Jonasz Szpoton

Zabezpieczanie i zatrzymywanie danych informatycznych w polskim postępowaniu karnym

Streszczenie

Artykuł omawia problematykę zabezpieczania i zatrzymywania danych informatycznych w polskiej procedurze karnej. Przedstawia podstawowe pojęcia związane z podejmowaniem tych czynności w sferze cyfrowej oraz porównuje je do metod klasycznych. Prezentuje cechy oraz sposoby zabezpieczenia danych informatycznych oraz określa zakres zastosowania przepisów dotyczących przeszukania oraz zatrzymania rzeczy w kontekście wirtualnym. W dalszej części autor prezentuje problemy związane z gromadzeniem danych informatycznych oraz przedstawia propozycje zmian mających na celu usprawnienie działania omawianej instytucji.

1. Wstęp

Wraz z rozwojem technologii problematyka pozyskiwania dowodów w ramach postępowania karnego nabiera nowego znaczenia. Jak ukazują statystyki[1], coraz więcej czynów zabronionych ma charakter tzw. cyberprzestępstw, czyli przestępstw w zakresie czynów skierowanych przeciwko systemowi komputerowemu i czynów dokonanych przy użyciu komputera jako narzędzia[2]. W związku z rosnącą liczbą przestępstw komputerowych zaistniała konieczność interwencji ustawodawcy w zakresie regulacji problematyki gromadzenia danych informatycznych przez organy ścigania, czego efektem jest m. in. wejście w życie art. 218a wraz z późniejszymi nowelizacjami, czy też obecność art. 236a Kodeksu postępowania karnego[3]. Celem niniejszego opracowania jest analiza regulacji kodeksowej i przepisów wykonawczych dotyczących pozyskiwania materiału cyfrowego na gruncie polskiej procedury

[1] Zob. raport CERT Polska (NASK), *Raport roczny z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego internetu*, 2021, s. 20.
[2] Międzynarodowa Organizacja Policji Kryminalnych „Interpol", https://www.interpol.int [dostęp 14.6.2023].
[3] Ustawa z 6.6.1997 r. - Kodeks postępowania karnego (t.j. Dz. U. z 2024 r. poz. 37), dalej: „k.p.k.", „Kodeks".

karnej, także w kontekście standardów Rady Europy w tym zakresie oraz omówienie problematyki związanej z metodami zabezpieczania i zatrzymywania danych informatycznych.

2. Podstawowe pojęcia

Przed przystąpieniem do analizy tematyki zabezpieczania i zatrzymywania danych informatycznych należy dokonać niezbędnej systematyzacji pojęciowej, która to — biorąc pod uwagę istotę problemu — wydaje się nadzwyczaj istotna. W szczególności wynika to ze specyfiki stosowanych wyrażeń oraz z faktu, że w wielu przypadkach stosowanie zwrotów mających swoją genezę w sferze materialnej do domeny wirtualnej może napotykać pewne problemy natury konceptualnej.

Po pierwsze należy sprecyzować znaczenie pojęcia danych informatycznych. W doktrynie rozumie się przez nie zapis określonej informacji przechowywanej na dysku komputera lub innym komputerowym nośniku informacji[4]. Ponadto zgodnie z definicją legalną z art. 1 lit. b Konwencji o cyberprzestępczości[5]: „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". Konwencja wprowadza również charakterystyczne rozróżnienie na dane dotyczące ruchu („traffic data") oraz dane dotyczące treści („content data"). Zgodnie z art. 1 lit. d Konwencji: „dane dotyczące ruchu oznaczają dowolne dane informatyczne odnoszące się do komunikowania się za pomocą systemu informatycznego, wygenerowane przez system informatyczny, który utworzył część w łańcuchu komunikacyjnym, wskazujące swoje pochodzenie, przeznaczenie, ścieżkę, czas, datę, rozmiar, czas trwania lub rodzaj danej usługi". Mogą mieć one formę statyczną (np. pod postacią logów zapisanych na serwerze) lub dynamiczną, zachodzącą w czasie rzeczywistym. Przykładem danych dotyczących ruchu są adresy IP. Konwencja nie definiuje jednocześnie pojęcia danych dotyczących treści, posługuje się nim jednak m. in. w art. 21 w zakresie obowiązku wprowadzenia przez strony regulacji nadających właściwym organom uprawnienia do ich przechwytywania czy art. 18 ust. 3 w celu zdefiniowania informacji odnoszących się

[4] A. Adamski, *Prawo karne komputerowe*, C.H. Beck, Warszawa 2000, s. 40.
[5] Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz. U. z 2015 r. poz. 728), dalej: „Konwencja".

do abonenta. Wydaje się, że są to wszelkiego rodzaju dane informatyczne inne niż dane dotyczące ruchu, np. pliki zawierające dokumenty tekstowe czy programy komputerowe.

Dysponentem jest osoba upoważniona do rozporządzania systemem, mającą go do dyspozycji, rozporządzającą nim według swego uznania, np. administratora sieci[6]. Pod pojęciem użytkownika rozumie się natomiast osobę używającą systemu, korzystającą z niego, eksploatującą go, czerpiącą jakieś korzyści z cudzego systemu, np. posiadacza konta poczty elektronicznej[7].

Po drugie, aby prawidłowo ustalić znaczenie przepisów rozdziału 25 k.p.k. w kontekście cyfrowym należy nakreślić chociażby podstawowe cechy instytucji zatrzymania rzeczy w aspekcie materialnym. Zgodnie z dominującym w doktrynie stanowiskiem poprzez zatrzymanie rzeczy rozumie się wydanie jej (w zależności od etapu postępowania) na żądanie sądu lub prokuratora. Może mieć ono charakter dobrowolny bądź też rzeczy mogą zostać przymusowo odebrane po uprzednim przeszukaniu. W postępowaniu przygotowawczym przeszukanie jest dopuszczalne na podstawie wydanego uprzednio postanowienia prokuratora albo w wypadkach niecierpiących zwłoki bez postanowienia prokuratora. W postępowaniu sądowym natomiast na podstawie wydanego uprzednio postanowienia sądu albo w wypadkach niecierpiących zwłoki bez postanowienia sądu. Doniosłe znaczenie praktyczne ma w tym przypadku fakt, że jeden z niewielu przejawów kontradyktoryjności postępowania przygotowawczego w postaci możliwości składania wniosków dowodowych przez strony implikuje również możliwość przeprowadzenia przeszukania na ich żądanie w przypadku pozytywnie rozpatrzonego wniosku dowodowego.

Katalog rzeczy podlegających zatrzymaniu określa § 159 Regulaminu wewnętrznego urzędowania powszechnych jednostek organizacyjnych prokuratury[8]. Są nimi rzeczy mogące stanowić dowód w sprawie, które:

1) służyły lub były przeznaczone do popełnienia przestępstwa;
2) zachowały na sobie ślady przestępstwa;
3) pochodzą bezpośrednio lub pośrednio z przestępstwa;
4) mogą służyć jako środek dowodowy do wykrycia sprawcy czynu lub ustalenia przyczyn okoliczności przestępstwa albo których posiadanie bez zezwolenia jest zabronione.

[6] D. Świecki (red.), B. Augustyniak, K. Eichstaedt, M. Kurowski, *Kodeks postępowania karnego. Komentarz aktualizowany.* Lex/el. 2023. Art. 236a, pkt 5.
[7] D. Świecki (red.), B. Augustyniak, K. Eichstaedt, M. Kurowski, op.cit.
[8] Rozporządzenie Ministra Sprawiedliwości z 7.4.2016 r. Regulamin wewnętrznego urzędowania powszechnych jednostek organizacyjnych prokuratury (t.j. Dz. U. z 2023 r. poz. 1115 z późn. zm.).

Ponadto w celu właściwej interpretacji art. 236a k.p.k. konieczne jest również sprecyzowanie znaczenia pojęcia odpowiedniego stosowania. Zgodnie z tezą wyroku SN z 24.5.2018 r. (sygn. IV KK 337/17)[9] odpowiednie stosowanie przepisu stanowi szczególny przykład analogii, która nie implikuje jednak bezwarunkowego obowiązku zastosowania wszystkich przepisów z odesłania. W zależności bowiem od różnic między konstrukcjami prawnymi, do których przynależy przepis odsyłający i przepis odesłania odpowiednie stosowanie może przybierać trojaki charakter. Po pierwsze, przepis odesłania może być stosowany wprost (tj. bez żadnych zmian do innego zakresu odniesienia[10]). Po drugie, przepis może być stosowany z odpowiednimi modyfikacjami, czy też w końcu po trzecie, jego zastosowanie może być całkowicie niedopuszczalne. Niedopuszczalność zastosowania przepisu do zakresu innego zagadnienia może wynikać z bezprzedmiotowości czy też sprzeczności z przepisami ustanowionymi dla rzeczonego zagadnienia.

3. Zabezpieczenie danych informatycznych

Artykuł 218a k.p.k. reguluje problematykę zabezpieczania danych informatycznych. Warto zauważyć, że przepis ten podlegał już znaczącym zmianom pod wpływem rozwoju technologicznego. Zakresem podmiotowym jego pierwotnej wersji, dodanej do k.p.k. w 2004 r.[11] objęte były jedynie na urzędy, instytucje państwowe i podmioty prowadzące działalność komunikacyjną. Znaczącej modyfikacji tego przepisu dokonano wskutek nowelizacji z 2021 r.[12], kiedy to katalog podmiotów zobowiązanych poszerzono o jednostki świadczące usługi drogą elektroniczną oraz dostawców usług cyfrowych (§ 1). Podmiotem zobowiązanym został również administrator treści w sytuacji zabezpieczania treści publikowanych lub udostępnianych drogą elektroniczną (§ 3). Ponadto w przypadku niektórych przestępstw przeciwko wolności seksualnej i obyczajności, przestępstwa polegającego na rozpowszechnianiu treści mogących ułatwić popełnienie przestępstwa o charakterze terrorystycznym oraz przestępstw określonych w rozdziale 7 ustawy o przeciwdziałaniu narkomanii[13] wprowadzono możliwość dodatkowego nałożenia obowiązku uniemożliwienia

[9] Prok. i Pr. 2018 nr 11, poz. 10.
[10] Wyrok SN z 15.2.2008 r., sygn. I CSK 357/07, OSNC 2009 nr 4, poz. 62, str. 83.
[11] Ustawa z 18.3.2004 r. o zmianie ustawy - Kodeks karny, ustawy - Kodeks postępowania karnego oraz ustawy - Kodeks wykroczeń (Dz. U. Nr 69, poz. 626), art. 2 pkt 2.
[12] Ustawa z 20.4.2021 r. o zmianie ustawy - Kodeks karny oraz niektórych innych ustaw (Dz.U. 1023), art. 3. Wejście w życie 22.06.2021.
[13] Ustawa z 29.7.2005 r. o przeciwdziałaniu narkomanii (t.j. Dz. U. z 2023 r. poz. 1939 z późn. zm.).

dostępu do tych danych. Sądy oraz prokuratura mogą dodatkowo (obok zabezpieczenia) zobowiązać podmioty do usunięcia treści publikowanych lub udostępnianych drogą elektroniczną w przypadku, gdy ich publikacja lub udostępnienie stanowiły czyn zabroniony (§ 4).

Celem instytucji zabezpieczenia danych informatycznych jest zapobieżenie ich utraty, w szczególności, gdy mogą mieć one istotne znaczenie dla postępowania. Obecność takiej regulacji wydaje się niezbędna ze względu na charakter danych informatycznych, które w wyjątkowo łatwy sposób mogą ulec deformacji, dezintegracji lub zniszczeniu.

Jak już wspomniano, organy uprawnione do zabezpieczania danych to (w zależności od etapu postępowania) sąd lub prokurator. Postanowienie powinno zawierać elementy wymienione w art. 94 k.p.k., a ponadto wymogiem szczególnym, zwłaszcza w przypadku zabezpieczenia danych dotyczących ruchu jest wskazanie dokładnej daty i godziny wygenerowania danych informatycznych na serwerze. Obowiązek ten jest konsekwencją dynamicznego charakteru adresów IP. Uzyskanie tego rodzaju danych bez wskazania momentu ich wygenerowania, w związku z brakiem możliwości identyfikacji użytkownika nie będzie więc możliwe.

Nie należy mylić instytucji zabezpieczenia danych informatycznych z ich zatrzymaniem. Jak wskazuje się w doktrynie, zabezpieczenie danych informatycznych powinno mieć charakter tymczasowy (do 90 dni). Jest to bowiem swoisty środka tymczasowego, mający na celu zapobieżenie zniszczeniu lub deformacji danych informatycznych, po którego zastosowaniu należy wydać osobne postanowienie o zatrzymaniu tych danych. W przypadku, jeśli okaże się, że zabezpieczone dane informatyczne nie mają znaczenia dla postępowania karnego, należy je niezwłocznie zwolnić spod zabezpieczenia[14].

Sposób zabezpieczenia danych informatycznych reguluje rozporządzenie Ministra Sprawiedliwości[15], wydane na podstawie delegacji ustawowej zawartej w art. 218b k.p.k. Zakresem przedmiotowym rozporządzenia objęte są procedury:

1) gromadzenia (zatrzymania) korespondencji, przesyłek oraz danych telekomunikacyjnych niestanowiących treści rozmowy telefonicznej lub innego przekazu informacji, jeżeli ich

[14] R. A. Stefański (red.), S. Zabłocki (red.), *Kodeks postępowania karnego. Tom II. Komentarz do art. 167-296.* Lex/el. 2018. Art. 218a, pkt 7.

[15] Rozporządzenie Ministra Sprawiedliwości z 18.6.2021 r. w sprawie sposobu technicznego przygotowania systemów i sieci służących do przekazywania informacji do gromadzenia danych informatycznych oraz danych niestanowiących treści rozmowy telefonicznej lub innego przekazu informacji, a także sposobów ich zabezpieczania w urządzeniach zawierających te dane oraz w systemach i na informatycznych nośnikach danych (Dz. U. poz. 1101), dalej jako: „rozporządzenie".

dysponentem są urzędy, instytucje i podmioty prowadzące działalność w dziedzinie poczty lub działalność telekomunikacyjną, urzędy celno-skarbowe oraz instytucje i przedsiębiorstwa transportowe [podkr. aut.] (§ 1 ust. 1 pkt 1 rozporządzenia w związku z art. 218 § 1 k.p.k.);
2) zabezpieczania danych informatycznych przechowywanych w urządzeniach zawierających te dane na nośniku lub w systemie informatycznym, jeżeli ich dysponentem są urzędy, instytucje i podmioty prowadzące działalność telekomunikacyjną lub świadczące usługi drogą elektroniczną oraz dostawcy usług cyfrowych [podkr. aut.] (§ 1 ust. 1 pkt 2 rozporządzenia);
3) zabezpieczania treści publikowanych lub udostępnianych drogą elektroniczną, przy czym podmiotem obowiązanym (dysponentem) do wykonania żądania sądu lub prokuratora może być również administrator treści [podkr. aut.] (§ 1 ust. 1 pkt 3 rozporządzenia).

Pozyskiwane dane muszą mieć ponadto znaczenie dla toczącego się postępowania.

Warto zwrócić uwagę na katalog dysponentów, w stosunku do których powyższe procedury mogą być zastosowane. Adresatem postanowienia o zabezpieczeniu danych informatycznych, z którym związana jest procedura określona w § 1 ust. 1 pkt 2 i 3 rozporządzenia w związku z kolejno art. 218a § 1 i § 3 k.p.k. może być dowolny podmiot publiczny, przepisy powyższe nie limitują bowiem zakresu potencjalnych adresatów (dysponentów danych) w ramach postanowienia o zabezpieczania danych informatycznych, co wynika bezpośrednio z interpretacji powyższych przepisów. W przypadku procedury zatrzymywania danych, wymienionej w § 1 ust. 1 pkt 1 w związku z art. 218 § 1 k.p.k. katalog dysponentów jest już natomiast ograniczony, co przesądza o niedopuszczalności jej zastosowania w stosunku do innych podmiotów niż te wymienione w art. 218 § 1 k.p.k.

Zgodnie z § 4 ust. 1 omawianego rozporządzenia zabezpieczenia danych zapisanych dokonuje się przy użyciu środków technicznych, w sposób umożliwiający ich późniejsze odczytanie. Pożądaną formą zabezpieczenia będzie więc zapisanie ich na informatycznym nośniku danych, takim jak dysk zewnętrzny, pendrive, płyta CD czy karta pamięci SD. Zasady oraz wytyczne związane z poszczególnymi metodami pozyskiwania danych informatycznych zostaną określone w sposób bardziej szczegółowy w dalszej części opracowania. Ponadto, jak stanowi ust. 2, zabezpieczenia danych zapisanych oraz treści zapisanych dokonuje osoba upoważniona przez podmiot obowiązany, przy użyciu środków technicznych podmiotu obowiązanego, w urządzeniach zawierających te dane, w systemie lub na nośniku informatycznym. Osoba zabezpieczająca dane powinna sporządzić notatkę z czynności zabezpieczenia. Zobowiązana jest również do zapisania lub oznaczenia na nośniku zawierającym zabezpieczone dane:

1) sygnatury akt sprawy, w której czynność ta została zlecona;
2) swojego imienia, nazwiska i stanowiska służbowego;
3) danych dotyczących podstawy zabezpieczenia;
4) czasu dokonania zabezpieczenia.

Zgodnie z § 7 zabezpieczone dane zapisane oraz treści zapisane przechowuje się w sposób zabezpieczający przed ich utratą, zniekształceniem lub nieuprawnionym ujawnieniem oraz zniszczeniem lub uszkodzeniem nośnika informatycznego. Wydaje się, ze względu na specyfikę tego rodzaju danych, że mowa tutaj o zastosowaniu zarówno fizycznych, jak i cyfrowych zabezpieczeń. Cyfrowe zabezpieczenie danych powinno mieć charakter co najmniej dwuetapowy, tzn. chroniony powinien być dostęp do oprogramowania umożliwiającego odczyt danych, a ponadto zabezpieczone (np. hasłem) powinny zostać same dane.

Uprawnienia organów ścigania w zakresie zabezpieczania danych informatycznych nie mają jednak charakteru absolutnego. Przykładem ich limitacji może być wspomniana już konieczność uzyskania upoważnienia przez podmiot obowiązany oraz nakaz używania środków technicznych podmiotu obowiązanego przy zabezpieczaniu danych. Kolejne ograniczenie, tym razem w przypadku zabezpieczenia połączonego z obowiązkiem uniemożliwienia dostępu do danych statuuje § 8 ust. 2 omawianego rozporządzenia. Zgodnie z nim następuje ono w sposób niewpływający na integralność danych oraz umożliwiający niezwłoczne umożliwienie dostępu przez podmiot obowiązany (na żądanie podmiotu uprawnionego albo w wyniku upływu terminu, o którym mowa w postanowieniu podmiotu uprawnionego). Wydaje się, że *ratio legis* rzeczonych przepisów było ograniczenie możliwości podejmowania dyskrecjonalnych decyzji przez organy ścigania w zakresie nadmiernie długotrwałego uniemożliwiania dostępu do zabezpieczonych danych, które mogłyby prowadzić do nadużyć, zwłaszcza w kontekście swobody działalności gospodarczej i wolnego rynku.

Istotny w szczególności z punktu widzenia poszanowania prawa do prywatności użytkowników jest również fakt, że postanowienie o zabezpieczeniu danych informatycznych może być adresowane wyłącznie do podmiotów prowadzących działalność telekomunikacyjną oraz urzędów i instytucji, zatem osoby prywatne nie mogą być zobowiązane do zabezpieczenia

takich danych, nawet jeśli znajdują się one w ich posiadaniu i mają znaczenie dla toczącego się postępowania karnego[16].

Powyższe ograniczenia wydają się niezbędne w procedurze zabezpieczania danych informatycznych i są zapewne konsekwencją regulacji zawartej w art. 15 Konwencji, zwłaszcza jego ust. 2 stanowiącego, że warunki gwarantujące odpowiednią ochronę wolności i praw człowieka powinny obejmować, stosownie do rodzaju danego uprawnienia lub procedury, m.in. ograniczenia co do zakresu i czasu stosowania takich uprawnień i procedur.

W doktrynie dominuje pogląd, że na postanowienie o zabezpieczeniu danych informatycznych ani na postanowienie o zwolnieniu danych informatycznych spod zabezpieczenia nie przysługuje zażalenie[17]. Jak stanowi bowiem art. 236., zażalenie jest dopuszczalne jedynie w przypadku postanowień dotyczących przeszukania, zatrzymania rzeczy i w przedmiocie dowodów rzeczowych oraz na inne czynności. Artykuł niniejszy nie przesądza jednocześnie o dopuszczalności zażalenia w przypadku zabezpieczenia danych. Nie znajduje również uzasadnienia normatywnego dopuszczalność zażalenia na podstawie art. 459 k.p.k. Należy więc uznać dominujący pogląd za słuszny.

Pomimo braku możliwości złożenia zażalenia na postanowienie o zabezpieczeniu danych informatycznych na podstawie art. 236 k.p.k. w doktrynie podkreśla się, że podlega ono jednak zażaleniu w postępowaniu przygotowawczym zgodnie z art. 302 § 1 k.p.k.[18]. Przysługuje więc osobom niebędącym stronami w przypadku, gdy narusza ich prawa.

Należy zauważyć, że art. 218a k.p.k. odpowiada postanowieniom Konwencji zawartym w art. 16 oraz 17, które ustanawiają obowiązek wprowadzenia przez strony regulacji związanych z zabezpieczeniem przechowywanych danych informatycznych i danych dotyczących ruchu.

W praktyce wykorzystanie przez organy procesowe postanowienia z art. 218a k.p.k. jako metody zabezpieczenia danych informatycznych jest stosowane jedynie sporadycznie[19]. Najczęściej stosowanymi metodami zabezpieczenia danych informatycznych pozostają nadal formy klasyczne, znacząco ograniczające możliwość zachowania integralności i autentyczności zabezpieczanych danych, a co za tym idzie ich wiarygodności dowodowej. Są to metody

[16] R. A. Stefański (red.), S. Zabłocki (red.), op.cit., art. 218a, pkt 3.
[17] Tamże.
[18] K. Dudka (red.), M. B. Janicz, C. Kulesza, Jarosław Matras, H. Paluszkiewicz, B. Skowron, *Kodeks postępowania karnego. Komentarz, wyd. 3*. Lex/el. 2023. Art. 218a, pkt 2.
[19] P. Waszkiewicz (red.), M. Tomaszewska-Michalak, S. Rabczuk, B. Stromczyński, *Media społecznościowe w pracy organów ścigania*, INP PAN, Warszawa 2021.

takie jak notatka służbowa ze zrzutem ekranu, protokół oględzin strony internetowej z załączonymi zrzutami ekranu albo treścią strony internetowej czy żądanie wydania danych skierowane do operatora mediów społecznościowych. Wydaje się, że może to wynikać z braku dostatecznych umiejętności technicznych organów. Korzystanie z pomocy biegłego wydaje się więc niezbędnym elementem w sprawach, w których występuje potrzeba zabezpieczenia danych informatycznych.

4. Przeszukanie systemu informatycznego i zatrzymanie danych informatycznych

Zgodnie z art. 236a k.p.k. przepisy rozdziału 25 k.p.k. znajdują odpowiednie zastosowanie 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. W doktrynie zaznacza się jednak, że w przypadku przeszukania systemu informatycznego czy informatycznego nośnika danych zastosowanie znajduje jedynie część przepisów[20]. *Per analogiam*, nie wszystkie przepisy wspomnianego rozdziału znajdą zastosowanie również w przypadku zatrzymania danych informatycznych.

Przepisy rozdziału stosowane wprost do przeszukania i zatrzymania danych informatycznych to m.in. art. 226 k.p.k. (wykorzystanie dokumentów zawierających tajemnicę), art. 227 k.p.k. (dyrektywy przeprowadzenia przeszukania), art. 236 k.p.k. (zażalenie na postanowienie o przeszukaniu).

Charakter przeszukania danych informatycznych umożliwia przeprowadzenie tej czynności w sposób zdalny (na odległość). W takim przypadku zastosowania nie będzie miał art. 221 regulujący kwestie czasu przeszukania.

Odpowiednie stosowanie przepisów rozdziału 25 zostało ponadto przedmiotowo ograniczone tylko do danych przechowywanych na urządzeniu zawierającym dane informatyczne lub w systemie informatycznym należącym do dysponenta i użytkownika albo na nośniku znajdującym się w dyspozycji lub użytkowaniu dysponenta i użytkownika.

[20] F. Radoniewicz, *Przeszukanie systemów informatycznych oraz informatycznych nośników danych w kodeksie postępowania karnego*, Cybersecurity and Law 8(2), 2022, s. 146-159.

Okoliczność, że tego rodzaju dane znajdują się w zasięgu wymienionych osób w taki sposób, że mają one do nich legalny dostęp wystarczy do spełnienia powyższych przesłanek[21].

Opierając się na kryterium stopnia szczegółowości hierarchii zagadnień proceduralnych informatyki kryminalistycznej wyróżnić można 3 poziomy przewodnich motywów dotyczących pozyskiwania danych informatycznych przez organy[22]. Po pierwsze są to zasady podstawowe, będące ogólnymi koncepcjami postępowania z tego rodzaju danymi i charakteryzujące się najbardziej uniwersalnym charakterem. Pośrednim stopniem zagadnień związanych problemem informatyki kryminalistycznej są tzw. polityki i praktyki, które mają przede wszystkim charakter wskazówek organizacyjnych. Największym stopniem szczegółowości odznacza się kwestia ustalenia procedur i technik pozyskiwania danych informatycznych, w ramach której wyróżnia się już poszczególne rozwiązania techniczne dotyczące przeprowadzania tego rodzaju czynności.

Przed przystąpieniem do analizy możliwych metod zatrzymywania danych informatycznych należy zaznaczyć, że ich badaniem zajmuje się przede wszystkim dziedzina informatyki kryminalistycznej, natomiast szczegółowy opis tego rodzaju czynności ma w znacznej mierze charakter techniczny i wykracza poza ramy niniejszej publikacji. Należy jednak zwrócić uwagę przede wszystkim na wskazywane w doktrynie podstawowe zasady postępowania z tego rodzaju danymi, mającymi na celu zachowanie ich integralności i wiarygodności dowodowej oraz nakreślić fundamentalne warunki wymagające spełnienia podczas stosowania metod związanych z ich pozyskiwaniem. Standardy w tym zakresie wynikają również z norm ukształtowanych przez Międzynarodową Organizację Normalizacyjną, w szczególności z normy ISO/IEC 27037:2012, przetłumaczonej na język polski przez Polski Komitet Normalizacyjny (PN-EN ISO/IEC 27037:2016), i występującej jako „Technika informatyczna — Techniki bezpieczeństwa — Wytyczne dotyczące identyfikowania, gromadzenia, przejmowania i przechowywania cyfrowego materiału dowodowego, ale także z norm ISO/IEC 27041:2015, czy ISO/IEC 27043/2015[23].

Katalog zasad postępowania z danymi informatycznymi nie ma charakteru jednolitego, wynikają jednak z niego pewne uniwersalne konkluzje, które nie są zazwyczaj kwestionowane

[21] K. Eichstaedt, op.cit., art. 236a, pkt 5.
[22] P. Lewulis, *Dowody cyfrowe - teoria i praktyka kryminalistyczna w polskim postępowaniu karnym*, wyd. 1, Warszawa 2021, s. 148.
[23] M. Szmit, *O standardach informatyki śledczej*, Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach 2018, nr 355, s. 81-91.

w doktrynie[24]. Zgodnie z nimi pośród naczelnych zasad informatyki kryminalistycznej wyróżnia się zatem w szczególności:

1) niedopuszczalność dokonywania jakichkolwiek modyfikacji danych, chyba że są one niezbędne, właściwie uzasadnione i należycie opisane

2) obowiązek odpowiedniego uwierzytelnienia pozyskanych danych (zachowując ich autentyczność i integralność)

3) konieczność utworzenia co najmniej jednej pełnej, uwierzytelnionej kopii danych oraz jej zachowania w celu prowadzenia dalszych analiz

4) wymóg posiadania odpowiednich kwalifikacji — czynności techniczne na pozyskanych danych powinny być dokonywane wyłącznie przez osoby wyspecjalizowane (np. biegłych z zakresu informatyki)

5) nakaz szczegółowej dokumentacji dokonywanych czynności

Powyższe ogólne zasady są konkretyzowane przez polityki i praktyki dotyczące postępowania z materiałem cyfrowym oraz poszczególne procedury i techniki pozyskiwania danych informatycznych, które jednak muszą na każdym etapie pozostawać z nimi zgodne lub służyć ich realizacji.

Zatrzymanie danych informatycznych może mieć trojaki charakter. Po pierwsze, dane mogą zostać zatrzymane wraz z nośnikiem. W takim przypadku zastosowanie znajduje wyłącznie art. 217 k.p.k. ze względu na materialny charakter rzeczonego nośnika. Po drugie, mogą one zostać zatrzymane bez nośnika lub też zostać skopiowane (art. 217 k.p.k. w zw. z art. 236a k.p.k.). Dane mogą również zostać zatrzymane po uprzednim przeszukaniu systemu informatycznego (art. 219 k.p.k. w zw. z art. 236a k.p.k.).

Jak zaznacza się w doktrynie[25], zatrzymanie danych informatycznych wraz z nośnikiem znajduje uzasadnienie m.in. w sytuacjach, gdy:

1) dotarcie do samej informacji w ramach danego systemu jest niemożliwe, np. ze względu na zastosowane zabezpieczenia;

2) skopiowanie danych jest niemożliwe lub utrudnione albo może wpłynąć na ich integralność lub wiarygodność, np. na dysku twardym zainstalowano specjalistyczne oprogramowanie, sposób zabezpieczenia danych przez ich dysponenta uniemożliwia ich skopiowanie, czas trwania zatrzymania byłby znacząco wydłużony;

[24] P. Lewulis, op.cit., s. 169.
[25] R. A. Stefański (red.), S. Zabłocki (red.), op.cit., art. 236a, pkt 7.

3) znaczenie dowodowe ma również sam nośnik, na którym dane są przechowywane;
4) nośnik zawiera informacje objęte tajemnicą prawnie chronioną, a organ dokonujący zatrzymania nie ma uprawnień do jej uchylenia.

Zaznacza się również, że nieuzasadnione zatrzymanie danych wraz z nośnikiem jest sprzeczne z zasadą proporcjonalności i nie powinno mieć miejsca.

Najbardziej pożądaną metodą gromadzenia danych informatycznych jest ich zatrzymanie bez nośnika. Powinno być ono stosowane w każdym przypadku, jeśli tylko charakter danych na to pozwala. Może nastąpić w szczególności poprzez klonowanie albo sporządzenie obrazu dysku.

Klonowanie dysku polega na wykonaniu jego pełnego duplikatu mającego charakter kopii lustrzanej na nowym nośniku. Warto zauważyć, że charakter klonowania znacząco różni się od zwykłego skopiowania dysku. Po pierwsze odbywa się za pomocą specjalistycznych programów do tego przeznaczonych, a po drugie umożliwia pełniejsze odtworzenie zawartości klonowanego dysku z racji, że niektóre znajdujące się na nim pliki mogą być zabezpieczone przed kopiowaniem. Dodatkową przewagą klonowania dysku nad standardowym kopiowaniem jest fakt, że uwzględnia ono również dane niewidoczne (np. usunięte) oraz niezalokowane obszary oryginalnego nośnika. W przeciwieństwie natomiast do sporządzenia obrazu dysku, w przypadku klonowania istnieje możliwość zamontowania klonu dysku w komputerze i uruchomienia z jego poziomu systemu operacyjnego. Wadą tej metody zatrzymania danych informatycznych może natomiast okazać się jej modyfikowalny charakter. Szczególnie problematyczne są zmiany zachodzące w dziennikach zdarzeń (tzw. logach) plików z każdym uruchomieniem systemu operacyjnego. Zwraca się uwagę, że w przypadku skorzystania z klonowania dysku należy więc wykonać co najmniej dwa duplikaty dysku - jeden o charakterze dowodowym, drugi natomiast w celach kryminalistycznych.

Drugą metodą zatrzymania danych informatycznych bez nośnika jest sporządzenie obrazu dysku. Ma ona zbliżony charakter do duplikatu sporządzonego za pomocą klonowania i przeprowadzana jest również za pomocą specjalistycznych programów. Istotną różnicą jest natomiast fakt, że obraz dysku jest mniej podatny na różnego rodzaju modyfikacje. Jak już wspomniano, nie ma również możliwości uruchomienia systemu operacyjnego z poziomu obrazu dysku. Istnieją jednak programy umożliwiające konwersję obrazu dysku do postaci klonu. Wydaje się więc, że z perspektywy dowodowej jest to optymalna metoda zatrzymywania danych informatycznych bez nośnika.

Podczas stosowania powyższych metod pozyskiwania danych istnieje znaczne ryzyko ich modyfikacji, co wynika z zasad działania dysku po podłączeniu do stacji roboczej (każde podłączenie dysku z pozyskanymi danymi do komputera powoduje zmiany w tychże danych). Wskazuje się zatem, że w celu spełnienia nadrzędnej przesłanki informatyki kryminalistycznej, jaką jest zachowanie autentyczności danych, a co za tym idzie ich wiarygodności dowodowej bezwzględnym obowiązkiem jest skorzystanie z urządzeń blokujących zapis (tzw. bloker). Zastosowanie blokera sprawia, że komunikacja między stacją roboczą a dyskiem przebiega wyłącznie jednostronnie, zapobiegając tym samym modyfikacji danych. Zaznacza się jednocześnie, że zastosowanie blokera jest niezbędne tylko na etapie klonowania czy sporządzania obrazu dysku, nie wymaga się go natomiast już na dalszych etapach postępowania z danymi[26].

Kolejnym elementem pozwalającym na uwiarygodnienie pozyskanych danych jest wyliczenie ich tzw. sumy kontrolnej. Jej celem, podobnie zresztą jak w przypadku użycia blokera jest zagwarantowanie, że dane nie zostały zmodyfikowane na żadnym etapie postępowania. Zaznacza się wobec tego, że wyliczenie sumy kontrolnej ma charakter obligatoryjny[27], służy bowiem realizacji jednej z naczelnych zasad informatyki kryminalistycznej jaką jest obowiązek odpowiedniego uwierzytelnienia danych. Czynność polegająca na wyliczeniu sumy kontrolnej może mieć jednak charakter następczy względem czynności pozyskania danych (następuje w momencie zabezpieczenia lub już po ich zabezpieczeniu lub zatrzymaniu). Istotą zastosowania sumy kontrolnej jest wytworzenie skrótu odcinka danych (tzw. „hash"), która dla tego samego rodzaju danych na każdym etapie postępowania musi przybrać taką samą wartość, co jest gwarancją tożsamości danych z danymi pierwotnymi. Należy zauważyć, że metoda wyliczania sumy kontrolnej jest powszechnie akceptowanym przez sądy sposobem uwierzytelniania danych cyfrowych[28].

Pozyskanie danych w sposób prawidłowy zmniejsza prawdopodobieństwo kwestionowania ich wiarygodności przed sądem, co jest niezwykle istotne z perspektywy dowodowej. Warto mieć na uwadze, że — ze względu na jego specyfikę — brak jest możliwości swoistej „konwalidacji" wadliwie zatrzymanego materiału cyfrowego. Wydaje się zatem, mając na względzie możliwie najpełniejszą realizację zasady prawdy materialnej, że istotne jest zastosowanie się do powyższych wytycznych. Implikacje zaniedbań w tym

[26] M. Chrabkowski, K. Gwizdała, *Zabezpieczenie dowodów elektronicznych*, Prok.i Pr. 2015, nr 12, s. 164-178.
[27] Tamże.
[28] P. Lewulis, op.cit., s. 190.

zakresie, związane z możliwością uznania przez sąd dowodu za wadliwy i wykluczeniem go z materiału dowodowego mogą okazać się bowiem niezwykle dotkliwe, nie wykluczając skutku w postaci umorzenia postępowania czy uniewinnienia oskarżonego.

Należy ponadto zauważyć, że treść art. 236a k.p.k. implementuje postanowienia zawarte w art. 19 Konwencji. Przepis niniejszy nakłada na jej strony obowiązek zapewnienia właściwym organom możliwości przeszukania i zajęcia przechowywanych danych informatycznych oraz określa warunki tego przeszukania lub zajęcia. Wydaje się, że kwestia rozszerzenia przeszukania na inny system zawarta art. 19 ust. 2 Konwencji znajduje odzwierciedlenie bezpośrednio w treści art. 236a k.p.k. *in fine*. Upoważnia on bowiem organy do zatrzymania danych informatycznych w zakresie dysponenta i użytkownika urządzenia zawierającego te dane, ale odnosi się również do danych znajdujących się w jego dyspozycji lub użytkowaniu. O zgodności prawa polskiego z ust. 4 omawianego przepisu świadczy natomiast obecność art. 195 k.p.k. ustanawiającego możliwość powołania osoby dysponującej specjalistyczną wiedzą z dziedziny informatyki w charakterze biegłego.

5. Podsumowanie

Pomimo obecności przepisów odnoszących się do materii gromadzenia danych informatycznych w ramach postępowania karnego nie ulega wątpliwości, że *de lege lata,* zwłaszcza w kontekście przeszukania systemu informatycznego oraz zatrzymania danych informatycznych jest to regulacja o wysokim stopniu ogólności. W szczególności przy doborze metod pozyskiwania materiału cyfrowego na potrzeby postepowania karnego konieczne może być zatem odwołanie się do standardów wypracowanych w doktrynie.

Warto mieć na uwadze, że nieprecyzyjna bądź zbyt ogólna regulacja materii pozyskiwania danych cyfrowych może skutkować niewystarczającą legitymizacją prawną do dokonywania tego rodzaju czynności przez organy wskutek braku ustanowienia procedury ich gromadzenia w prawie krajowym w sposób przewidywalny i powtarzalny, co potwierdza utrwalona linia orzecznicza Europejskiego Trybunału Praw Człowieka[29], zgodnie z którą przewidywalność procedury w prawie krajowym jest jednym z elementów koniecznych,

[29] Europejski Trybunał Praw Człowieka z siedzibą w Strasburgu, dalej: „Trybunał".

a zarazem kluczowym do uznania czynności pozyskiwania danych informatycznych za uzasadnione[30].

Kwestią odrębną pozostaje, czy wykształcone doktrynalne standardy pozyskiwania cyfrowego materiału dowodowego mają taki charakter. Wydaje się natomiast, że sama procedura w tym zakresie, nakreślona w rozdziale 25 k.p.k. oraz przepisach wykonawczych może nie spełniać powyższych przesłanek w odniesieniu do nieobjętych jej zakresem podmiotowym dysponentów w ramach zastosowania procedury przeszukania i zatrzymywania danych informatycznych bez ich uprzedniego zabezpieczania. Jak już bowiem wspomniano we wcześniejszej części opracowania, zakresem podmiotowym rozporządzenia ustanawiającego ww. procedurę w kontekście gromadzenia (zatrzymania) danych (§ 1 ust. 1 rozporządzenia) objęte są bowiem jedynie podmioty wymienione w art. 218 § 1 k.p.k., czyli urzędy, instytucje i podmioty prowadzące działalność w dziedzinie poczty lub działalność telekomunikacyjną, urzędy celno-skarbowe oraz instytucje i przedsiębiorstwa transportowe. Problem wydaje się zanikać w sytuacji, kiedy postanowienie o zatrzymaniu danych jest konsekwencją ich uprzedniego zabezpieczenia, bowiem rozporządzenie w tym przypadku nie limituje zakresu podmiotów, co do których procedura ma zastosowanie, a świadczy o tym m.in. odwołanie w ramach § 1 ust. 3 rozporządzenia do art. 218a § 3 k.p.k. Należy jednak spodziewać się incydentów polegających na wydaniu postanowienia o zatrzymaniu danych cyfrowych (np. w przypadku zatrzymania danych wraz nośnikiem) w stosunku do dysponenta niewymienionego w ramach zakresu podmiotowego art. 218 § 1 k.p.k., bez ich uprzedniego zabezpieczenia, co może skutkować — w kontekście wspomnianego orzecznictwa Trybunału — naruszeniami w tym zakresie związanymi m.in. z brakiem ustanowienia przewidywalnej procedury w prawie krajowym. Wydaje się zatem, że kwestia zachowania jasności terminologicznej jest w tym zakresie kluczowa.

W związku z powyższym, *de lege ferenda*, pożądana jest modyfikacja zakresu podmiotowego art. 218 § 1 k.p.k. w ten sposób, aby obejmował również inne podmioty, jak np. podmioty świadczące usługi drogą elektroniczną, dostawców usług cyfrowych, czy administratora treści publikowanych lub udostępnianych drogą elektroniczną, analogicznie do wspomnianej już nowelizacji art. 218a § 1 oraz 3, wprowadzonej w 2021 r. Pozwoli to w pełni rozwiązać kwestię niezgodności polskiej procedury pozyskiwania danych

[30] Zob.: wyroki Europejskiego Trybunału Praw Człowieka z 3.12.2019 r., [I], skarga nr 14704/12; z 24.7.2018 r., [I], skarga nr 62357/14.

informatycznych ze standardami Rady Europy, która to — jak się wydaje — w głównej mierze ma charakter jedynie terminologiczny.

Z perspektywy stosowania omawianych przepisów istotne wydaje się regularne przeprowadzanie szkoleń dotyczących technicznych aspektów zabezpieczania i zatrzymywania danych informatycznych. Biorąc jednak pod uwagę fakt, że — jak przedstawiono — czynności z tym związane wymagają często wiedzy specjalistycznej alternatywą jest korzystanie z pomocy biegłych.

Summary

Securing and seizing computer data in the Polish criminal procedure

The article discusses the issue of securing and seizing computer data in the Polish criminal procedure. It presents the basic vocabulary related to the subject as well as pointing at the conceptual differences related to undertaking these activities in the digital background in comparison to traditional ways. It shows the basic features and methods of securing computer data and specifies the application of the provisions related to searching and seizing of physical items to a virtual environment. Furthermore, the author presents the disadvantages of the current regulation regarding to the collection of computer data and proposes changes aimed at improving the functioning of the discussed institution.

Jonasz Szpoton

Student V roku prawa stacjonarnego na Wydziale Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie. Członek Koła Naukowego Prawa Karnego Materialnego i Prawa Nowych Technologii. Zainteresowania badawcze — prawo karne (materialne i procesowe) oraz wpływ postępu technologicznego na jego tworzenie i stosowanie; prawa człowieka.

Bibliografia:

1. D. Świecki (red.), B. Augustyniak, K. Eichstaedt, M. Kurowski, *Kodeks postępowania karnego. Komentarz aktualizowany*. Lex/el. 2023.
2. K. Dudka (red.), M. B. Janicz, C. Kulesza, J. Matras, H. Paluszkiewicz, B. Skowron, *Kodeks postępowania karnego. Komentarz*, wyd. 3. Lex/el. 2023.
3. R. A. Stefański (red.), S. Zabłocki (red.), *Kodeks postępowania karnego. Tom II. Komentarz do art. 167-296*. Lex/el. 2018.
4. M. Mozgawa (red.), M. Budyn-Kulik, P. Kozłowska-Kalisz, M. Kulik, *Kodeks karny. Komentarz aktualizowany*. Lex/el. 2023.
5. K. Kremens, Przeszukanie (w:) J. Skorupka (red.), *System prawa karnego procesowego, Tom VIII. Dowody, część 1*, Wolters Kluwer, Warszawa 2019
6. F. Radoniewicz, *Przeszukanie systemów informatycznych oraz informatycznych nośników danych w kodeksie postępowania karnego*, Cybersecurity and Law 8(2), 2022
7. A. Adamski, *Prawo karne komputerowe*, C.H. Beck, Warszawa 2000
8. P. Waszkiewicz (red.), M. Tomaszewska-Michalak, S. Rabczuk, B. Stromczyński, *Media społecznościowe w pracy organów ścigania*, INP PAN, Warszawa 2021
9. M. Chrabkowski, K. Gwizdała, *Zabezpieczenie dowodów elektronicznych*, Prokuratura i Prawo 2015 nr 12.
10. P. Lewulis, *Dowody cyfrowe - teoria i praktyka kryminalistyczna w polskim postępowaniu karnym*, Wydawnictwa Uniwersytetu Warszawskiego, wyd. 1, Warszawa 2021.
11. P. Lewulis, *Gromadzenie i ocena dowodów cyfrowych w polskim postępowaniu karnym. Kluczowe wnioski z badań aktowych*, Prokuratura i Prawo 3, 2022.
12. M. Szmit, *O standardach informatyki śledczej*, Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach 2018, nr 355.
13. CERT Polska (NASK), *Raport roczny z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego internetu*, 2021.
14. Międzynarodowa Organizacja Policji Kryminalnych „Interpol", https://www.interpol.int/ [dostęp 14.5.2023].
15. P. Rojek-Socha, *Przepis na ciastka z konopi? Prokurator zdecyduje o usunięciu z sieci*, https://www.prawo.pl/prawnicy-sady/zabezpieczenie-danych-i-tresci-cyfrowych-wkrotce-zmiany-w,508813.html, 14.06.2021, [dostęp 25.4.2023].