Filip Radoniewicz*

Przeszukanie systemów informatycznych oraz informatycznych nośników danych w kodeksie postępowania karnego

Streszczenie

Tematem niniejszego opracowania jest czynność operacyjna polegająca na przeszukiwaniu systemów informatycznych (zarówno połączonych z innymi systemami informatycznymi, jak i stanowiącymi samodzielne jednostki), „urządzeń zawierających dane" oraz (informatycznych) nośników danych. Problematyka ta została uregulowana poprzez odesłanie zawarte w art. 236a kodeksu postępowania karnego z 1997 roku do przepisów rozdziału 25 „Zatrzymanie rzeczy. Przeszukanie" przewidującego odpowiednie ich stosowanie do dysponenta i użytkownika urządzenia zawierającego dane informatyczne lub systemu informatycznego w zakresie danych przechowywanych w tym urządzeniu lub systemie albo na nośniku znajdującym się w jego dyspozycji lub użytkowaniu, w tym korespondencji przesyłanej pocztą elektroniczną.

Słowa kluczowe: cyberprzestępczość, przeszukanie, zabezpieczenie dowodów, chmura obliczeniowa, konwencja o cyberprzestępczości

* Dr Filip Radoniewicz, adiunkt w Katedrze Prawa Cyberbezpieczeństwa i Nowych Technologii, Instytut Prawa Akademii Sztuki Wojennej, ekspert w Akademickim Centrum Polityki Cyberbezpieczeństwa Akademii Sztuki Wojennej, e-mail: f.radoniewicz@akademia.mil.pl, ORCID: 0000-0002-7917-4059.

Tematem niniejszego opracowania jest czynność operacyjna polegająca na przeszukiwaniu cyberprzestrzeni, tj. powiązanych ze sobą systemów informatycznych, a także samodzielnych systemów informatycznych (niewymieniających danych z innymi systemami) oraz informatycznych nośników danych w celu uzyskania danych informatycznych mających wartość dowodową. Bezdyskusyjnie należy przyjąć, że jest to materia świeża, nieuregulowana w pełni w przepisach prawnych, które – jak zwykle zresztą – nie nadążają za zmianami w rzeczywistości, zwłaszcza że w takiej dziedzinie jak informatyka i teleinformatyka następują one wyjątkowo szybko. Nie ulega wątpliwości, że przed przystąpieniem do omówienia tejże problematyki należy wyjaśnić podstawowe pojęcia, tj.: „system komputerowy", „system informatyczny", „dane komputerowe", „dane informatyczne", „cyberprzestrzeń", „hosting", „chmura obliczeniowa" oraz „informatyczny nośnik danych".

Zgodnie z art. 1 lit. a Konwencji o cyberprzestępczości[1] systemem informatycznym[2] jest każde urządzenie lub grupa wzajemnie połączonych lub

1 Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r., Dz.U. 2015, poz. 728. Polska podpisała Konwencję jako jedno z pierwszych państw – w momencie otwarcia do podpisu. Ponadto uczestniczyła w pracach nad jej treścią. Pierwsza nowelizacja, mająca dostosować polskie przepisy do jej postanowień, została przeprowadzona w 2004 r. ustawą z dnia 18 marca 2004 r. o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz ustawy – Kodeks wykroczeń, Dz.U. 2004, nr 69, poz. 626, ale ratyfikacja nastąpiła dopiero w 2015 r.

2 Interpretacja pojęcia „system komputerowy" (podobnie jak później wprowadzonego terminu „system informatyczny") w zasadzie od momentu pojawienia się go w kodeksie karnym (ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, t.j., Dz.U. 2021, poz. 2345, z późn. zm.) rodziła problemy (zob. szerzej np.: F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016, s. 275–278; M. Siwicki, *Cyberprzestępczość*, Warszawa 2013, Legalis), które dodatkowo przybrały na sile po ratyfikacji przez Polskę Konwencji o cyberprzestępczości. Pojęcie „system komputerowy" zostało wprowadzone do kodeksu karnego w 2004 r. w związku z podpisaniem przez Polskę Konwencji o cyberprzestępczości. Pojęcie „system informatyczny zostało dodane nowelizacją z 2008 r., związaną z implementacją decyzji ramowej Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne (Dz. Urz. UE 2005, L 69/67), dokonaną ustawą z dnia 24 października 2008 r. o zmianie ustawy – Kodeks karny i niektórych innych ustaw (Dz.U. 2008, nr 214, poz. 1344). Wskazane byłoby rozumienie tegoż terminu zgodnie z definicją zawartą w tym akcie oraz w zastępującej go dyrektywie Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne i uchylającej decyzję ramową Rady 2005/222/WSiSW (Dz. Urz. UE 2013, L 218/8). Pojęcie „system informatyczny" – mimo podobieństwa do definicji z Konwencji o cyberprzestępczości (definicja zawarta w art. 2 lit. a dyrektywy 2013/40 brzmi: „system informatyczny oznacza urządzenie lub grupę wzajemnie połączonych lub powiązanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, dokonuje automatycznego przetwarzania danych komputerowych, jak również danych komputerowych przechowywanych, przetwarzanych, odzyskanych lub

powiązanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, wykonuje automatyczne przetwarzanie danych.

Zgodnie z „Explanatory Report"[3] system informatyczny jest to urządzenie, na które składa się sprzęt (*hardware*) i oprogramowanie (*software*). Sprzęt to w szczególności urządzenia wejścia/wyjścia oraz magazynujące dane. Programem komputerowym jest zestaw instrukcji, które mogą być wykonane w celu osiągnięcia zamierzonego rezultatu przez system informatyczny. System komputerowy zazwyczaj tworzy wiele urządzeń. Niezbędnym elementem jest procesor. Pozostałymi nieobligatoryjnymi składnikami są urządzenia peryferyjne, czyli urządzenia, które wykonują określone zadania, wchodząc w interakcje z jednostką centralną (np. monitor, drukarka, napęd DVD, urządzenie magazynujące dane). Systemem informatycznym zgodnie z Konwencją o cyberprzestępczości będzie zatem telefon komórkowy, dekoder, a przede wszystkim to, co potocznie rozumie się jako samodzielny komputer (*personal computer* – PC), czyli pojedynczy host. Co najmniej dwa niezależne, powiązane ze sobą (tj. zdolne do wymieniania między sobą danych) systemy informatyczne będą stanowiły sieć. Dane w jej ramach mogą być przesyłane przez różne media:

przekazanych przez to urządzenie lub tę grupę urządzeń, w celach ich eksploatacji, użycia, ochrony lub utrzymania") – ma szerszy zakres przedmiotowy, gdyż może oznaczać zarówno urządzenie przetwarzające dane komputerowe, jak i zespół takich urządzeń, czyli sieć (np. lokalną). Tłumacząc tekst Konwencji o cyberprzestępczości, popełniono wiele błędów. Jednym z nich jest przetłumaczenie pojęcia „system komputerowy" (*computer system*) jako system informatyczny. Zakres przedmiotowy pojęcia „system komputerowy" z Konwencji jest – jak wskazano wyżej – węższy niż pojęcia „system informatyczny" z dyrektywy 2013/40. Powoduje to wątpliwości co do zakresu pojęcia „system informatyczny" na gruncie kodeksu karnego. Mimo że Konwencja o cyberprzestępczości w momencie jej ratyfikacji stała się częścią porządku prawnego, definicji systemu informatycznego (komputerowego) nie można stosować bezpośrednio, ze względu właśnie na omawiane problemy. Istniejący zamęt potęguje to, że w tłumaczeniu definicji pojęcia „dane informatyczne" w art. 2 lit. b Konwencji (*computer data* przetłumaczonych jako „dane informatyczne") posłużono się pojęciem systemu komputerowego („dane informatyczne oznaczają dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny"). Ponadto terminu „system komputerowy" użyto w tłumaczeniu protokołu dodatkowego do Konwencji Rady Europy o cyberprzestępczości dotyczącego penalizacji czynów o charakterze rasistowskim lub ksenofobicznym popełnionych przy użyciu systemów komputerowych z dnia 28 stycznia 2003 r (Dz.U. 2015, poz. 730). Wydaje się, że w przypadku omawianej regulacji należy przyjąć, że ustawodawca posłużył się pojęciem „system informatyczny" w znaczeniu węższym, tj. w takim, w jakim użył go, błędnie tłumacząc pojęcie *computer system* w Konwencji o cyberprzestępczości.

3 *Explanatory Report to Convention on Cybercrime*, Budapest, 23 IX 2001, pkt 23, 24, https://rm.coe.int/16800cce5b [dostęp: 1.04.2022].

przewodowo (kable) i bezprzewodowo (np. drogą radiową). Może mieć różny zasięg terytorialny – od małej sieci lokalnej składającej się z kilku komputerów, do rozległej, obejmującej swoim zasięgiem większe obszary. Systemy informatyczne wchodzące w skład sieci mogą być jej zakończeniami (pojedynczymi hostami, dekoderami, telefonami itp.) albo uczestniczyć w procesie transferu danych, np. routery. Warunkiem koniecznym uznania danej struktury za sieć jest przesyłanie za jej pośrednictwem danych informatycznych.

Dane informatyczne to dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie informatycznym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny.

W art. 1 lit. d Konwencji o cyberprzestępczości zdefiniowano ponadto dane dotyczące ruchu (*traffic data*) jako dowolne dane informatyczne odnoszące się do komunikowania się za pomocą systemu informatycznego, wygenerowane przez system informatyczny (np. telefon, komputer, serwer, ale też router czy switch – jako punkty na trasie transferu danych), który utworzył część w łańcuchu komunikacyjnym, wskazując swoje pochodzenie (miejsce, w którym transfer danych został zainicjowany, jako przede wszystkim numer IP, ewentualnie numer telefonu lub w inny podobny sposób zidentyfikowane urządzenie komunikacyjne, dla którego usługodawca internetowy świadczy usługę) i przeznaczenie (analogiczne dane identyfikujące urządzenie komunikacyjne, do którego transmisja jest kierowana, jak w przypadku urządzenia komunikacyjnego będącego miejscem, w którym transfer danych został zainicjowany), trasę, czas, datę, rozmiar, czas trwania i rodzaj danej usługi (np. transfer plików, poczta elektroniczna). Dane dotyczące ruchu mogą występować w postaci dynamicznej, tj. jako dane w trakcie transmisji (dane zawarte w nagłówkach pakietów danych), oraz statycznej, jako logi systemowe przechowywane w firewallach, routerach lub w serwerach (zawierające informacje o wszelkich zdarzeniach zachodzących w sieci wraz z podaniem uczestniczących w nich podmiotów). Danymi dotyczącymi ruchu niewątpliwie są adresy e-mail oraz adresy IP[4].

Termin *cyberspace* (słowo powstałe z połączenia słów *cybernetics* i *space* – przestrzeń cybernetyczna) pojawił się w latach 80. Za jego autora uważa się kanadyjskiego pisarza Williama Gibsona. Użył tego słowa w wydanej w 1984 roku powieści „Neuromancer" na określenie generowanych przez komputer

4 Zob. szerzej J. Clough, *Principles of Cybercrime*, Nowy Jork 2013, s. 153–154.

rzeczywistości wirtualnych, w których znajdowali się jego bohaterowie. Termin ten przeniknął do kultury masowej i obecnie określa się nim przede wszystkim wirtualną przestrzeń, czyli przestrzeń komunikacji za pomocą sieci komputerowych.

W polskim prawie definicję cyberprzestrzeni znajdziemy w art. 2 ust. 1a ustawy z dnia 21 czerwca 2002 r. o stanie wyjątkowym[5], art. 3 ust. 1 pkt 4 ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej[6] oraz art. 2 ust. 1b ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej[7]. W jej świetle przez to pojęcie należy rozumieć „przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne[8] – wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami". Systemem teleinformatycznym, w rozumieniu ustawy o informatyzacji, jest zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego. Z tej stosunkowo szerokiej definicji wynika, że w rozumieniu ustawodawcy cyberprzestrzeń to nie tylko systemy teleinformatyczne, czyli tworzące je urządzenia (*hardware*) wraz z programami (*software*) zapewniającymi wykonywanie funkcji przez te systemy (przetwarzanie, przechowywanie i przesyłanie danych komputerowych), lecz także dane komputerowe oraz interakcje między urządzeniami a ich użytkownikami[9].

Nośnik danych – w polskim prawie został zdefiniowany informatyczny nośnik danych (w art. 3 pkt 1 ustawy o informatyzacji) jako materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych

5 Dz.U. 2019, poz. 1928, z późn. zm.
6 Dz.U. 2017, poz. 1897, z późn. zm.
7 Dz.U. 2019, poz. 1932, z późn. zm.
8 Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz.U. 2021, poz. 2070, z późn. zm.
9 Zob. szerzej np.: T.R. Aleksandrowicz, K. Liedel, *Społeczeństwo informacyjne – sieć – cyberprzestrzeń. Nowe zagrożenia* [w:] *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, red. K. Liedel, P. Piasecka, T.R. Aleksandrowicz, Warszawa 2014, s. 23–27; K. Liderman, *Bezpieczeństwo informacyjne*, Warszawa 2012, s. 62–63; P. Trąbiński, *Podział kompetencji w zapewnianiu cyberbezpieczeństwa* [w:] *Internet. Strategie bezpieczeństwa*, red. G. Szpor, A. Gryszczyńska), Warszawa 2017, s. 70–74; D. Wall, *Cybercrime. The Transformation of Crime in the Information Age*, Malden 2013, s. 10–11

w postaci cyfrowej. Można przyjąć, że ustawodawca, regulując kwestie z zakresu informatyki, posłużył się pojęciem „nośnik danych", ale miał na myśli pojęcie „informatyczny nośnik danych[10]". Zaznaczyć należy, że nośnikiem danych („nieinformatycznym"), w przypadku danych informatycznych, może być np. rolka papieru, na której zostaną one zapisane w systemie binarnym.

Hosting to przechowywanie przez usługodawcę danych pochodzących od osób trzecich (usługobiorców). Zazwyczaj polega na udostępnieniu przez usługodawcę zasobów własnych serwerów (czy też zasobów tzw. chmury obliczeniowej – zob. dalsze rozważania) przez wydzielenie serwerów wirtualnych, o których przeznaczeniu decyduje usługobiorca. Jedynym ograniczeniem jest ilość przyznanej pamięci, dlatego użytkownik może założyć serwer www (i umieścić na nim witryny internetowe) czy serwer pocztowy.

Rozwiązaniem zbliżonym do omówionego wyżej zwykłego hostingu opartego na wirtualnych serwerach jest hosting zapewniany przy użyciu chmury obliczeniowej. Przez pojęcie „chmura obliczeniowa" powszechnie rozumie

10 Należy podkreślić, że w art. 61 ust. 2 ustawy o informatyzacji przewidziano, że „[...] ilekroć w przepisach dotyczących informatyzacji zawartych w odrębnych ustawach jest mowa o: elektronicznym nośniku informacji, elektronicznym nośniku informatycznym, elektronicznym nośniku danych, komputerowym nośniku informacji, komputerowym nośniku danych, nośniku elektronicznym, nośniku magnetycznym, nośniku informatycznym albo nośniku komputerowym – należy przez to rozumieć, w przypadku wątpliwości interpretacyjnych, informatyczny nośnik danych, o którym mowa w art. 3 pkt 1 niniejszej ustawy". Oczywiście można dywagować, czy omawiane w niniejszym artykule przepisy można zaliczyć do regulujących kwestię informatyzacji i odmówić im takiego charakteru, ale niewątpliwie mimo wszystko terminologia używana w ramach systemu prawnego powinna być spójna i jednolita. Zresztą jest to wymóg uznania go za system, gdyż przez pojęcie to rozumie się powszechnie „[...] skoordynowany układ elementów, zbiór tworzący pewną całość, uwarunkowaną stałym, logicznym uporządkowaniem jego części składowych" (*Słownik języka polskiego*, red. M. Szymczak, t. 3, Warszawa 1995, s. 361). Ponadto ustawa o informatyzacji zobowiązała Radę Ministrów do przygotowania – w terminie 2 lat od dnia wejścia w życie ustawy o informatyzacji, do przygotowania projektu ustawy dotyczącej dostosowania terminologii w przepisach odrębnych ustaw dotyczących informatyzacji do określeń wymienionych w jej art. 3 pkt 1 i 2 (tj. informatyczny nośnik danych i dokument elektroniczny). Realizująca to zobowiązanie ustawa z dnia 4 września 2008 r. o zmianie ustaw w celu ujednolicenia terminologii informatycznej (Dz.U. 2008, nr 171, poz. 1056) wprowadzała określenia: „informatyczny nośnik danych", „dokument elektroniczny", „system teleinformatyczny" oraz „środki komunikacji elektronicznej" (wymienione w art. 3 pkt 1–4 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne) do innych ustaw (m.in. ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego, Dz.U. 2021, poz. 1805, z późn. zm. czy kodeksu karnego), ale nie do ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz.U. 2021, poz. 554, z późn. zm.), co uznać można za przeoczenie. Jednakże nie stanowi to negacji wcześniejszych uwag dotyczących wymogu jednolitości siatki pojęciowej w ramach całego systemu.

się system zapewniający dostęp do zasobów serwerowych (mocy obliczeniowej, pamięci masowej, interfejsów sieciowych) poprzez interfejs (aplikację), pozwalający na płynne jej skalowanie w zależności od aktualnego obciążenia (w uproszczeniu – korzystanie z tych serwerów, które w danym momencie są najmniej obciążone i tym samym są w stanie zagwarantować najwyższą wydajność). W przypadku zwykłego hostingu, gdy zacznie brakować zasobów fizycznego serwera, ponieważ inny serwer wirtualny na tym samym serwerze fizycznym (serwerach fizycznych) tak się rozrósł, że zajął niemal wszystkie zasoby, użytkownik (usługobiorca hostingu) nie ma możliwości szybkiego przeniesienia danych i oprogramowania na inny fizyczny serwer (serwery), jest to bowiem zazwyczaj pracochłonny i czasochłonny proces, który może trwać od kilku godzin do wielu dni. Inaczej jest w przypadku serwerów działających w chmurze – nie są ograniczane w żaden sposób przez aktualną dostępność zasobów. Jeżeli zaczynają się one wyczerpywać (np. zaczyna brakować pamięci, mocy obliczeniowej procesorów itd.), to serwer użytkownika w chmurze zostaje automatycznie przeniesiony na inny fizyczny serwer dysponujący wolnymi zasobami.

Zgodnie z pkt 17 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa NIS)[11] pojęcie „usługa przetwarzania w chmurze" obejmuje „[...] usługi, które umożliwiają dostęp do skalowanego i elastycznego zbioru zasobów komputerowych do wspólnego wykorzystywania". Użyte w definicji pojęcia oznaczają: 1) zasoby obliczeniowe sieci – serwery lub inną infrastrukturę, pamięć, aplikacje i usługi, niezależnie od położenia geograficznego zasobów; 2) elastyczny zbiór – jego zmienny skład i możliwość jego adaptacji do zmieniających się warunków; 3) skalowanie – zasoby komputerowe udostępniane są przez usługodawcę, niezależnie od położenia geograficznego zasobów, jako reakcja na zmienne zapotrzebowanie; 4) wspólne wykorzystywanie – zasoby obliczeniowe są udostępniane wielu użytkownikom, którzy współdzielą wspólny dostęp do usług, ale przetwarzanie odbywa się oddzielnie dla każdego z nich, choć usługa jest świadczona przez tego samego usługodawcę oraz z tego samego sprzętu elektronicznego.

Wyróżnia się trzy zasadnicze modele przetwarzania w chmurze: 1) IaaS (infrastruktura IT jako usługa) – polega na dostarczeniu usługobiorcy infrastruktury informatycznej (IT), czyli oprogramowania, usługi serwisowania,

11 Dz. Urz. UE 2016, L 194/1.

komputerów, serwerów, przestrzeni dyskowej, pamięci, mocy obliczeniowej; 2) PaaS (platforma jako usługa) – polega na sprzedaży gotowego, często dostosowanego do indywidualnych potrzeb użytkownika (na zamówienie) oprogramowania, np. systemu operacyjnego, systemu zarządzania bazą danych, środowiska zapewniającego funkcjonowanie aplikacji (oczywiście platforma znajduje się na serwerach dostawcy); usługobiorca ma dostęp do interfejsu (zwykle w postaci ujednoliconego środowiska pracy) poprzez program klienta (może to być przeglądarka internetowa); 3) SaaS (oprogramowanie jako usługa) – prostu forma dystrybucji oprogramowania – aplikacja, której udostępnianie w tym wypadku stanowi usługę, jest przechowywana i udostępniana przez producenta użytkownikom za pomocą internetu, co z kolei eliminuje potrzebę instalacji i uruchomiania programu na komputerze użytkownika. Programy działają na serwerze dostawcy. Usługi dostępne są online w czasie rzeczywistym w chmurze obliczeniowej.

W polskim kodeksie postępowania karnego[12] kwestię przeszukania środowiska informatycznego – zarówno systemów informatycznych, jak i informatycznych nośników danych – reguluje art. 236a, który ma charakter przepisu odsyłającego, przewidujący, że przepisy rozdziału 25 („Zatrzymanie rzeczy. Przeszukanie") stosuje się odpowiednio do dysponenta i użytkownika urządzenia zawierającego dane informatyczne lub systemu informatycznego, w zakresie danych przechowywanych w tym urządzeniu lub systemie albo na nośniku znajdującym się w jego dyspozycji lub użytkowaniu[13], w tym korespondencji przesyłanej pocztą elektroniczną.

Na wstępie należy zaznaczyć, że zbędne jest wyodrębnienie pojęcia „urządzenie zawierające dane informatyczne", ponieważ zgodnie z podanymi na wstępie definicjami będzie to – w zależności od stopnia skomplikowania – albo informatyczny nośnik danych (np. klasyczny, tj. magnetyczny, dysk twardy

12 Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego, Dz.U. 2021, poz. 554, z późn. zm.

13 Przez dysponenta należy rozumieć osobę upoważnioną do rozporządzania systemem, mającą ten system do dyspozycji, podejmującą decyzje dotyczące jego funkcjonowania, będącą twórcą regulaminu sieci, decydującą o zakresie uprawnień użytkowników (jeżeli uprawnienie to nie jest scedowane na administratora), np. właściciela systemu, administratora. Użytkownik to osoba używająca systemu, korzystająca z niego w zakresie swoich uprawnień (nadanych przez dysponenta systemu lub administratora), może to być jednocześnie dysponent systemu. Zob. szerzej A. Lach, *Gromadzenie dowodów elektronicznych po nowelizacji kodeksu postępowania karnego*, „Prokuratura i Prawo" 2005, nr 10, s. 20.

– *hard disk drive*[14]) albo system informatyczny (np. smartfon, komputer). Przez określenie „dysponent" należy rozumieć osobę upoważnioną do rozporządzania systemem, mającą ten system do dyspozycji, rozporządzającą nim według swego uznania, czyli np. właściciela systemu, administratora. Użytkownikiem jest osoba korzystająca z systemu, eksploatująca go, czerpiąca jakieś korzyści z cudzego systemu, np. posiadacz konta poczty elektronicznej[15].

Możliwe jest wyróżnienie trzech rodzajów przeszukania środowiska informatycznego. Po pierwsze, przeszukanie zdalne systemu informatycznego[16] przeprowadzane z użyciem komputera znajdującego się np. w siedzibie jednostki policji, w sposób niejawny (bez informowania jego użytkownika przed przystąpieniem do czynności), dokonywane za pomocą oprogramowania śledczego, będącego po prostu oprogramowaniem typu *spy-ware*[17]. Systemów informatycznych i nośników danych nie przeszukuje się na miejscu ich zatrzymania. Robi się to po odpowiednim zabezpieczeniu i przewiezieniu do laboratorium. Można powiedzieć, że jest to drugi rodzaj przeszukania (chyba najpowszechniejszy; więcej na ten temat zob. dalsze rozważania). Trzecim typem (pozostaje poza zakresem niniejszego opracowania, gdyż nie jest uregulowany w żadnym ustawodawstwie krajowym) jest przewidziane w art. 19 Konwencji o cyberprzestępczości tzw. przeszukanie rozszerzone. Polega ono – jak nazwa wskazuje – na poszerzeniu przeszukania na inne (tj. odrębne) systemy informatyczne (wtórne), do których można uzyskać dostęp z systemu informatycznego będącego przedmiotem przeszukania (system pierwotny). Przykładem jest przeszukiwanie kolejno komputerów znajdujących się w sieci

14 Dyski twarde (*hard disk drive* – HDD) – zbudowane są z okrągłych talerzy ułożonych jeden nad drugim, na których dane zapisywane są z obu stron przez głowice elektromagnetyczne w postaci impulsów elektromagnetycznych. Ponadto coraz częściej (zwłaszcza w tzw. ultrabookach) spotyka się zamiast tradycyjnych dysków twardych dyski SSD (*solid-state drive*), które działają na tej samej zasadzie, co pamięć *flash*. Mają zwykle mniejszą pojemność niż klasyczne dyski twarde, ale są odporniejsze na czynniki zewnętrzne, a przede wszystkim charakteryzuje je znacznie krótszy czas dostępu do danych.

15 Zob. szerzej A. Lach, *Gromadzenie…*, s. 20.

16 Nie ma w zasadzie takiej możliwości w przypadku informatycznego nośnika danych, dlatego że nie jest on samodzielny i może zostać przeszukany tylko wówczas, gdy jest podłączony do systemu informatycznego na stałe, stanowi jego element, np. jako dysk twardy (obojętne czy hdd czy ssd), bądź przejściowo, np. jako płyta dvd odtwarzana w systemie informatycznym czy podłączony do niego pendrive z danymi. W tym drugim wypadku można wyobrazić sobie, że osoba dokonująca przeszukania zdalnego systemu informatycznego jednocześnie uzyska dostęp do danych znajdujących się na nośniku podłączonym w ten sposób do niego.

17 A. Lach, *Przeszukanie na odległość systemu informatycznego*, „Prokuratura i Prawo" 2011, nr 9, s. 68.

lokalnej jedynie na podstawie możliwości uzyskiwania dostępu do nich z przeszukiwanych komputerów i istnieniu prawdopodobieństwa, że mogą na nich znajdować się dane mające wartość dowodową w prowadzonym postępowaniu karnym. Nie ma chyba konieczności tłumaczenia, że umożliwienie organom ścigania przeprowadzania takich czynności bez dodatkowych mechanizmów zapewniających ich kontrolę i nadzór nad nimi stanowi naruszenie praw człowieka, zwłaszcza że w Konwencji jest wymóg ich stworzenia (zob. art. 15 Konwencji).

W art. 236a k.p.k. przewidziano odpowiednie stosowanie do dysponenta i użytkownika urządzenia zawierającego dane informatyczne lub systemu informatycznego, w zakresie danych przechowywanych w tym urządzeniu lub systemie albo na nośniku znajdującym się w jego dyspozycji lub użytkowaniu przepisów rozdziału 25 („Zatrzymanie rzeczy. Przeszukanie"). Odpowiednie stosowanie oznacza sięganie do rozwiązań innej regulacji (w tym wypadku przepisów z tej samej ustawy). Może ono przybrać trzy formy:

1) zastosowania konkretnego przepisu ustawy wprost;

2) zastosowania z odpowiednimi modyfikacjami (z uwzględnieniem celu ustawy oraz specyfiki regulowanego zagadnienia);

3) odmowy zastosowania.

W każdym wypadku należy czynić to z zachowaniem szczególnej ostrożności[18].

W przypadku przeszukania systemu informatycznego czy informatycznego nośnika danych zastosowanie – ze względu na specyfikę tej czynności – znajdzie jedynie część przepisów. Na pewno będzie to art. 217 k.p.k. regulujący wydanie, odebranie i zatrzymanie rzeczy mogącej stanowić dowód. W przypadku danych informatycznych wydanie może polegać zarówno na wydaniu fizycznego nośnika danych (np. płyta dvd, pendrive) czy systemu informatycznego (np. komputera, smartfona), w którym znajduje się nośnik danych (np. dysk twardy) zawierający dane informatyczne, jak i udostępnienie danych w celu ich skopiowania czy wykonania klona lub obrazu nośnika[19], bez jednoczesnego

18 Por. np. Wyrok SN z dnia 5 listopada 2003 r., „Orzeczenia Sądu Najwyższego" 2003, nr 67.

19 Obraz zawartości dysku – wszelkie zapisane na nim dane, łącznie z danymi usuniętymi oraz pustymi obszarami (gdzie również mogą znajdować się dane). Klonowanie danych – utworzenie lustrzanej kopii zawartości dysku dowodowego na odrębnym dysku twardym, z uwzględnieniem – podobnie jak w przypadku obrazu dysku – wszystkich danych, wraz z niewidocznymi lub usuniętymi oraz pustymi przestrzeniami. Możliwe jest umieszczenie takiego klona na dysku i zamontowanie go na komputerze, z którego pochodzi przeszukiwany

wydania samego nośnika czy systemu informatycznego zawierającego nośnik. Możliwe jest wtedy pozostawienie nośnika danych czy systemu informatycznego przetwarzającego dane w posiadaniu dysponenta, żeby umożliwić mu np. prowadzenie działalności gospodarczej, jeżeli system informatyczny temu służył, zwłaszcza że dowodem są dane komputerowe, a nie sprzęt. Może się, oczywiście zdarzyć, że wartość dowodową będą mieć zarówno dane komputerowe, jak i sprzęt, np. gdy sprawca korzystał z kradzionego komputera. Innym przykładem konieczności zabezpieczenia informatycznego nośnika danych jest sytuacja, gdy skopiowanie zarówno całości, jak i części danych jest wykluczone. Ma to miejsce po pierwsze, gdy dane (lub ich część) stanowią tajemnicę prawnie chronioną, korespondencję osób trzecich czy też dane dotyczące innego podmiotu niż objęty przeszukaniem. W związku z tym organy procesowe muszą zabezpieczyć nośnik (bez jego przeglądania) i przekazać organowi właściwemu do uchylenia tajemnicy. Ewentualnie mogą skopiować dane komputerowe nieobjęte zakazami dowodowymi pod warunkiem, że ich wyodrębnienie jest możliwe. Na marginesie należy podkreślić, że nigdy nie prowadzi się czynności na oryginalnych danych, żeby uniknąć ich modyfikacji – pracuje się na ich kopiach lub obrazach. Jak wspominano, specyfiką przeszukań nośników czy systemów informatycznych jest to, że przeprowadzone są w laboratorium, a nie w miejscu ich zajęcia.

Oczywiście, w razie przeszukania systemu informatycznego czy informatycznego nośnika danych znajdą zastosowanie przepisy kodeksu postępowania karnego – art. 220 wskazujący organ właściwy do dokonania przeszukania oraz regulujący tryb natychmiastowego przeszukania oraz art. 225–226 dotyczące postępowania z danymi mogącymi być informacjami chronionymi, tj. stanowiącymi informacje niejawne lub będące informacjami objętymi tajemnicą zawodową lub inną tajemnicą prawnie chronioną albo mające charakter osobisty (bez odczytania przekazuje się je prokuratorowi lub sądowi w opieczętowanym opakowaniu) czy też obejmujące okoliczności związane z wykonywaniem funkcji obrońcy (zwraca je w całości lub w części osobie, od której je zabrano, albo wydaje postanowienie o ich zatrzymaniu dla celów postępowania). Zastosowanie znajdą również przepisy kodeksu postępowania karnego regulujące tryb przeszukania, tj.: art. 227 zawierający dyrektywy przeszukania, przewidujący, że przeszukanie powinno odbywać się zgodnie

dysk, uruchomienie systemu operacyjnego i korzystanie z niego jak z systemu na pierwotnym dysku. Zob. szerzej np. M. Chrabkowski, K. Gwizdała, *Zabezpieczenie dowodów elektronicznych*, „Prokuratura i Prawo" 2015, nr 12, s. 167–169.

z celem tej czynności, z zachowaniem umiaru oraz w granicach niezbędnych do osiągnięcia celu tych czynności z zachowaniem należytej staranności, w poszanowaniu prywatności i godności osób, których ta czynność dotyczy, oraz bez wyrządzania niepotrzebnych szkód i dolegliwości, art. 228 dotyczący zabezpieczenie dowodów, art. 229 określający treść protokołu, art. 230 dotyczący zatwierdzenia zatrzymania oraz zwrotu rzeczy, art. 231 regulujący kwestię złożenia rzeczy do depozytu sądowego, art. 234 określający czynności prawne z udziałem rzeczy zatrzymanych, art. 235 określający właściwość organów oraz art. 236 regulujący tryb odwoławczy.

Ze względu na specyfikę przeszukania informatycznych nośników danych i systemów informatycznych w stosunku do danych w nich zawartych nie znajdą zastosowania przepisy kodeksu postępowania karnego zawarte w art. 222 (przeszukanie pomieszczeń instytucji państwowej, samorządowej i wojska), art. 223 (przeszukanie osoby), art. 221 (pora przeszukania). Będą one miały zastosowanie do sprzętu oraz informatycznych nośników danych. Samo przeszukanie systemu informatycznego z reguły ma charakter niejawny – często odbywa się bez wiedzy dysponenta, np. przy przeszukaniu zdalnym, czy bez jego obecności – sprzęt informatyczny eksplorowany jest w bezpiecznym miejscu, w siedzibie organu wymiaru sprawiedliwości prowadzącego sprawę, wykonywany jest na kopiach danych lub obrazach dysków i trwa często wiele godzin. Stąd też zwykle nic nie stoi na przeszkodzie, żeby zwrócić go dysponentowi (obojętne, czy podejrzanemu czy osobie trzeciej), zwłaszcza wówczas, gdy stanowi on narzędzie pracy.

Jak powszechnie przyjmuje się w doktrynie, w przypadku systemu informatycznego przeszukanie polega na sięgnięciu do wszystkich danych, których dysponentem jest użytkownik, a zatem, do których ma dostęp, np. danych na dysku twardym w przypadku komputera, karty pamięci w przypadku telefonu komórkowego, a także danych znajdujących się w chmurze obliczeniowej, na dysku, na serwerze ftp czy zasobach hostingodawcy. Dane te nie muszą znajdować się na terytorium Polski (i zwykle tak jest), gdyż serwery, na których są przechowywane, mogą znajdować się poza jej granicami.

W artykule 236a k.p.k. znajduje się jeszcze jedno sformułowanie, które specjalnie nie zostało wyjaśnione wcześniej, gdyż to miejsce jest właściwsze. W przepisie jest mowa, że „[...] przepisy rozdziału niniejszego stosuje się odpowiednio do […] korespondencji przesyłanej pocztą elektroniczną". Poczta elektroniczna występuje zasadniczo w dwóch postaciach, mianowicie jako dane przesyłane siecią oraz w formie zgromadzonej, czy to w systemie informatycznym użytkownika czy na serwerze pocztowym i oczekujące na pobranie

lub wysłanie[20]. W doktrynie jest prezentowane stanowisko, że w kodeksie postępowania karnego, w zależności od sytuacji, do korespondencji przesyłanej drogą elektroniczną mają zastosowanie różne regulacje. Artykuł 241 k.p.k. przewiduje stosowanie przepisów dotyczących kontroli i utrwalania rozmów odpowiednio do kontroli oraz do utrwalania z wykorzystaniem środków technicznych treści innych rozmów lub przekazów informacji, w tym korespondencji przesyłanej pocztą elektroniczną. Z kolei zatrzymanie i kontrolę korespondencji reguluje art. 218 k.p.k., co prowadzi do tego, że korespondencja, a zatem na mocy art. 236a również poczta elektroniczna w postaci danych zgromadzonych na serwerze pocztowym czy w skrzynce adresata bądź nadawcy, korzysta ze znacznie słabszej ochrony[21]. Uważam, że konstrukcja jest nielogiczna i wymaga zmiany. Nie ma jakichkolwiek powodów, żeby przyznawać różną ochronę danym informatycznym w zależności od tego, czy są one wiadomościami e-mailowymi przesyłanymi siecią czy tymi wiadomościami zeskładowanymi w jakikolwiek sposób – na dysku użytkownika czy na serwerze pocztowym[22]. W związku z tym bez względu na formę powinny podlegać ochronie prawnej identycznej jak korespondencja elektroniczna, a co za tym idzie – powinny korzystać z gwarancji ochrony zapewnionych w rozdziale 26 kodeksu postępowania karnego („Kontrola i utrwalanie rozmów").

Omawiana regulacja jest stworzona, delikatnie mówiąc, nieporadnie. Świadczy o tym przede wszystkim brak zrozumienia dla specyfiki poczty elektronicznej (różnicowanie poziomu ochrony w zależności od tego, czy wiadomość znajduje się na serwerze pocztowym lub na komputerze użytkownika czy jest przesyłana siecią) czy zastosowana wadliwa terminologia (urządzenie przetwarzające dane informatyczne, nośnik danych), która jak wskazano w głównej części artykułu powinna być spójna i identyczna w ramach całego systemu prawa.

20 Odmiennie przedstawia się sytuacja w przypadku kwalifikacji prawnej zachowań polegających na uzyskaniu dostępu do wiadomości znajdujących się na serwerze lub na komputerze użytkownika, ale przechwytywanych jako dane przesyłane siecią. W tym pierwszym wypadku będzie to *hacking*, a zatem właściwa będzie kwalifikacja z art. 267 § 1 lub § 2 k.k., w drugim – podsłuch komputerowy, a zatem czyn kryminalizowany w art. 267 § 3 tegoż kodeksu

21 A. Lach, *Karnoprocesowe instrumenty zwalczania pedofilii i pornografii dziecięcej w Internecie*, „Prokuratura i Prawo" 2005, nr 10, s. 55; J. Grajewski, S. Steinborn, [w:] *Komentarz aktualizowany do art. 1–424 Kodeksu postępowania karnego*, red. L.K. Paprzycki, LEX/el. 2015, art. 236(a), pkt 2; R.A. Stefański, S. Zabłocki, [w:] *Kodeks postępowania karnego*, t. 2, *Komentarz do art. 167–296*, red. nauk. R.A. Stefański, S. Zabłocki, Warszawa 2019, art. 236(a), pkt 4.

22 Upraszczając problem i przenosząc to rozumowanie na grunt ochrony zwykłej korespondencji, należałoby przyjąć, że inne standardy ochrony należy przyjąć w przypadku korespondencji skradzionej listonoszowi, a inne odnośnie do listu wyjętego ze skrzynki pocztowej adresata.

Bibliografia

Aleksandrowicz T.R., Liedel K., *Społeczeństwo informacyjne– sieć – cyberprzestrzeń. Nowe zagrożenia* [w:] *Sieciocentryczne bezpieczenstwo. Wojna, pokój i terroryzm w epoce informacji*, red. K. Liedel, P. Piasecka, T.R. Aleksandrowicz, Warszawa 2014.
Clough J., *Principles of Cybercrime*, Nowy Jork 2013.
Chrabkowski M., Gwizdała K., *Zabezpieczenie dowodów elektronicznych*, „Prokuratura i Prawo" 2015, nr 12.
Grajewski J., Steinborn S., [w:] *Komentarz aktualizowany do art. 1–424 Kodeksu postępowania karnego*, red. L. K. Paprzycki, LEX/el. 2015.
Lach A., *Gromadzenie dowodów elektronicznych po nowelizacji kodeksu postępowania karnego*, „Prokuratura i Prawo" 2005, nr 10.
Lach A., *Karnoprocesowe instrumenty zwalczania pedofilii i pornografii dziecięcej w Internecie*, „Prokuratura i Prawo" 2005, nr 10.
Lach A., *Przeszukanie na odległość systemu informatycznego*, „Prokuratura i Prawo" 2011, nr 9.
Liderman K., *Bezpieczeństwo informacyjne*, Warszawa 2012.
Radoniewicz F., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016.
Siwicki, *Cyberprzestępczość*, Warszawa 2013.
Słownik języka polskiego PWN, red. M. Szymczak, t. 3, Warszawa 1995.
Kodeks postępowania karnego, t. 2, *Komentarz do art. 167–296*, red. nauk. R.A. Stefański, S. Zabłocki, Warszawa 2019.
Trąbiński P., *Podział kompetencji w zapewnianiu cyberbezpieczeństwa* [w:] *Internet. Strategie bezpieczeństwa*, red. G. Szpor, A. Gryszczyńska, Warszawa 2017.
Wall D., Cybercrime. *The Transformation of Crime in the Information Age*, Malden 2015

Search IT systems and IT data carriers in the Code of Criminal Procedure

Abstract

The subject of the article is investigatory powers consisting in searching for IT systems (both connected with other IT systems and being independent units), „devices containing data" and (IT) data carriers. This issue is regulated by the reference contained in Art. 236a of the Code of Penal Procedure of 1997 to the provisions of Chapter 25. „Seizure. Search", providing for appropriate use to the holder and user of a device containing IT data or an IT system, in the scope of data stored in this device or system or on a carrier at its disposal or use, including correspondence sent by electronic mail.

Key words: cybercrime, search, preservation of evidence, cloud computing, Convention on Cybercrime