazuje sądowi celem oceny ich przydatności dla celów prowadzonego postępowania i w odniesieniu do dalszego dysponowania dokumentami wydaje dalsze decyzje.

Zatrzymanie i przeszukanie w aspekcie art. 236 a kpk.

Przeszukanie i zatrzymanie dokonywane w odniesieniu do systemów komputerowych, nośników i zasobów poczty e-mail uregulowała nowela do kodeksu postępowania karnego z dnia 10.01.2003 r. (Dz. U. Nr 17, poz. 155), która weszła w życie z dniem 01.07.2003 r. Wprowadziła ona między innymi do rozdziału 25 kpk traktującego o tematyce zatrzymania rzeczy i przeszukania zapis art. 236 a, którego treść brzmi: "Przepisy działu niniejszego stosuje się odpowiednio do dysponenta i użytkownika systemu informatycznego w zakresie danych przechowywanych w tym systemie lub na nośniku znajdującym się w jego dyspozycji lub użytkowaniu, w tym korespondencji przesłanej drogą elektroniczną."

Przedmiotem prowadzonych czynności procesowych są dane w postaci elektronicznej, które mogą być przechowywane bądź w systemie komputera, na nośniku informacji lub też mogą też wchodzić w skład zasobów poczty elektronicznej.

Adresatami normy określonej w przepisie art. 236a kpk będą zarówno użytkownicy systemów informatycznych, nośników czy też zasobów poczty elektronicznej jak również i ich dysponenci. tak więc do bycia stroną prowadzonej czynności procesowej nie jest wymagany fakt bezpośredniego korzystania z danych elektronicznych, wystarczy również sam fakt posiadania informacji w formie elektronicznej.

Analizując zakres zastosowanego przez ustawodawcę pojęcia "system informatyczny" - należy przez to rozumieć funkcjonujący w tym otoczeniu zespół (na ogół liczny) elementów powiązanych ze sobą różnorodnymi zależnościami, który istnienie ma na celu spełnienie określonych funkcji⁹.

Najbardziej podstawowym zbiorem opisywanych części będzie system operacyjny komputera, który jest programem działającym jako pośrednik pomiędzy użytkownikiem komputera a sprzętem komputerowym. Jego zadaniem jest stworzenie bezpiecznego i niezawodnego środowiska, w którym istnieje możliwość wydajnej i efektywnej obsługi programów. W praktyce możemy wskazać na kilka systemów operacyjnych, w tym m.in.: systemy z graficznym interfejsem

⁹ Na podstawie Z. Płoska - "Słownik encyklopedyczny informatyka" Wyd. Europa 1999 oraz wirtualnej encyklopedii www.wiem.onet.pl.

użytkownika, np. WINDOWS, systemy z interfejsem tekstowym, np. MS DOS lub UNIX, czy też różnorodne odmiany systemów wzorcowych (np. systemy uniksowe).

Do systemów informatycznych zaliczamy także bazy danych, czyli rodzaj komputerowego zbioru kartotek, magazynu danych o określonej budowie. Baza danych jest modelowym ujęciem fragmentu rzeczywistości będącego przedmiotem zainteresowania osób, instytucji, organizacji, firm, zakładów, itp., reprezentującym fakty dotyczące tej rzeczywistości w formie umożliwiającej ich przetwarzanie w komputerze¹⁰. W obecnej rzeczywistości praktycznie nie ma instytucji, zakładu pracy czy też firmy bez bazy danych, która ewidencjonuje np. spisy środków trwałych, faktur zakupu i sprzedaży, spisy towarów, spisy pracowników czy też innych rzeczy w zależności od potrzeb danego podmiotu.

W pojęciu "systemy informatyczne" zawierają się także sieciowe systemy operacyjne, w których komputery połączone są w sieć informatyczną na zasadzie klient - serwer. Najogólniej mówiąc sieć komputerowa jest zbiorem komputerów połączonych między sobą w celu udostępnienia odległym użytkownikom zarówno zasobów mocy obliczeniowej poszczególnych systemów, pojemności danych jak i posiadanych przez nie urządzeń zewnętrznych i wewnętrznych. Sieci dają niezwykle duże możliwości wymiany, przetwarzania i gromadzenia informacji. Przykładem takich systemów może być: LINUX, UNIX, czy NOVELL NETWARE. Niezależnie od tego każdy z komputerów podłączonych do sieci korzysta ze swojego systemu operacyjnego.

Ponadto dysponent czy też użytkownik systemu komputerowego są zobowiązani do udostępnienia organom procesowym posiadanych nośników danych czyli urządzeń, na których można zapisywać, bądź odtwarzać informacje¹¹, np. twardy dysk, dyskietka, nośnik CD, taśma stream, dysk ZIP. Podobna sytuacja ma miejsce w przypadku poczty elektronicznej czyli systemu polegającego na przekazywaniu listów elektronicznych - wiadomości tekstowych, dodatkowo opatrzonych adresem email odbiorcy i nadawcy. Oprócz wiadomości tekstowych listy mogą zawierać pliki dowolnych formatów (obrazy dźwięki, dane) przesyłane jako załączniki. Z punktu widzenia art. 236 a możliwość uzyskania wglądu do zasobów poczty email będzie dotyczyła wszystkich informacji, jakie zostały nadesłane, wysłane, lub które są przechowywane w zasobach należących do użytkownika bądź dysponenta systemu komputerowego.

Omawiana regulacja prawna dzięki swojej konstrukcji zapewnia efektywność procesową zatrzymania i przeszukania w sprawach karnych wiążących się z wykorzystaniem środowiska komputerowego. Regulacja ta daje organowi procesowemu możliwość uzyskania bezpośredniego

¹⁰ Na podstawie Z. Płoska - "Słownik encyklopedyczny informatyka" Wyd. Europa 1999 oraz wirtualnej encyklopedii www.wiem.onet.pl.

¹¹ Na podstawie "Słownika Encyklopedycznego Edukacja Obywatelska" Wydawnictwa Europa. Autorzy: Roman Smolski, Marek Smolski, Elżbieta Helena Stadtmüller. ISBN 83-85336-31-1. Rok wydania 1999.

dostępu do danych przechowywanych przez użytkownika czy też dysponenta sprzętu komputerowego, zgromadzonych na tym komputerze lub też na nośnikach elektronicznych oraz poczty elektronicznej. Możliwość bezpośredniego zbadania zasobów informatycznych do tej pory była niemożliwa do realizacji przy klasycznym przeszukaniu pomieszczeń czy też osób. Nie istniała do tej pory prawna podstawa do monitorowania zasobów systemowych, ani też do wglądu do miejsc, w których magazynowane i przetwarzane są dane w postaci elektronicznej. W ramach ww. czynności można było jedynie zatrzymać sprzęt komputerowy jako rzecz bez możliwości niezwłocznego udokumentowania procesowego jego zawartości.

Możliwym jest nadal wykonywanie tych czynności celem odnalezienia i zabezpieczenia sprzętu komputerowego, lecz ponadto w szczególnych przypadkach uzasadnionych przedmiotem toczącego się procesu można dokonać monitoringu zasobów systemowych, danych zawartych na nośnikach oraz informacji zawartych w poczcie elektronicznej, co pozwala na uzyskanie wielu cennych informacji w krótkim czasie.

Regulacja prawna tematyki procesowego uzyskiwania dowodów ze środowiska komputerowego w naszym kraju stanowi realizację części norm ustanowionych aktami prawa europejskiego. Kwestia skutecznej walki z przestępczością komputerową została omówiona szczegółowo w Zaleceniach Rady Europy Nr R (95) 13 dotyczących "Problemów karnoprosesowych związanych z nowoczesną technologią przetwarzania informacji"¹². Zagadnienia ujęte w niniejszej regulacji znalazły swoje odniesienie w Europejskiej Konwencji w Sprawie Cyberprzestępczości z dnia 23.11.2001 roku¹³. Obydwa akty traktują czynności zatrzymania i przeszukania jako podstawowe narzędzia gromadzenia materiału dowodowego w sprawach związanych z przestępstwami popełnianymi przy wykorzystaniu komputera. W związku z tym stwierdzono, iż niezbędne będzie odniesienie warunków dopuszczalności tradycyjnego zatrzymania i przeszukania do działań procesowych wobec systemów komputerowych i znajdujących się w nich danych. Ponadto za istotny warunek uznano zrównanie w procedurze karnej klasyczną dokumentację z dokumentacją elektroniczną mając na uwadze zmiany jakie dokonują się w systemie komunikacji międzyludzkiej, a w szczególności powszechnej informatyzacji. Europejska Konwencja w Sprawie Cyberprzestępczości postuluje ponadto wprowadzenie nowych form czynności procesowych, które mają zmierzać do bardziej sprawnego realizowania podstawowych celów procedury karnej. Tymi nowymi czynnościami procesowymi są:

- Przyspieszone zabezpieczenie przechowywanych danych komputerowych - czynność mająca polegać na zobowiązaniu dysponenta określonych danych do niezwłocznego zabezpieczenia

¹² <http://cm.coe.int/ta/rec/1995/95r13.htm>

¹³ <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>

danych gromadzonych w zarządzanych zasobach. Zabezpieczenie takie ma polegać na zapewnieniu integralności i nienaruszalności danych do czasu zaznajomienia się z nimi przez organy procesowe. Zobowiązanie takie ma dawać właściwym organom czas na uzyskanie przewidzianego prawem zezwolenia na dostęp do tych danych. Czynność ta w przypadku kiedy dotyczy transmisji danych może zobowiązywać do udostępnienia informacji niezbędnych do identyfikacji dostawców usług komunikacyjnych co ma pozwolić na przesłedzenie drogi danego przekazu komputerowego.

- Nakaz przedstawienia danych komputerowych - odnosi się do sytuacji w której organ procesowy może zobowiązać osobę posiadającą w swojej dyspozycji określone dane do ich przedstawienia niezależnie od sposobu ich przechowywania. W odniesieniu do dostawców usług komunikacyjnych nakaz ten może oznaczać wskazanie szczegółowych danych dotyczących abonenta korzystającego z określonych usług. Potrzeba uzyskania takich danych będzie musiała wynikać ze zgromadzonego materiału procesowego i być ściśle określona do konkretnych osób i zdarzeń.

- Bieżące gromadzenie danych ruchowych - polega na wyposażeniu organów procesowych w uprawnienia do zbierania lub zapisywania w czasie rzeczywistym informacji związanych z transmisją danych pomiędzy określonymi podmiotami działającymi w danych systemach informatycznych. Czynność ta może być realizowana jedynie na terytorium danego państwa i nie obejmuje swoim zakresem transmisji poza tym terenem.

- Przechwytywanie w czasie rzeczywistym danych dotyczących komunikowanej treści - związane jest z umożliwieniem dostępu do treści informacji przekazywanych w formie elektronicznej pomiędzy osobami co do których może istnieć podejrzenie uczestnictwa w szczególnie szkodliwych przestępstwach. Realizacja takiej czynności polegać ma na przechwytywaniu w czasie rzeczywistym tych informacji a następnie ich zapisywaniu w sposób umożliwiający późniejsze odtworzenie i przeanalizowanie na drodze procesowej.

Nadmienić należy, że zarówno wskazane wyżej Zalecenie Rady Europy, jak i Konwencja w Sprawie Cyberprzestępczości postulują wyposażenie organów ścigania w uprawnienia do prowadzenia tzw. zdalnego przeszukania systemów komputerowych za pomocą sieci informatycznych¹⁴. Czynność taka odbywa się inaczej niż przy klasycznym przeszukaniu, bez uprzedniego zawiadomienia ani też udziału strony wobec której czynność jest prowadzona. Zdalne przeszukanie zostało już prawnie uregulowane w innych krajach, np. w Holandii i polega ono na penetracji systemu informatycznego, zbieraniu i zapisywaniu ujawnionych w nim danych pod kontrolą organu procesowego. Czynność taka może być podejmowana w przypadkach kiedy zwłoka

¹⁴ Szerzej na ten temat A. Adamski - "Prawo karne komputerowe" Warszawa 2000 oraz A. Adamski - "Przestępczość w cyberprzestrzeni..." - Toruń 2001.

w działaniu mogłaby uniemożliwić uzyskanie danych na drodze zwykłego przeszukania. Taka forma czynności procesowej, choć skuteczna jednak w naszym kraju nie posiada odpowiednich podstaw prawnych do swojego funkcjonowania. Dlatego też nie można tej metody procesowego uzyskiwania dowodów stosować, gdyż za podstawę niezbędną do prawidłowego przeprowadzenia omawianej czynności procesowej uznaje się m.in. obowiązek zawiadomienia o przeszukaniu podmiotów u których taka czynność ma zostać przeprowadzona, a także wymóg obecności podczas prowadzenia czynności przez organy procesowe, co wiąże się z możliwością zgłoszenia do protokołu ewentualnych zastrzeżeń co do sposobu oraz formy przeszukania.

BIBLIOGRAFIA

Książki:

- Andrzej Adamski - "Prawo karne komputerowe" - Warszawa 2000;
- Andrzej Adamski - "Przestępczość w cyberprzestrzeni. Karne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy" - Toruń 2001;
- Zbigniew Czczot, Tadeusz Tomaszewski - "Kryminalistyka ogólna" - Toruń 1996;
- Zdzisław Uniszewski - "Przeszukanie. problematyka kryminalistyczna" - Warszawa 2000;
- P. Hofmański, E. Sadzik, K. Zgryzek - "Kodeks postępowania karnego - Komentarz" - Tom I, Warszawa 1999;
- Kodeks karny, Kodeks postępowania karnego, Kodeks karny wykonawczy - teksty jednolite wraz z indeksem rzeczowym" - Warszawa 2003;
- Stanisław Waltoś - "Proces karny - zarys systemu" - Warszawa 1995
- Z. Płoski - "Słownik encyklopedyczny informatyka" - Wrocław 1999;
- R. Smolski, M. Smolski, E. Stadtmüller "Słownik Encyklopedyczny Edukacja Obywatelska" - Wrocław 1999;
- Jacek Gołaczyński (red.) - "Prawne i ekonomiczne aspekty komunikacji elektronicznej" - Warszawa 2003;

Artykuły:

- K. J. Jakubski "Przestępczość komputerowa - podział i definicja" - "Problemy kryminalistyki" 1997 nr 217;

- W. Grzeszczyk - Organy uprawnione do podejmowania decyzji w przedmiocie dowodów rzeczowych w postępowaniu przygotowawczym - "Prokuratura i Prawo" 2001/2/163;
- M. Białkowski - "Haking międzynarodowy" - Gazeta Sądowa, Styczeń 2002;
- G. Kędzierska - "Kryminalistyczne badania informatyczne" - artykuł opublikowany pod adresem: http://www.wspol.edu.pl/per/pbs/1-2/ibs_1i2_99/a11_1-2_99.html;
- A. Adamski - "Podstawy prawne zatrzymania sprzętu komputerowego przez Policję w sprawach o piractwo komputerowe" - konspekt wykładu wygłoszonego na seminarium "VI edycja Prawo komputerowe" - Centrum Promocji Informatyki, Warszawa, 13 lutego 2002 r. : http://www.law.uni.torun.pl/KOMP-LEX/Jabl_3.pdf.

Inne:

- Encyklopedia wirtualna www.wiem.onet.pl;
- Zalecenie Rady Europy Nr R (95) 13 - <http://cm.coe.int/ta/rec/1995/95r13.htm>
- Europejska Konwencja w Sprawie Cyberprzestępczości - <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>