Monika Nowikowska*

Procesowa kontrola danych informatycznych w chmurze obliczeniowej

Streszczenie

Autorka artykułu podjęła próbę analizy procesowej kontroli korespondencji przechowywanej w pamięci wirtualnej, czyli w tzw. chmurze (cloud computing). Opracowanie stanowi próbę odpowiedzi na pytanie, w jaki sposób urządzenia mobilne i chmury są badane i jaki wpływ na realizację czynności procesowych mają przepisy prawa odnośnie do prywatności. Wzrost zainteresowania chmurą obliczeniową skutkuje pojawieniem się wielu nowych problemów prawnych, które przekładają się m.in. na praktykę i zasady działania organów ścigania. W pierwszej kolejności omówiono pojęcie „chmura obliczeniowa" oraz poddano analizie przepisy dotyczące pozyskiwania dowodów elektronicznych. Uniezależnienie systemów teleinformatycznych od funkcjonowania klasycznego środowiska pracy opartego na pojedynczej stacji roboczej pozwoliło także postawić pytanie o transgraniczność usług świadczonych w chmurze. Dane informatyczne przekazywane poprzez chmurę obliczeniową mogą być zapisywane na kilkunastu urządzeniach zlokalizowanych w różnych państwach.

Słowa kluczowe: chmura obliczeniowa, obrazowanie fizyczne, obrazowania logiczne, przeszukanie, zabezpieczenie dowodów

* Dr Monika Nowikowska, adiunkt w Katedrze Prawa Informatycznego, Wydział Prawa i Administracji, Akademia Sztuki Wojennej, radca prawny, e-mail: m.nowikowska@akademia.mil.pl, ORCID: 0000-0001-5166-8375.

Wstęp

Rozwój nowych technologii daje z jednej strony możliwości samorealizacji jednostki, z drugiej, niesie za sobą zagrożenia. Wraz ze wzrostem możliwości i złożoności urządzeń mobilnych wzrosła zarówno liczba ich użytkowników, jak i ilość informacji przechowywanych na tych urządzeniach. Przykładowo, najnowsze smartfony mają możliwość obsługi kart pamięci o pojemności 1 Tb[1]. Prowadzi to do sytuacji, w której użytkownicy przechowują w swoich smartfonach ogrom danych i informacji, w tym dane wrażliwe ze sfery życia prywatnego[2].

Łatwość dostępu do nowych technologii oraz ich powszechność sprawia, że ten obszar działalności człowieka staje się także narzędziem działań przestępczych[3]. Nie jest zaskoczeniem, że wraz ze wzrostem liczby urządzeń rośnie potencjał przechowywania przez nie istotnych danych dla procesu karnego. To wszystko czyni ze smartfonów, komputerów i internetu także narzędzie do popełniania przestępstw[4].

W artykule podjęto próbę analizy operacyjnej i procesowej kontroli korespondencji przechowywanej w pamięci wirtualnej, czyli w tzw. chmurze (cloud computing – CC)[5]. Na wstępie należy zauważyć, że jest to temat ważny i złożony, gdyż dochodzi w tym przypadku do kolizji dwóch dóbr – naturalnej antynomii pomiędzy bezpieczeństwem państwa (czynności operacyjne i procesowe) a prywatnością jednostki[6]. Czynność procesowa polegająca na przeszukaniu mieszkania lub osoby stanowi wyjątek od konstytucyjnie zagwarantowanej nienaruszalności mieszkania i korespondencji (art. 49 i 50 Konstytucji RP[7]) i musi być stosowana z bardzo dużą rozwagą. Z drugiej strony, zwiększona

1 https://www.apple.com/pl/iphone-13-pro/specs/ [dostęp: 2.09.2022].

2 K. Chałubińska-Jentkiewicz, M. Nowikowska, *Bezpieczeństwo, tożsamość, prywatność – aspekty prawne*, Warszawa 2020, s. 216; A. Etzioni, *Privacy in a cyber age, Policy and Practice*, Hampshire 2015, s. 67.

3 A. Gobeo, C. Fowler, W.J. Buchanan, *GDPR and Cyber Security for Business Information Systems*, Gistrup 2018, s. 99.

4 M. Siwiecki, P. Kowalski, *Przeszukanie i zatrzymanie rzeczy w sprawach o cyberprzestępstwa. Udział specjalistów i biegłych w czynnościach procesowych*, „Kwartalnik Policyjny" 2021, t. 57, nr 2, s. 3.

5 E. Molenda-Kropielnicka, *Cloud Computing – zagadnienia prawne*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej" 2013, nr 119, s. 113.

6 D. Szumiło-Kulczycka, *Między ochroną prywatności a bezpieczeństwem – uwagi na tle orzecznictwa ETPCz i TSUE* [w:] *Pozyskiwanie informacji w walce z terroryzmem*, red. P. Herbowski, D. Słapczyńska, D. Jagiełło, Warszawa 2017, s. 68.

7 Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. 1997, nr 78, poz. 483.

świadomość zarówno obywateli, jak i producentów urządzeń ochrony danych doprowadziła do tego, że urządzenia te są bardziej bezpieczne, ale odbywa się to kosztem bezpieczeństwa i zdolności organów ścigania do zwalczania nielegalnych działań[8]. Należy zauważyć, że w sprawach karnych sukces dochodzenia może zależeć od zdolności śledczego do uzyskania dostępu do dowodów przechowywanych zarówno w urządzeniu mobilnym, jak i w chmurze. Artykuł stanowi próbę odpowiedzi na pytanie: w jaki sposób urządzenia mobilne i chmury są badane i jaki wpływ na realizację czynności procesowych mają przepisy prawa odnośnie do prywatności. W pierwszej kolejności omówienia wymaga pojęcie „chmura obliczeniowa". W dalszej kolejności analizie poddano przepisy dotyczące pozyskiwania dowodów elektronicznych. Wzrost zainteresowania chmurą obliczeniową skutkuje pojawieniem się wielu nowych problemów prawnych, które przekładają się m.in. na praktykę i zasady działania organów ścigania. Podczas wykonywania czynności operacyjno-rozpoznawczych czy dochodzeniowo-śledczych pojawia się konieczność uwzględnienia transgraniczności, dlatego że dane informatyczne przekazywane poprzez chmurę obliczeniową mogą być zapisywane na kilkunastu urządzeniach zlokalizowanych w różnych państwach[9]. Uniezależnienie systemów teleinformatycznych od funkcjonowania klasycznego środowiska pracy opartego na pojedynczej stacji roboczej nasuwa także pytanie o potrzebę reinterpretacji tradycyjnego rozumienia miejsca popełnienia przestępstwa oraz zabezpieczenia mienia w celach dowodowych, które wiąże się zarówno z przeszukaniem, jak i zabezpieczeniem danych przechowywanych na nośnikach zlokalizowanych w jednym państwie[10].

Cloud computing – ogólna charakterystyka (pojęcie, cechy, funkcje)

Chmura obliczeniowa jest modelem gwarantującym wszechobecny, wygodny, szybki i możliwy na żądanie dostęp do dzielonych zasobów obliczeniowych (serwerów, pamięci masowej, aplikacji, usług) za pośrednictwem sieci.

8 D. Kahvedžic, *Digital forensics and DSAR effect in ERA Forum*, t. 22, Berlin 2021, s. 356.
9 F. Casino i in., *SoK: cross-border criminal investigations and digital evidence*, „Journal of Cybersecurity" 2022, t. 8, s. 1–18.
10 M. Siwicki, *Przetwarzanie danych informatycznych w chmurach obliczeniowych. Wybrane aspekty prawnokarne i procesowe*, „Palestra" 2015, nr 1–2, s. 31.

W literaturze przedmiotu podkreśla się, że zasoby te są zapewniane i uwalniane przy minimalnym zarządzeniu i ingerencji dostawcy[11]. Telefon czy komputer przestają być nośnikiem danych. Dane są przenoszone do wirtualnych pamięci zewnętrznych. Ułatwienia kierowane do użytkowników związane z funkcjonowaniem chmury, przy braku szczegółowej regulacji w tym zakresie, stają się także nowym wyzwaniem dla organów porządku publicznego[12].

Należy podkreślić, że usługa przetwarzana w chmurze wykazuje podobieństwo do outsourcingu. Polega ona na wykorzystywaniu cudzych programów komputerowych, infrastruktury, narzędzi programistycznych hostowanych przez dostawcę w celu tworzenia własnych aplikacji.

W przypadku tych nowych metod przetwarzania danych prawie wszystkie zadania obliczeniowe, w tym: instalacja, administrowanie usługami i przesyłanie danych, odbywają się niezależnie od lokalizacji poszczególnych elementów fizycznych sprzętu komputerowego. Cechą użytkowania CC jest uniezależnienie systemów teleinformatycznych od użytkowanego sprzętu. Trafnie zauważa Maciej Siwicki, że „[...] szczególną cechą wskazanych usług jest zatem tzw. wirtualizacja, a więc oddzielenie warstwy logicznej od warstwy fizycznej systemu informatycznego, dzięki połączeniu wirtualnych maszyn w jeden fizyczny serwer oraz uniezależnieniu funkcjonowania systemu IT użytkownika od funkcjonowania klasycznego środowiska pracy, opartego zazwyczaj na pojedynczej stacji roboczej i jednym systemie operacyjnym”[13]. Kolejną cechą, na którą zwraca on uwagę, jest to, że dane informatyczne, np. pliki zawierające dokumenty tekstowe, w trakcie przesyłania do użytkownika mogą być w tym czasie zapisywane w kilku miejscach, tzn. na serwerach, które mogą być zlokalizowane w różnych państwach. Wskazuje to, że chmura bazuje na współdziałaniu, udostępnianiu i możliwości korzystania z zasobów informacyjnych niezależnie od geograficznej lokalizacji poszczególnych jej elementów[14]. Należy zauważyć, że rozproszenie zasobów informatycznych jest dokonywane głównie ze względów funkcjonalnych i związane z charakterystyką techniczną chmury obliczeniowej, która polega na wyszukiwaniu najkorzystniejszego miejsca zapisu. Miejscem stałego zapisu danych nie będzie komputer,

11 J. Wrona, Z. Zawadzka, *Cyberbezpieczeństwo w prawie własności intelektualnej* [w:] *Cyberbezpieczeństwo. Zarys wykładu*, red. C. Banasiński, Warszawa 2018, s. 377–378.

12 J. Kudła, A. Staszak, *Procesowa i operacyjna kontrola korespondencji przechowywanej w tzw. chmurze*, „Prokuratura i Prawo” 2017, nr 8–7, s. 31.

13 M. Siwicki, op. cit., s. 32–33.

14 J. Kudła, A. Staszak, op. cit., s. 32.

z którego korzysta użytkownik. Oznacza to, że użytkownik nie jest zarówno właścicielem sprzętu, na którym są zapisywane jego dane, jak i nie zna lokalizacji[15]. Ta cecha funkcjonowania CC implikuje poważne problemy prawne z punktów widzenia funkcjonowania organów ścigania. Z powodu konieczności określenia lokalnego miejsca zapisu danych utrudnione jest określenie właściwości miejscowej sądu czy też uprawnień poszczególnych organów ścigania.

Zagadnienie CC zostało poruszone w dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 roku w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa NIS)[16]. W preambule w pkt 17 wskazano, że usługi przetwarzania w chmurze obejmują szeroki zakres działań, które mogą być realizowane według różnych modeli. Ustawodawca unijny pojęciem „usługi przetwarzania w chmurze" objął usługi, które umożliwiają dostęp do skalowalnego i elastycznego zbioru zasobów komputerowych do wspólnego wykorzystywania. Tak skonstruowane pojęcie pozwala na wyróżnienie czterech elementów: 1) skalowanie, 2) elastyczny zbiór, 3) zasoby obliczeniowe, 4) wspólne wykorzystywanie.

Skalowalnie odnosi się do zasobów komputerowych, które są elastycznie przydzielane przez dostawcę usługi niezależnie od położenia geograficznego zasobów jako reakcja na zmiany zapotrzebowania.

Pojęcie „elastyczny zbiór" odnosi się do opisu tych zasobów obliczeniowych, które są przydzielane i uwalniane zależnie od zapotrzebowania, żeby szybko zwiększać i zmniejszać dostępne zasoby w zależności od obciążenia.

Przez zasoby obliczeniowe rozumie się takie zasoby, jak: sieci, serwery lub inną infrastrukturę, pamięć, aplikacje i usługi.

Pojęcie „wspólne wykorzystywanie" dotyczy opisu zasobów obliczeniowych udostępnianych wielu użytkownikom, którzy dzielą wspólny dostęp do usługi, ale przetwarzanie odbywa się oddzielnie dla każdego z nich, mimo że usługa ta jest świadczona z tego samego sprzętu elektronicznego. Zgodnie z art. 4 pkt 5 dyrektywy NIS usługę przetwarzania w chmurze należy zaliczyć do rodzaju usług cyfrowych[17].

15 M. Siwicki, op. cit., s. 33.

16 Dyrektywa 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, Dz. Urz. UE 2016, L 194/1.

17 K. Chałubińska-Jentkiewicz, *Prawna ochrona treści cyfrowych*, Warszawa 2022, s. 66 i n.

Pojęcie chmury obliczeniowej zostało także opisane w komunikacie Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Wykorzystanie potencjału chmury obliczeniowej w Europie"[18]. Model chmury obliczeniowej zdefiniowano w nim jako przechowywanie, przetwarzanie i wykorzystanie danych, do których dostęp uzyskuje się przez internet, na znajdujących się w innej lokalizacji komputerach. Oznacza to, że użytkownicy mogą na życzenie dysponować nieograniczonymi mocami obliczeniowymi, nie muszą dokonywać znacznych inwestycji kapitałowych w celu zrealizowania swoich potrzeb oraz mogą uzyskiwać dostęp do swoich danych z każdego miejsca, w którym mają połączenie z internetem. W komunikacie wskazano ponadto, że dzięki chmurze obliczeniowej będzie możliwe ograniczenie wydatków użytkowników na technologie informacyjne (IT) oraz opracowanie nowych usług. O ile światowa sieć internetowa (World Wide Web) oferuje dostęp do informacji wszystkim i wszędzie, o tyle chmura obliczeniowa pozwala na dostęp wszystkim i wszędzie do mocy obliczeniowej.

Reasumując, chmurę obliczeniową można określić jako model informatyzacji, w którym do realizacji zadań informatycznych, czyli przechowywania i przetwarzania danych, wykorzystuje się zewnętrzne, tj. znajdujące się poza przedsiębiorstwem, zasoby komputerowe (sprzęt, oprogramowanie) udostępniane użytkownikom z wykorzystaniem internetu[19].

Chmura obliczeniowa bazuje na architekturze zorientowanej na usługi informatyczne (Service-Oriented Architecture). Główną funkcją chmury obliczeniowej jest dostarczanie na życzenie użytkownika różnego rodzaju usług. Do tych najpopularniejszych należą: 1) chmura aplikacyjna (cloud applications) – obejmuje ona usługi związane z dostarczaniem i dystrybucją oprogramowania. Software as a Service (SaaS) – oprogramowanie jako usługa, w tym model sprzętu, platforma oraz odpowiednio skonfigurowane aplikacje udostępniane są przez usługodawcę użytkownikowi[20]. Użytkownik końcowy widzi w swoim systemie tylko i wyłącznie aplikacje, z których korzysta. Sprzęt i platforma nie są dla użytkownika widoczne – działają one na serwerze dostawcy (usługodawcy), dostęp do nich ma tylko usługodawca. Jednym z elementów

18 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów Wykorzystanie potencjału chmury obliczeniowej w Europie, COM/2012/0529 final.

19 J. Kudła, A. Staszak, op. cit., s. 39; J. Jurek, *Wdrożenia informatycznych systemów zarządzania*, Warszawa 2016, s. 70–73.

20 Ł. Pirożek, *Prawne aspekty świadczenia usług w modelu SaaS przez przedsiębiorcę telekomunikacyjnego*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2015, nr 6, s. 76.

dotyczącym udostępniania oprogramowania w modelu SaaS jest interfejs użytkownika; 2) chmura ze „środowiskiem oprogramowania" (Cloud Software Environment) określana jest także jako PaaS – Platform as a Service. Polega ona na udostępnianiu przez dostawcę wirtualnego środowiska (platformy) pracy. W tym modelu użytkownik otrzymuje komplet aplikacji, co nie wiąże się z koniecznością zakupu przez użytkownika sprzętu ani instalacją oprogramowania. Użytkownik ma dostęp do interfejsu poprzez program klienta – przeglądarkę internetową. Świadczone usługi są dostępne z dowolnego komputera połączonego z siecią internet; 3) chmura z infrastrukturą do oprogramowania (Cloud Software Infrastructure) obejmuje infrastrukturę informatyczną, czyli sprzęt, serwery odpowiedzialne za uruchamianie istniejących aplikacji i systemów operacyjnych (Infrastructure as a Service – IaaS), usługi związane z przechowywaniem i gromadzeniem danych oraz udostępnianie ich na żądanie użytkownika (Data as a Service – DaaS) oraz usługi związane z zapewnieniem optymalizacji pracy programów poprzez kontrolę ich środowiska działania i procesu translacji kodu (Communications as a Service – CaaS). Infrastruktura jako usługa IaaS to model, w którym usługodawca dostarcza usługobiorcy cały sprzęt, infrastrukturę informatyczną, czyli oprogramowanie, usługi serwisowania, komputery, urządzenia do przechowywania danych, serwery. Co do zasady sprzęt ten jest własnością dostawcy usług w chmurze obliczeniowej, a nie użytkownika, który uzyskuje jedynie dostęp do chmury za pośrednictwem internetu[21]. Komunikacja jako usługa (Communications as a service – Caas) polega na tym, że usługodawca zapewnia platformę pod telekomunikacyjne środowisko pracy.

Inny prezentowany podział chmury obliczeniowej wyróżnia chmury prywatną, publiczną i hybrydową. Wszystkie zasoby chmury prywatnej są przeznaczone do korzystania tylko dla jednego podmiotu. Chmura prywatna może być usługą albo infrastrukturą przeznaczoną dla jednego klienta i nie jest dostępna dla innego użytkownika. Zasoby chmury publicznej udostępnia się wielu odbiorcom, którzy mogą korzystać z tego samego sprzętu i oprogramowania. Różnica polega na tym, że w przypadku chmury publicznej dostawca powinien zapewnić odpowiednią separowalność danych[22]. W przypadku chmury hybrydowej część jej zasobów jest przeznaczona do korzystania dla jednego wyznaczonego podmiotu, inna zaś jej część jest udostępniana publicznie.

21 M. Siwicki, op. cit., s. 31; J. Kudła, A. Staszak, op. cit., s. 39.
22 Ibidem, s. 41.

Podsumowując przeprowadzone rozważania, można stwierdzić, że chmura obliczeniowa nie jest ograniczona geograficznie i co do zasady dostępna jest z każdego miejsca na świecie. Tworzy ona zbiór usług cyfrowych, i jest stale rozwijana. Wykorzystany sprzęt w chmurze obliczeniowej co do zasady nie jest dostępny dla użytkownika końcowego i często nie ma on wiedzy, który sprzęt i w jakim momencie faktycznie go obsługuje. W celu możliwie najlepszego wykorzystania sprzętu w chmurze obliczeniowej dostawcy usług często przenoszą dane i aplikacje poszczególnych użytkowników.

Można wskazać następujące cechy chmury obliczeniowej: 1) samoobsługa na żądanie – dostęp do nowych zasobów obliczeniowych jest możliwy bez konieczności kontaktu z dostawcą usługi; 2) nieograniczony dostęp do sieci za pośrednictwem każdego urządzenia z dostępem do internetu; 3) wielodzierżawa, tj. agregacja pozwalająca na gromadzenie i dzielenie zasobów między wielu użytkowników jednocześnie; 4) elastyczność; 5) mierzalność usługi (zakres i intensywność korzystania z danej usługi musi być na bieżąco monitorowania)[23].

Użytkownicy mogą korzystać z usługi przetwarzania w chmurze obliczeniowej w celu przechowywania na tzw. serwerze wirtualnym wszystkich dostępnych informacji. Dane te, w postaci różnego rodzaju dokumentów cyfrowych, są przekazywane do zasobów chmury obliczeniowej np. pocztą elektroniczną. Tak zapisane w chmurze pliki cyfrowe pozwalają na ich odtworzenie w momencie dowolnie wybranym przez użytkownika.

Podstawy prawne dostępu organów procesowych do danych przechowywanych w chmurze obliczeniowej

W prawie polskim zagadnienie przeszukania środowiska informatycznego zostało uregulowane w ustawie z 6 czerwca 1997 roku kodeks postępowania karnego[24]. Regulacje dotyczące pozyskiwania dowodów elektronicznych[25] znajdują się przede wszystkim w art. 217, 218, 218a, 219, 236a, 237, 241.

23 E. Molenda-Kropielnicka, op. cit., s. 111; J. Wrona, Z. Zawadzka, op. cit., s. 378; F. Radoniewicz, *Przeszukanie systemów informatycznych oraz informatycznych nośników danych w kodeksie postępowania karnego*, „Cybersecurity and Law" 2022, nr 2, s. 152–153.

24 Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego, t.j., Dz.U. 2022, poz. 1375, z późn. zm.

25 A. Lach, *Dowody elektroniczne w procesie karnym*, Toruń 2004, s. 94.

Procesowe zasady przeszukania i zatrzymania danych informatycznych

Na wstępie należy zaznaczyć, że rozdział 25 k.p.k. jest poświęcony zatrzymaniu rzeczy i przeszukaniu. Podstawą przeszukania jest uzasadnione podejrzenie, że osoby poszukiwane lub poszukiwane rzeczy (dane informatyczne) znajdują się tam, gdzie są poszukiwane[26]. Należy podkreślić, że danych informatycznych nie należy traktować jako rzeczy w rozumieniu karnoprocesowym. Dane informatyczne stanowią odrębną kategorię niematerialnych źródeł dowodowych[27]. Przepisy rozdziału 25 „Zatrzymanie rzeczy. Przeszukanie", zgodnie z art. 236a k.p.k., znajdują do nich jednak odpowiednie zastosowanie. Dyspozycja art. 236a stanowi, że „[...] przepisy rozdziału niniejszego 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, w tym korespondencji przesyłanej pocztą elektroniczną".

Należy wyraźnie wskazać różnice i oddzielić przeszukanie od zatrzymania rzeczy, które zostały określone w art. 217 i 219 k.p.k. Od zatrzymania rzeczy przeszukanie różni się przede wszystkim wyższym stopniem ingerencji, gdyż łączy się z penetracją pomieszczeń, odzieży, zasobów pamięci systemu informatycznego. Ponadto przeszukanie stanowi wykrywczą czynność dowodową, która jednocześnie jest środkiem przymusu pozwalającym na wkroczenie w określoną sferę praw i wolności jednostki[28].

W wypadku pozyskiwania danych przetwarzanych w chmurze zastosowanie znajdzie art. 217 k.p.k. w zw. z art. 236a, zgodnie z którym możliwe jest żądanie wydania danych przechowywanych na urządzeniu, w systemie lub na nośniku od dysponenta lub użytkownika tego urządzenia, nośnika lub systemu. Po drugie, możliwe będzie także przeszukanie urządzenia lub systemu informatycznego w celu znalezienia danych mogących stanowić dowód w sprawie na podstawie art. 219 w zw. z art. 236a k.p.k. Wreszcie, możliwe jest żądanie wydania korespondencji elektronicznej oraz wykazów połączeń teleinformatycznych na podstawie art. 218 w zw. z art. 236a k.p.k.

Należy podkreślić, że nie chodzi tu o przeszukanie w znaczeniu tradycyjnym, ale o penetrację[29] – przy użyciu odpowiedniego oprogramowania –

26 M. Siwiecki, P. Kowalski, op. cit., s. 4.
27 M. Siwicki, op. cit., s. 37; A. Lach, op. cit., s. 94.
28 M. Siwiecki, P. Kowalski, op. cit., s. 4.
29 M. Siwicki, op. cit., s. 37.

zawartych w urządzeniu lub systemie danych w celu znalezienia i zabezpieczenia ich dla procesu. Istotne jest tu rozróżnienie danych technicznych – związanych z przekazem informacji, miejsca logowań do systemu, wielkości i charakterystyki przekazywanych plików – od danych merytorycznych, treściowo istotnych z punktu widzenia realizacji celów postępowania karnego.

Dane te na urządzeniu mobilnym mogą znajdować się w pamięci urządzenia lub systemie plików. System plików jest organizowany i zarządzany przez system operacyjny urządzenia (SO)[30]. W przypadku utworzenia przez użytkownika informacji system operacyjny określa, gdzie w systemie plików można zapisać dane i zarządza sposobem ich pobierania. W przypadku usunięcia danych SO usuwa te informacje z systemu plików. Zdarza się, że system operacyjny nie usuwa informacji z systemu plików, usuwa jedynie odniesienie do tej części systemu. W takim wypadku dane pozostają w systemie plików do momentu, w którym zostaną nadpisane nowymi danymi. Dane te można także odzyskać za pomocą odpowiedniego oprogramowania[31].

Stosowane oprogramowanie kryminalistyczne powinno wydobywać zarówno dane znajdujące się na urządzeniu, jak i wszelkie usunięte informacje. Zasadne jest opracowywanie takich oprogramowań dla organów procesowych, które zapewniałyby, że wszystkie dane odzyskane z urządzeń są wiarygodne, dokładne i mogą być wykorzystane jako dowody w postępowaniu sądowym. Oprócz zapewnienia, że odpowiednie dane (merytoryczne treściowo z punktu widzenia realizacji celów postępowania karnego) zostaną pobrane ważne jest także zapewnienie, że proces ten jest przejrzysty i możliwy do zweryfikowania. Szczególnie ważne jest upewnienie się, że dane na urządzeniu nie zostały w żaden sposób zmodyfikowane. Dostęp do kryminalistycznych urządzeń zbierających dane powinien być kontrolowany, a wszystkie dane przeniesione do kopii zapasowej. Oznacza to, że wszelkie analizy powinny być wykonywane na skopiowanych danych, podczas gdy oryginał jest bezpiecznie przechowywany[32].

Procesowe zasady kontroli i utrwalania rozmów

Rozdział 26 k.p.k. jest poświęcony kontroli i utrwalaniu rozmów. Po wszczęciu postępowania sąd, na wniosek prokuratora, może zarządzić kontrolę i utrwalanie treści rozmów telefonicznych w celu wykrycia i uzyskania dowodów dla

30 W iPhonach system ten nosi nazwę iOS lub Android w smartfonach Google.
31 D. Kahvedžic, op. cit., s. 358.
32 Ibidem, s. 360.

toczącego się postępowania lub zapobieżenia popełnieniu nowego przestępstwa. Ustawodawca w art. 237 § 3 k.p.k. w katalogu zamkniętym wskazał enumeratywnie przestępstwa, co do których można przeprowadzać tę czynność. W literaturze przedmiotu słusznie podkreśla się, że zarządzenia podsłuchu telefonicznego w sprawie o przestępstwo niekatalogowe nie uzasadnia nawet interes społeczny wielkiej wagi[33].

Zgodnie z art. 241 k.p.k. przepisy rozdziału o kontroli i utrwalaniu rozmów stosuje się odpowiednio do kontroli oraz do utrwalania z wykorzystaniem środków technicznych treści innych rozmów lub przekazów informacji, w tym korespondencji przesyłanej pocztą elektroniczną. Oznacza to, że dopuszczalne jest podsłuchiwanie treści wiadomości przesyłanych przez internet. Jednakże warto zauważyć, że ustawa ogranicza pod względem przedmiotowym stosowanie podsłuchu do enumeratywnie wyliczonych w § 3 art. 237 k.p.k. najcięższych przestępstw. Zdaniem Siwickiego „[...] takie przedmiotowe ograniczenie podsłuchu komputerowego powoduje sytuację, w której jego zastosowanie będzie wyłączone w stosunku do najczęstszych cyberprzestępstw. Obecnie zakresem zastosowania kontroli i utrwalania treści rozmów objęte będą mogły być jedynie sprawy o szpiegostwo lub ujawnienie informacji niejawnych o klauzuli tajności »tajne« lub »ściśle tajne«, przechowywanych w chmurze obliczeniowej”[34]. Jedną z technik pozwalających analizować pakiety przesyłane przez sieć komputerową jest tzw. głęboka inspekcja pakietów (Deep Packet Inspection).

Transgraniczność usług świadczonych w chmurze

Dane przechowywane w chmurze mogą stanowić ważny dowód w postępowaniu sądowym. Obecne narzędzia kryminalistyczne mają możliwości wyodrębnienia potencjalnych dowodów z chmury z urządzenia mobilnego. Wprawdzie nie mogą one otrzymać dostępu do samej usługi w chmurze, ale dostarczają wskazówek, do których usług w chmurze mógł być uzyskany dostęp[35].

Można ponadto wywnioskować, które chmury prawdopodobnie zostały użyte na podstawie typu danego urządzenia. Apple iPhone posiada głęboką

33 K. Boratyńska, P. Czarnecki, A. Lach, *Komentarz do art. 237 k.p.k.* [w:] *Kodeks postępowania karnego*, *Komentarz*, red. A. Sakowicz, Warszawa 2023.
34 M. Siwicki, op. cit., s. 37.
35 D. Kahvedžic, op. cit., s. 364.

integrację z iCloud, telefony z systemem Android korzystają z Google Drive, a telefony z systemem Windows zazwyczaj z OneDrive firmy Microsoft. W najnowszych urządzeniach korzystanie z chmury jest wyraźnie zachęcane już przy pierwszym uruchomieniu urządzenia. Przyjęcie chmury jako zewnętrznego medium pamięci masowej wzrosło ze względu na darmową (lub tanią) jej dostępność oraz rosnącą szybkość łączności, na którą pozwalają szybsze sieci telekomunikacyjne. Jako przykład można wskazać aplikację Microsoft Office, która pozwala użytkownikom zapisywać swoje dokumenty poza urządzeniem bezpośrednio do chmury Microsoftu. Jest to jeden z przykładów oprogramowania łączącego swoje usługi z chmurą. Dostęp do chmury jest coraz częściej ułatwiony i zintegrowany z istotą funkcjonalności urządzenia.

Przeszukanie danych w chmurze stawia przed organami ścigania nowe wyzwania. Głównym problemem jest to, że dane są przechowywane przez dostawcę chmury w imieniu użytkownika. Użytkownik – co do zasady – nie wie, gdzie dane są przechowywane dopóki może je odzyskać za pomocą urządzenia mobilnego. Wszechobecność danych jest jedną z głównych cech chmury, ale jest również jednym z głównych problemów organów śledczych[36].

Międzynarodowy charakter chmury obliczeniowej może utrudniać prowadzenie śledztwa i pozyskiwanie dowodów elektronicznych. Należy podkreślić, że w przeciwieństwie do urządzenia mobilnego, miejscem przechowywania danych w chmurze jest centrum danych należące do dostawcy chmury, do którego nie można uzyskać dostępu ani go przejąć w taki sam sposób jak do urządzeń mobilnych. Organy procesowe przy użyciu specjalistycznych urządzeń nie mogą uzyskać dostępu do danych bez właściwych danych uwierzytelniających użytkownika.

Dla pozyskiwania dowodów z urządzeń mobilnych podstawowe znaczenie ma obrazowanie. Metoda ta polega na wyodrębnianiu kopii wszystkich informacji przechowywanych w systemie plików urządzenia. Celem tego procesu jest stworzenie dokładnego duplikatu danych, co umożliwia organowi ścigania przeprowadzenie dokładnego dochodzenia na kopii danych urządzenia, a nie na oryginale.

Oprócz wydobywania danych, które były widziane i do których użytkownik ma dostęp, specjalistyczne oprogramowania stosowane przez organy ścigania mają także możliwość zobrazowanie informacji wcześniej usuniętych. Dostęp do tych obszarów jest zwykle uniemożliwiony przez system operacyjny

36 Ibidem, s. 362.

urządzenia. Z punktu widzenia przeszukania i zdobycia istotnych informacji ważne jest obejście tych zabezpieczeń i uzyskanie dostępu do tych obszarów w sposób kontrolowany, żeby ujawnić ukryte w nich informacje.

W literaturze przedmiotu wskazuje się dwa główne rodzaje obrazowania, tj. fizyczne i logiczne[37].

Obrazowanie fizyczne jest metodą, w której system operacyjny urządzenia jest całkowicie pomijany, a wszystkie informacje są odczytywane bezpośrednio z systemu plików. Zapewnia ona, że wszystkie dane, które znajdują się na urządzeniu, są z niego kopiowane. Gwarantuje to, że wszystkie usunięte, ukryte i tymczasowe pliki są niezawodnie kopiowane bez oporu przez jakiekolwiek zabezpieczenia systemu operacyjnego. Poprzez pominięcie systemu operacyjnego uprawniony organ nie wie jak pliki są zorganizowane w systemie plików. Fizyczne wyodrębnianie danych jest wykonywane najrzadziej, ponieważ uzyskanie pełnego dostępu do pamięci wewnętrznej urządzenia mobilnego jest całkowicie zależne od systemu operacyjnego i środków bezpieczeństwa zastosowanych przez producentów. Fizyczne wydobywanie danych z urządzenia mobilnego opiera się na tej samej podstawowej koncepcji, co fizyczne obrazowanie kryminalistyczne dysku twardego komputera (kopia binarna). Fizyczne pozyskiwanie polega na wykonywaniu kopii bit po bicie całej zawartości pamięci flash urządzenia mobilnego. Ta metoda umożliwia gromadzenie wszystkich danych istniejących, a także danych, które zostały usunięte lub są ukryte przez użytkownika[38].

Obrazowanie logiczne to proces, w którym dane są zbierane za pomocą systemu operacyjnego. Oprogramowanie do obrazowania żąda danych od systemu operacyjnego i zbiera dane, które są mu dostarczane. Ten proces obrazowania zależy od dostępu, który umożliwia system operacyjny. W obrazowaniu logicznym narzędzia kryminalistyczne komunikują się z systemem operacyjnym urządzenia mobilnego. Proces pozwala na pobieranie większości widocznych danych. Urządzenie do badania musi zostać uruchomione (następuje nieuniknione, ale udokumentowane naruszenie integralności danych)[39].

Proces obrazowania logicznego pozwala na zebranie takich danych, jak m.in.: dzienniki połączeń, SMS, zdjęcia, nagrania wideo, kontakty. Nie jest on tak kompleksowy jak proces obrazowania fizycznego. Jest to po prostu zbiór

37 Ibidem, s. 360.
38 *Mobilna informatyka śledcza*, https://olszta.it/strona-1/mobilna-informatyka-sledcza/ [dostęp: 2.01.2023].
39 Ibidem.

treści, które OS umożliwia badaczowi. System operacyjny nie pobiera żadnych informacji, do których nie ma dostępu, takich jak wcześniej usunięte pliki. Obrazowanie logiczne przeprowadza się tylko wtedy, kiedy nie ma dostępu do fizycznego systemu plików lub nie jest znany sposób, w jaki system operacyjny przechowuje swoje pliki. Obrazowanie fizyczne jest zawsze preferowaną metodą, ponieważ skutkuje bardziej niezawodnym i kompleksowym przechwytywaniem danych[40].

W tym miejscu należy podkreślić, że dostawcy usług działają w imieniu użytkowników i są zobowiązani do zapewnienia ochrony prywatności i bezpieczeństwa ich danych. Prywatność i bezpieczeństwo danych odgrywają coraz większą rolę w opracowywaniu urządzeń przez producentów[41]. Coraz częściej urządzenia są blokowane za pomocą złożonego kodu, wzoru, hasła lub odcisku palca. Skutkuje to rygorystycznymi kontrolami dostępu, a przede wszystkim domyślnym pełnym szyfrowaniem dysku. Przykładowo, po ustawieniu kodu PIN w telefonie iPhone wszystkie dane na urządzeniu są zaszyfrowane i nie mogą być dostępne dla nieuprawnionych użytkowników. Według szacunków firmy Apple odgadnięcie kodu PIN poprzez wypróbowanie wszystkich możliwych kombinacji zajęłoby nawet pięć i pół roku. Powoduje to, że w obecnych smartfonach organy ścigania nie mają możliwości odblokowania urządzenia bez kodu dostępu. Producenci urządzeń poprzez wprowadzanie coraz to silniejszych zabezpieczeń uniemożliwiają dowolnej aplikacji bezpośredni dostęp do systemu plików nawet po jego odblokowaniu. Wpływa to na funkcjonowanie organów ścigania, w aspekcie poszukiwania przez nich istotnych dowodów. Funkcje te uniemożliwiają oprogramowaniu kryminalistycznemu zignorowanie systemu operacyjnego i uzyskanie dostępu do systemu plików. Jedynym sposobem, w jaki dane mogą być skopiowane z urządzenia, pozostaje obrazowanie logiczne przez system operacyjny. Oznacza to, że preferowane fizyczne obrazowanie urządzeń raczej nie będzie normą w najbliższej przyszłości, a uprawnione organy będą skupione na metodzie obrazowania logicznego.

Podsumowując, w urządzeniach mobilnych coraz częściej stosuje się szyfrowanie w celu zakodowania danych na urządzeniach w bezpieczny sposób. W połączeniu z silnymi kodami dostęp do urządzenia stał się znacznie trudniejszy dla organów ścigania. Ponieważ producenci zaczęli ograniczać urządzenia poprzez ich zabezpieczenia, otworzyli je zatem także pod względem ich

40 D. Kahvedžic, op. cit., s. 362.
41 Ibidem, s. 364.

integracji z internetem. Dodawane są funkcje, które w coraz większym stopniu opierają się na łatwości i wszechobecności chmury w celu tworzenia kopii zapasowych danych i łączenia użytkownika z różnymi usługami w chmurze. Chmura pozwoliła producentom zaoferować swoim użytkownikom praktycznie nieograniczoną przestrzeń dyskową do celów takich, jak: kopia zapasowa danych osobowych, przepływ danych między urządzeniami czy udostępnianie informacji w sieciach społecznościowych.

W odniesieniu do wydobywania danych z chmury kopię tych danych można uzyskać w taki sam sposób, w jaki na urządzeniu mobilnym dokonuje się przejęć logicznych. Dane są kopiowane z chmury na bezpieczne i kontrolowane urządzenie. Możliwe jest zażądanie kopii danych od dostawcy usług za pomocą odpowiedniego wniosku, wezwania lub nakazu sądowego, ale to dostawca chmury odpowiada na te wnioski i wydobywa te dane. Praktyka w tym zakresie jest niejasna i w dużej mierze zależy od dostawcy. Kolejnym problemem jest to, że dostawcy usług w chmurze tworzą kopie zapasowe danych w wielu lokalizacjach ze względu na redundancję, opóźnienia i tworzenie kopii zapasowych. Dlatego dane mogą znajdować się w wielu jurysdykcjach i mogą podlegać polityce ochrony danych wielu krajów. Jako przykład skutków prawnych można wskazać sprawę Microsoftu. Firma Microsoft odmówiła przekazana danych poczty elektronicznej przechowywanych w Irlandii na wniosek amerykańskich organów ścigania. Microsoft zakwestionował zdolność Stanów Zjednoczonych Ameryki do gromadzenia tych danych za pomocą amerykańskiego nakazu i zwrócił się do amerykańskich organów ścigania, żeby zamiast tego wystąpiły do sądu irlandzkiego o nakaz sądowy[42].

Zakończenie

Chmura obliczeniowa i urządzenia mobilne są ze sobą ściśle powiązane. Oba urządzenia sprawiły, że przechowywanie, tworzenie i udostępnianie danych stało się niezwykle łatwe w codziennym użytkowaniu. Wraz ze wzrostem ilości danych przechowywanych przez te urządzenia wzrosło także zainteresowanie organów ścigania pozyskiwaniem oraz analizą tych informacji.

Do wydobywania danych z urządzeń mobilnych stosowany jest proces zarówno logiczny, jak i fizyczny. Jak wykazano w opracowaniu, obrazowanie

42 Ibidem.

fizyczne jest preferowaną metodą, ponieważ wydobywa wszystkie możliwe przechowywane na urządzeniu dane. Ponieważ producenci urządzeń, w wyniku stosowanych zabezpieczeń, uniemożliwiają innym aplikacjom bezpośredni dostęp do systemu plików, więc uprawnione organy mają utrudniony dostęp do tych danych. Jedynym sposobem skopiowania danych z urządzenia pozostaje obrazowanie logiczne przez system operacyjny. Oznacza to, że preferowane fizyczne obrazowanie urządzeń raczej nie będzie normą w najbliższej przyszłości, a uprawnione organy będą skupione na metodzie obrazowania logicznego.

Przeprowadzone rozważania pozwalają ponadto wskazać na dychotomiczną rolę dostawców usług w chmurze. Z jednej strony odgrywają oni istotną rolę w poszukiwaniu przez uprawnione organy istotnych dowodów, z drugiej, działają oni również w imieniu użytkowników i są zobowiązani do zapewnienia ochrony prywatności i bezpieczeństwa danych swoich użytkowników. Prywatność i bezpieczeństwo danych odgrywają coraz większą rolę w opracowywaniu urządzeń przez producentów. Te same zasady są stosowane przez twórców chmur, co może powodować, że uprawnione organy będą miały coraz trudniejszy lub niemożliwy dostęp do potrzebnych im danych[43].

Wzrost zainteresowania nowym modelem przetwarzania danych – chmurą obliczeniową – wymaga także powszechnej dyskusji na temat potrzeby podjęcia międzynarodowej współpracy w zdobywaniu dowodów cyfrowych. Dane w chmurze charakteryzuje to, że poprzez stosowaną metodę zapisywania informacji na kilkunastu urządzeniach zlokalizowanych w różnych państwach znajdują się one w wielu jurysdykcjach i mogą podlegać polityce ochrony danych wielu krajów.

Bibliografia

Boratyńska K., Czarnecki P., Lach A., *Komentarz do art. 237 k.p.k.* [w:] *Kodeks postępowania karnego, Komentarz*, red. A. Sakowicz, Warszawa 2023.

Casino F. i in., *SoK: cross-border criminal investigations and digital evidence*, „Journal of Cybersecurity" 2022, t. 8.

Chałubińska-Jentkiewicz K., *Prawna ochrona treści cyfrowych*, Warszawa 2022.

Chałubińska-Jentkiewicz K., Nowikowska M., *Bezpieczeństwo, tożsamość, prywatność – aspekty prawne*, Warszawa 2020.

Etzioni A., *Privacy in a cyber age, Policy and Practice*, Hampshire 2015.

Gobeo A., Fowler C., Buchanan W.J., *GDPR and Cyber Security for Business Information Systems*, Gistrup 2018.

Jurek J., *Wdrożenia informatycznych systemów zarządzania*, Warszawa 2016.

43 Ibidem, s. 365.

Kahvedžic D., *Digital forensics and DSAR effect in ERA Forum*, t. 22, Berlin 2021.
Kudła J., Staszak A., *Procesowa i operacyjna kontrola korespondencji przechowywanej w tzw. chmurze*, „Prokuratura i Prawo" 2017, nr 8–7.
Lach A., *Dowody elektroniczne w procesie karnym*, Toruń 2004.
Molenda-Kropielnicka E., *Cloud Computing – zagadnienia prawne*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej" 2013, nr 119.
Pirożek Ł., *Prawne aspekty świadczenia usług w modelu SaaS przez przedsiębiorcę telekomunikacyjnego*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2015, nr 6.
Radoniewicz F., *Przeszukanie systemów informatycznych oraz informatycznych nośników danych w kodeksie postępowania karnego*, „Cybersecurity and Law" 2022, nr 2.
Siwicki M., *Przetwarzanie danych informatycznych w chmurach obliczeniowych. Wybrane aspekty prawnokarne i procesowe*, „Palestra" 2015, nr 1–2.
Siwiecki M., Kowalski P., *Przeszukanie i zatrzymanie rzeczy w sprawach o cyberprzestępstwa. Udział specjalistów i biegłych w czynnościach procesowych*, „Kwartalnik Policyjny" 2021, t. 57, nr 2.
Szumiło-Kulczycka D., *Między ochroną prywatności a bezpieczeństwem – uwagi na tle orzecznictwa ETPCz i TSUE* [w:] *Pozyskiwanie informacji w walce z terroryzmem*, red. P. Herbowski, D. Słapczyńska, D. Jagiełło, Warszawa 2017.
Wrona J., Zawadzka Z., *Cyberbezpieczeństwo w prawie własności intelektualnej* [w:] *Cyberbezpieczeństwo. Zarys wykładu*, red. C. Banasiński, Warszawa 2018.

Procedural surveillance of correspondence stored in the cloud computing

Abstract

The article attempts to analyze the process control of correspondence stored in virtual memory, i.e. in the so-called Cloud Computing. The study is an attempt to answer the question of how mobile devices and clouds are examined and what impact the law on privacy has on the implementation of procedural activities. The growing interest in cloud computing results in the emergence of many new legal problems, which translate into, among others, on the practice and operation of law enforcement agencies. First, the concept of „cloud computing" was discussed and the provisions on obtaining electronic evidence were analyzed. The independence of ICT systems from the functioning of a classic work environment based on a single workstation also allowed us to raise the question of the cross-border nature of services provided in the cloud. IT data transmitted via cloud computing can be saved on several devices located in different countries.

Key words: cloud computing, physical imaging, logical imaging, search, securing evidence