Martyna Kusak
Uniwersytet im. Adama Mickiewicza w Poznaniu, Polska
m.kusak@amu.edu.pl
ORCID: 0000-0002-7596-9022

https://doi.org/10.26881/gsp.2024.2.05

Dostęp do danych elektronicznych dotyczących treści w postępowaniu karnym – wyzwania krajowe i międzynarodowe[1]

Wprowadzenie

Postęp technologiczny XXI w. znacząco zmienił sposób komunikowania się na odległość. Powszechne stało się posiadanie smartfonów oraz innych urządzeń przenośnych umożliwiających komunikację za pomocą aplikacji, komunikatorów internetowych, poczty elektronicznej, portali społecznościowych, a także korzystanie z telefonii internetowej. Użytkownicy internetowej łączności generują ogromne ilości danych elektronicznych, które z uwagi na ich znaczenie dla społeczeństwa i gospodarki są lub dynamicznie stają się przedmiotem uregulowań w różnych gałęziach prawa[2]. Rosnąca

[1] Artykuł powstał w ramach projektu naukowego finansowanego przez Narodowe Centrum Nauki nr 2016/23/D/HS5/00182 pt. „Minimalne standardy gromadzenia dowodów elektronicznych w transgranicznych postępowaniach w UE i ich wzajemna dopuszczalność".

[2] Szeroko zakrojone prace prowadzi w tym zakresie zwłaszcza Unia Europejska. Wśród podjętych działań kluczową rolę odgrywa reforma ochrony danych osobowych i wejście w życie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO) (Dz. Urz. UE L 119 z 4.05.2016, s. 1) oraz, na gruncie spraw karnych, dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 4.05.2016, s. 89). Unia Europejska konsekwentnie znosi również bariery przepływu danych nieosobowych między państwami członkowskimi i sektorami oraz dąży do zwiększania dostępności danych sektora publicznego – zob. dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (Dz. Urz. UE L 172 z 26.06.2019, s. 56); rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej (Dz. Urz. UE L 303 z 28.11.2018, s. 59). Rosnące ilości danych i ich znaczenie dla gospodarki oraz społeczeństwa zaowocowało przyjęciem europejskiej strategii w zakresie danych (COM(2020) 66 final), w której wyrażono wizję wspólnej europejskiej przestrzeni danych oznaczającej

liczba danych elektronicznych ma również znaczenie w sprawach karnych. Coraz większa liczba dowodów lub informacji przydatnych dla postępowania to właśnie dane elektroniczne wygenerowane w związku z korzystaniem z usług internetowych.

Dane elektroniczne najczęściej ujmowane są w trzech kategoriach, odzwierciedlających różne nasilenie oddziaływania na prawa podstawowe[3]: dane dotyczące treści (*content data*)[4], dane dotyczące abonenta (*subscriber data*)[5] i dane dotyczące ruchu (*traffic data*)[6]. Dane dotyczące abonenta zwykle służą zidentyfikowaniu konkretnej

---

rynek wewnętrzny danych, na którym dane mogłyby być wykorzystywane, zgodnie z obowiązującymi przepisami, bez względu na fizyczne miejsce ich przechowywania w UE. Strategia ta ma znaczenie zwłaszcza dla rozwoju technologii sztucznej inteligencji. Urzeczywistniając tę wizję, w 2022 r. przyjęto rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z dnia 30 maja 2022 r. w sprawie europejskiego zarządzania danymi i zmieniające rozporządzenie (UE) 2018/1724 (akt w sprawie zarządzania danymi) (Dz. Urz. UE L 152 z 3.06.2022, s. 1) oraz projekt w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania (akt w sprawie danych) (COM(2022) 68 final).

[3] W literaturze wskazuje się na nieadekwatność tego podziału danych, wypracowanego na potrzeby regulowania sfery dostawców usług, do spraw karnych: C. Warken, L. van Zwietenband, D. Svantesson, *Re-thinking the categorisation of data in the context of law enforcement cross-border access to evidence*, „International Review of Law, Computers & Technology" 2020, vol. 34, s. 44–64, https://doi.org/10.1080/13600869.2019.1600871 [dostęp: 19.04.2024]. Autorzy ci proponują również ciekawe alternatywy kategoryzacji danych.

[4] „Dane dotyczące treści" oznaczają wszelkie dane przechowywane w formacie cyfrowym, takie jak tekst, głos, wideo, obrazy i dźwięk, inne niż dane abonenta, dane dostępu i dane dotyczące transakcji (finalny projekt rozporządzenia w sprawie europejskiego nakazu wydania dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych i europejskiego nakazu zabezpieczenia dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych – art. 2 pkt 10). Podobnie projekt rozporządzenia w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej – art. 4 ust. 1(b).

[5] Zgodnie z art. 2(7) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/1543 z dnia 12 lipca 2023 r. w sprawie europejskich nakazów wydania i europejskich nakazów zabezpieczenia dowodów elektronicznych w postępowaniu karnym oraz w postępowaniu karnym wykonawczym w związku z wykonaniem kar pozbawienia wolności (Dz. Urz. UE L 191 z 28.07.2023, s. 118) „dane abonenta" oznaczają wszelkie dane dotyczące: a) tożsamości abonenta lub klienta, takie jak podane imię i nazwisko, data urodzenia, adres pocztowy lub geograficzny, dane billingowe i dane płatności, numer telefonu lub adres e-mail; b) rodzaju usługi i czasu jej trwania, w tym dane techniczne i dane identyfikujące powiązane środki techniczne lub interfejsy wykorzystywane przez abonenta lub klienta lub im udostępniane oraz dane związane z walidacją użycia usługi, z wyjątkiem haseł i innych środków uwierzytelnienia stosowanych zamiast hasła, podanych przez użytkownika lub utworzonych na jego prośbę.

[6] Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz. U. z 2015 r., poz. 728) (dalej: Konwencja) definiuje „dane dotyczące ruchu" jako 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 (art. 1 lit. d). Do kategorii danych dotyczących ruchu powrócił również ustawodawca unijny w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2023/1543 z dnia 12 lipca 2023 r. w sprawie europejskich nakazów wydania i europejskich nakazów zabezpieczenia dowodów elektronicznych w postępowaniu karnym oraz w postępowaniu karnym wykonawczym w związku z wykonaniem kar pozbawienia wolności (Dz. Urz. UE L 191 z 28.07.2023, s. 118) (dalej: rozporządzenie ENWD), rezygnując jednocześnie z kategorii „danych dostępu" i „danych dotyczących transakcji", które pojawiły się w pierwszym projekcie rozporządzenia.

osoby i nie mają znaczenia dowodowego, a ich oddziaływanie na prawa podstawowe nie jest silne. Natomiast dane dotyczące ruchu i dane dotyczące treści mogą się okazać najbardziej adekwatne jako materiał dowodowy; są to również dane, których pozyskanie może stać w kolizji z prawami podstawowymi, a zwłaszcza z prawem do prywatności i tajemnicą komunikowania się. Dlatego w wielu aktach prawnych wyodrębnia się inne w stosunku do danych dotyczących abonenta warunki przechowywania i dostępu do danych dotyczących ruchu i danych dotyczących treści.

Niniejszy artykuł dotyczy kategorii najgłębiej ingerującej w prawa podstawowe, tj. elektronicznych danych odnoszących się do treści. Przeanalizowane zostaną krajowe przepisy procesowe umożliwiające dostęp do tego rodzaju danych, a także instrumenty międzynarodowe służące gromadzeniu takich danych znajdujących się w obszarze innych jurysdykcji. Myślą przewodnią analizy jest standard dostępu do elektronicznych danych zawierających treść oraz zweryfikowanie, czy niuanse technologiczne i praktyczne związane z tego rodzaju danymi znajdują odzwierciedlenie w przepisach krajowych i międzynarodowych.

1. Wyzwania krajowe: ta sama treść, różny standard

Wszechobecność komunikatorów, w tym używanych na smartfonach, spowodowała, że komunikacja na odległość nie sprowadza się już do rozmów telefonicznych, ale obejmuje również wiadomości tekstowe, głosowe czy zdjęcia, w tym przesyłane za pomocą internetu (w szczególności w technologii VoIP – *Voice over Internet Protocol*[7]). Nie zważając na nowe trendy w sposobie komunikacji, które mogą kreować istotne dla postępowań karnych informacje, polski Kodeks postępowania karnego[8] od 2003 r. pozostaje niewzruszony na specyfikę danych elektronicznych, a tym bardziej na specyfikę elektronicznych danych dotyczących treści. W literaturze od dawna zaś wyrażane są poglądy o nieprzystawaniu przepisów Kodeksu postępowania karnego do dowodów elektronicznych i o konieczności wypracowania odrębnych zasad umożliwiających ich uzyskiwanie[9]. Niniejszy tekst wpisuje się w dotychczasowe poglądy doktryny o konieczności wprowadzenia zmian w Kodeksie postępowania karnego, przyjmując wąską optykę danych dotyczących treści. Wydawać by się mogło, że treść jakiejkolwiek komunikacji, niezależnie od środka przekazu danych oraz środka łączności, podlega

---

[7] M. Rogalski, *Kontrola i utrwalanie treści innych rozmów lub przekazów informacji* [w:] *System prawa karnego procesowego*, t. 8, *Dowody*, cz. 3, red. J. Skorupka, Warszawa 2019, s. 4059.

[8] Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (tekst jedn.: Dz. U. z 2024 r., poz. 37 ze zm.) (dalej: k.p.k.).

[9] A. Lach, *Gromadzenie dowodów elektronicznych po nowelizacji k.p.k.*, Prok. i Pr. 2003, nr 10, s. 16–25; K. Kremens, *O znaczeniu prawa porównawczego dla nauki polskiego procesu karnego na przykładzie przeszukań telefonów komórkowych* [w:] *W pogoni za rzetelnym procesem karnym. Księga dedykowana Profesorowi Stanisławowi Waltosiowi*, red. D. Szumiło-Kulczycka, Warszawa 2022, s. 550–560; P. Lewulis, *Dowody cyfrowe – teoria i praktyka kryminalistyczna*, Warszawa 2021, s. 98–109; K. Dudka, *Podsłuch komputerowy w polskim procesie karnym – wybrane zagadnienia praktyczne*, Prok. i Pr. 1999, nr 1, s. 79.

tej samej ochronie[10]. Na gruncie polskiego postępowania karnego tak jednak nie jest, co wynika głównie z braku przemyślanych rozwiązań oddających aktualne realia sposobów komunikacji.

W polskim Kodeksie postępowania karnego dowody i dane elektronicznie nie są zdefiniowane ani uregulowane konkretnymi przepisami, które uwzględniałyby ich specyfikę. Przyjęto zaś metodę odpowiedniego stosowania przepisów dotyczących innych dowodów. W ten sposób dane dotyczące treści można pozyskiwać na dwa sposoby: a) w czasie rzeczywistym – na podstawie art. 241 k.p.k., stosując przepisy o kontroli i utrwalaniu rozmów odpowiednio do „treści innych rozmów lub przekazów informacji, w tym korespondencji przesyłanej drogą elektroniczną" oraz b) w drodze przeszukania urządzenia zawierającego dane informatyczne, na podstawie art. 236a k.p.k. dotyczącego stosowania przepisów o zatrzymaniu rzeczy i przeszukaniu do urządzeń zawierających dane informatyczne[11]. Dane dotyczące treści, w przeciwieństwie do danych dotyczących ruchu i abonenta, nie będą natomiast dostępne w trybie wydania korespondencji (art. 218 k.p.k. w zw. z art. 236 k.p.k.), ponieważ przepis ten obejmuje jedynie dane określone w prawie telekomunikacyjnym, które nie dotyczą treści. O ścieżce dostępu do danych przesądza więc faza, w której dane te się znajdują – czy chodzi o dane „na żywo", czy też o dane już przechowywane. Wybór fazy jest zaś często podyktowany realną dostępnością danych wynikającą z technologicznych aspektów niektórych systemów komunikacji (zwłaszcza szyfrowania) lub przechowywaniem danych przez usługodawców.

W doktrynie od dawna wskazuje się na ułomność odpowiedniego stosowania przepisów o tradycyjnych czynnościach dowodowych do dowodów elektronicznych. W przypadku art. 241 k.p.k. problematyczne jest ustalenie treści pojęcia „innych przekazów informacji"[12], a zwłaszcza, gdzie się one odbywają (czy w sieci telekomunikacyjnej, czy poza nią). Stosowanie art. 241 k.p.k. do rozmów prowadzonych w technologii VoIP („telefonii internetowej") nie jest bowiem oczywiste, ponieważ pod względem technicznym sposób przechwycenia takich rozmów różni się od przechwytywania komunikacji prowadzonej za pomocą sieci telekomunikacyjnej[13]. Często rozmowy takie są szyfrowane, a kluczem kryptograficznym dysponują jedynie odbiorca i nadawca wiadomości (*end-to-end encryption*) – usługodawca nie ma zatem możliwości odszyfrowania i przechwycenia ich treści. Tym samym rzeczywista możliwość ich uzyskania wymaga nie tyle zwrócenia się do dostawcy usługi, co zainstalowania oprogramowania szpiegującego na urządzeniu końcowym użytkownika i przechwytywania

---

[10] P. Wiliński, *Ochrona tajemnicy komunikowania się (art. 49 Konstytucji RP)* [w:] *System prawa karnego procesowego. Tom I. Zagadnienia ogólne*, red. P. Hofmański, Warszawa 2013; D. Szumiło-Kulczycka, *Wolność i tajemnica komunikowania się* [w:] *eadem*, *Czynności operacyjno-rozpoznawcze i ich relacje do procesu karnego*, Warszawa 2012.

[11] A. Lach, *Dowody elektroniczne w procesie karnym*, Toruń 2004, s. 69–123.

[12] Por. na gruncie pierwotnego brzmienia art. 241 k.p.k. – uchwała SN z dnia 21 marca 2000 r., I KZP 60/99, OSNKW 2000, nr 3–4, poz. 26.

[13] M. Rogalski, *Kontrola i utrwalanie*…, s. 4058–4059.

już rozszyfrowanych treści[14]. W tym rozwiązaniu zaciera się granica pomiędzy treścią „na żywo" a treścią już przechowaną. W literaturze na nieadekwatność odpowiedniego stosowania rozdziału 25 k.p.k. do przeszukania telefonu komórkowego wskazuje Karolina Kremens, która słusznie zauważa, że „zasady przeszukania miejsc oraz osób i ich rzeczy ukształtowane na długo przed epoką rewolucji cyfrowej nie przewidziały bowiem nawet istnienia, a tym bardziej złożoności urządzeń elektronicznych przechowujących gigabajty danych. Reguły te w naturalny sposób koncentrują się więc na miejscach, osobach i przedmiotach fizycznych, a nie na danych elektronicznych dostępnych na różnych nośnikach"[15]. Opisywane poniżej niuanse pozyskiwania danych elektronicznych dotyczących treści jedynie potwierdzają wyrażane już poglądy o niewystarczającym charakterze odpowiedniego stosowania „tradycyjnych" czynności oraz konieczność określenia precyzyjnych reguł dostępu do nich.

Jak już wspomniano, ścieżka dostępu do elektronicznych danych dotyczących treści determinuje to, czy jest to treść w fazie transmisji (tj. „na żywo", „w locie"), czy też treść, która została już przesłana i jest przechowywana przez użytkownika (np. na smartfonie) lub dostawcę usługi[16]. Treść będąca w fazie transmisji może być bowiem uzyskana jedynie w drodze kontroli rozmów, na podstawie art. 241 k.p.k.[17] Czynność ta podlega więc wszystkim gwarancjom określonym w rozdziale 26 k.p.k. Przede wszystkim, zgodnie z art. 237 § 1 k.p.k., decyzja o zarządzeniu czynności podlega kontroli sądowej, co stanowi w założeniu istotny element redukcji nadużyć. Warunki dostępu do danych dotyczących treści są więc dość rygorystyczne – sprawa musi odnosić się do katalogu przedmiotowego określonego w art. 237 § 3 k.p.k., a kontrola rozmów do podmiotu wskazanego w art. 237 § 4 k.p.k. oraz podlegać kontroli sądu.

Treść z fazy transmisji najczęściej przechodzi w treść przechowywaną na urządzeniach końcowych lub w chmurze dostawcy usługi[18]. Najczęściej, ponieważ oba scenariusze zależą od pewnych czynników. W pierwszym przypadku od tego, czy użytkownik zachował treść komunikacji na swoim urządzeniu, a w drugim, czy na przechowywanie treści zezwala prawo krajowe, którym objęty jest dostawca usługi, oraz jego wewnętrzna polityka (np. oparcie komunikacji na szyfrowaniu *end-to-end*). Polskie przepisy prawa telekomunikacyjnego[19] oraz ustawy o świadczeniu usług dro-

---

14 P. Lewulis, *Dowody cyfrowe*…, s. 99.

15 K. Kremens, *O znaczeniu*…, s. 555.

16 W niniejszych rozważaniach odwołania wciąż są czynione do prawa telekomunikacyjnego (ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne; tekst jedn.: Dz. U. z 2024 r., poz. 34; dalej: p.t.). Ustawą mającą „unowocześnić" prawo telekomunikacyjne o kwestie komunikacji elektronicznej miała być ustawa – Prawo komunikacji elektronicznej (druk sejm. nr 2861), której projekt złożono 9 grudnia 2022 r. (został jednak wycofany 21 kwietnia 2023 r.).

17 M. Siwicki, *Przetwarzanie danych informatycznych w chmurach obliczeniowych. Wybrane aspekty prawnokarne i procesowe*, „Palestra" 2005, nr 1–2.

18 A. Lach nazywa to „fazą statyczną" – zob. *idem*, *Gromadzenie dowodów elektronicznych*…, s. 16.

19 Zgodnie z art. 180c p.t. retencji podlegają jedynie dane niedotyczące treści. Stanowisko to jest wątpliwe w świetle podejścia do retencji przez Trybunał Sprawiedliwości Unii Europejskiej (dalej: TSUE) – szerzej zob. A. Grzelak, K. Zielińska, *Między prawem do prywatności i ochrony danych osobowych a zapewnieniem bezpieczeństwa publicznego i walką z przestępczością. Problemu retencji danych ciąg dalszy – glosa do wyroków Trybunału Sprawiedliwości z 6.10.2020 r.: C-623/17, Privacy Internatio-*

gą elektroniczną[20] nie zezwalają dostawcom usług na zatrzymywanie danych dotyczących treści, a zatem za pośrednictwem krajowych dostawców treść można uzyskać tylko w czasie rzeczywistym. Możliwy jest jednak dostęp do treści przechowywanej na serwerach zagranicznych, o ile pozwala na to tamtejsze prawo, co będzie jednak wymagać uruchomienia współpracy międzynarodowej (*vide infra*). Podsumowując, zachowanie treści komunikacji będzie zależne od tego, czy sam użytkownik utrwala historię komunikacji na swoim urządzeniu oraz czy dostawca usługi przyjmuje politykę przechowywania takich danych w związku z oferowaną usługą.

Choć rzeczywista dostępność już przesłanych treści jest niewiadomą, to prawny model ich pozyskiwania jest zdecydowanie mniej rygorystyczny w przypadku treści „w locie". Ponieważ rozdział 26 k.p.k. dotyczy wyłącznie rozmów „na żywo", dostęp do przechowywanej treści komunikacji nie jest *de lege lata* możliwy w tym trybie. Z uwagi na wykluczenie danych dotyczących treści z art. 218 k.p.k. pozostaje więc czynność przeszukania urządzenia, na którym zapisano treść komunikacji (art. 219 k.p.k. w zw. z art. 236a k.p.k.), która może przybrać formę przeglądania jego zawartości lub przeszukania na odległość[21]. W odróżnieniu od kontroli treści „na żywo" czynności określone w rozdziale 25 k.p.k. mogą być zarządzone w każdej sprawie i nie podlegają ograniczeniom podmiotowym ani apriorycznej kontroli sądu. W przeciwieństwie do kontroli i utrwalania rozmów przeszukanie urządzenia powinno odbywać się w sposób jawny wobec osoby, której urządzenie jest przedmiotem czynności.

De lege lata funkcjonują więc dwa tryby pozyskiwania elektronicznych danych dotyczących treści, które wynikają wyłącznie z dopasowania przepisów Kodeksu postępowania karnego do fazy, w której treść ta się znajduje. Przechwycenie „na żywo" odbywa się na podstawie przepisów kontroli i utrwalania rozmów, natomiast dostęp do treści przechowywanej – na podstawie przepisów o przeszukaniu. Z punktu widzenia danych, o które chodzi, podział ten nie znajduje ani praktycznego, ani racjonalnego uzasadnienia, wprowadza natomiast niezrozumiałą dychotomię w standardzie ingerencji w wolność komunikowania się. Dostęp do treści będącej w fazie transmisji podlega bowiem ograniczeniom zmierzającym do zachowania proporcjonalności i subsydiarności ingerencji, a także redukcji nadużyć. Jednak treść już dostarczona i zachowana – przez użytkownika lub dostawcę – wpada w ramy prawne przeszukania, tj. czynności, której istotą nie jest ingerencja w komunikację, lecz wykrycie lub zatrzymanie albo przymusowe doprowadzenie osoby podejrzanej, a także znalezienie rzeczy mogących stanowić dowód w sprawie lub podlegających zajęciu w postępowaniu karnym. Tym samym ramy prawne przeszukania nie są w stanie sprostać wymogom

---

nal, oraz w sprawach połączonych C-511/18, C-512/18, C-520/18, La Quadrature du Net i in., EPS 2021, nr 8, s. 28–36; A. Grzelak, *Trybunał Sprawiedliwości ponownie o relacji między koniecznością zwalczania przestępczości a prawem do prywatności – glosa do wyroku TS z 21.12.2016 r. w sprawach połączonych C-203/15 Tele2 Sverige AB oraz C-698/15 Watson, Brice, Lewis*, EPS 2017, nr 3, s. 31–36.

[20] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (tekst jedn.: Dz. U. z 2020 r., poz. 344 ze zm.).

[21] A. Lach, *Przeszukanie na odległość systemu informatycznego*, Prok. i Pr. 2011, nr 9, s. 68; P. Lewulis, *Dowody cyfrowe…*, s. 93–95.

stawianym czynności zakładającej ingerencję w treść komunikacji. Przykładowo, na podstawie trybu przeszukania nie można określić, jak daleko wstecz jest możliwe przeglądanie treści komunikacji, a przecież precyzyjne wskazanie granic temporalnych to jeden z kluczowych wymogów stawianych kontroli i utrwalaniu rozmów[22].

Patrząc zaś na sprawę z perspektywy jednostki, nie ma specjalnego znaczenia, czy organ dotarł do treści konwersacji drogą podsłuchu, czy przeszukania smartfona. Istotne jest przełamanie tajemnicy komunikacji. Trudno o racjonalne argumenty, dlaczego na gruncie polskiego postępowania karnego ochrona dostępu do już istniejących danych dotyczących treści ma charakter znacznie słabszy niż w przypadku pozyskiwania danych w czasie rzeczywistym. Jawność czynności przeszukania również nie polepsza znacząco sytuacji osoby, której treść dotyczy, ponieważ przeszukanie jest jawne wobec użytkownika urządzenia zawierającego treść, a nie uczestników komunikacji.

2. Wyzwania w transgranicznym gromadzeniu danych

Z uwagi na globalizację usług komunikacji elektronicznej pozyskiwanie danych elektronicznych wymaga często zwrócenia się do usługodawcy zagranicznego. Potrzeba ta znajduje odzwierciedlenie w instrumentach współpracy, które w ostatnich latach obierają śmiały kurs i wprowadzają nowy model współpracy międzynarodowej w sprawach karnych oparty na bezpośredniej współpracy organów sądowych państwa, w którym prowadzi się postępowanie, z dostawcą usługi działającym w innej jurysdykcji.

Na gruncie Rady Europy funkcjonuje jedna z najważniejszych międzynarodowych konwencji, przywoływana już wcześniej Konwencja Rady Europy o cyberprzestępczości z 2001 r. Dokument ten m.in. wprowadza w systemach państw sygnatariuszy uniwersalne rozwiązania w zapobieganiu i zwalczaniu szeroko pojętej przestępczości, co ma ułatwić współpracę międzynarodową w tym zakresie. Konwencję ratyfikowało aż 68 państw, w tym również spoza Rady Europy. Do danych dotyczących treści odnosi się wprost art. 21 Konwencji, zgodnie z którym każda strona przyjmuje odpowiednie środki prawne i inne, które mogą być potrzebne dla nadania właściwym organom uprawnień w zakresie gromadzenia lub rejestrowania w czasie rzeczywistym danych dotyczących treści konkretnych przekazów. W raporcie wyjaśniającym podkreślono, że przechwytywanie treści przesyłanej w czasie rzeczywistym jest kluczową czynnością w ściganiu przestępstw, w przypadku których to właśnie treść ujawnia popełnienie czynu zabronionego (np. dziecięca pornografia)[23]. Co ważne, przechwytywanie powinno być możliwe w odniesieniu do „grupy poważnych przestępstw" (art. 21 Konwencji), a także gwarantować odpowiednią ochronę wolności i praw człowieka, w tym

[22] Por. wyrok Europejskiego Trybunału Praw Człowieka (dalej: ETPC) z dnia 24 kwietnia 1990 r. w sprawie Kruslin *v.* Francja, skarga nr 11801/85, § 35.

[23] Raport wyjaśniający do Konwencji Rady Europy o cyberprzestępczości, pkt 228, https://rm.coe.int/16800cce5b [dostęp: 19.04.2024].

sądową lub inną niezależną kontrolę, podawanie uzasadnienia stosowania czy ograniczenia co do zakresu i czasu stosowania (art. 15 Konwencji). Przeszukanie systemu informatycznego reguluje art. 19 Konwencji, nie odnosząc się jednak wprost do możliwości wglądu w treść przechowywanej korespondencji.

Na przestrzeni dwóch dekad funkcjonowania Konwencji konieczne stało się jej uaktualnienie. Z uwagi na postęp technologiczny i rozwój społeczeństwa informacyjnego dane elektroniczne są niezbędne już nie tylko w sprawach związanych z cyberprzestępczością[24]. Spowodowało to przytłoczenie niektórych organów krajowych państw sygnatariuszy Konwencji (zwłaszcza USA) liczbą wniosków kierowanych w sprawie dostępu do danych przechowywanych przez usługodawców. Stało się jasne, że model wzajemnej pomocy prawnej jest niewydajny i konieczne jest nowe podejście. Stąd w 2022 r. przyjęto Drugi protokół dodatkowy do konwencji budapesztańskiej o cyberprzestępczości[25] dotyczący wzmocnionej współpracy i ujawniania elektronicznego materiału dowodowego, wprowadzający m.in. model bezpośredniego kontaktu z dostawcami usług internetowych w sprawie przekazania danych – ale tylko tych dotyczących abonenta. W odniesieniu do danych, które są niezbędne dla identyfikacji na wczesnych etapach postępowania i rzadko mają znaczenie dowodowe, a jednocześnie których gromadzenie uważa się za najmniej ingerujące w prawa fundamentalne, przyjęto więc formułę ich bezpośredniego pozyskiwania od dostawców z innych jurysdykcji, z ominięciem organu sądowego tego państwa. Skrócenie drogi pozyskiwania danych ma odciążyć wzajemną pomoc prawną, bez uszczerbku dla praw osób, których te dane dotyczą.

W Unii Europejskiej dane elektroniczne, w tym dane dotyczące treści, są pozyskiwane w sprawach karnych dwiema drogami: europejskim nakazem dochodzeniowym (dalej: END)[26] oraz europejskim nakazem wydania dowodów (dalej: ENWD), który będzie stosowany od 18 sierpnia 2026 r.[27] Europejski nakaz dochodzeniowy jest właściwy w sprawach wymagających dokonania czynności dowodowej lub przekazania dowodu już istniejącego, podczas gdy ENWD stosuje się w przypadku danych przechowywanych przez dostawcę usługi, w formie bezpośredniego kontaktu – tj. z pominięciem organu wykonującego[28]. Innymi słowy, ENWD jest ścieżką dostępu do danych przechowywanych na serwerach usługodawcy[29] i nie obejmuje przechwytywania

[24] S. Tosza, *All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order*, „New Journal of European Criminal Law" 2020, vol. 11, no. 2, s. 168.

[25] Drugi protokół dodatkowy do Konwencji o cyberprzestępczości o rozszerzonej współpracy i ujawnieniu dowodów elektronicznych (Dz. Urz. UE L 134 z 11.05.2022, s. 15).

[26] Zob. dyrektywa Parlamentu Europejskiego i Rady nr 2014/41/EU z dnia 3 kwietnia 2014 r. w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych (Dz. Urz. UE L 130 z 1.05.2014, s. 1) (dalej: dyrektywa END).

[27] Zob. rozporządzenie ENWD.

[28] Więcej o roli dostawców usług w tym modelu zob. S. Tosza, *Internet service providers as law enforcers and adjudicators. A public role of private actors*, „Computer Law & Security Review" 2021, no. 43, https://doi.org/10.1016/j.clsr.2021.105614 [dostęp: 19.04.2024].

[29] Rozporządzenie ENWD odnosi się do trzech grup danych: dotyczących abonenta, ruchu oraz treści.

przekazów telekomunikacyjnych w czasie rzeczywistym, a END – do gromadzenia danych „na żywo" za pomocą podsłuchu oraz przeszukania urządzenia końcowego, a także przekazania już istniejących danych, o ile są w posiadaniu organu wykonującego[30]. Oba instrumenty opierają się nie tylko na różnych modelach współpracy, ale operują również inną siatką pojęciową. W wąskim kontekście danych dotyczących treści zwiastuje to problemy.

Europejski nakaz dochodzeniowy, flagowy instrument unijnego przepływu dowodów w sprawach karnych, jest niestety pokłosiem trudnych negocjacji i niekompletnego zrealizowania wizji wzajemnego uznawania dowodów w sprawach karnych w UE[31]. Jest to też instrument generyczny, nieuwzględniający w żaden sposób specyfiki dowodów elektronicznych[32]. Przede wszystkim zaś END jest wręcz „przygotowany" na różnice krajowe w czynnościach dowodowych państwach członkowskich, co wynika z zamrożenia przez Unię planu wprowadzenia wzajemnych minimalnych standardów opartych na art. 82.2 Traktatu o funkcjonowaniu Unii Europejskiej[33]. I tak, można odmówić wykonania END, jeśli istnieją istotne przesłanki uznania, że wykonanie czynności dochodzeniowej wskazanej w END byłoby nie do pogodzenia ze spoczywającymi na państwie wykonania obowiązkami wynikającymi z art. 6 Traktatu o Unii Europejskiej i z Karty praw podstawowych UE (art. 11 ust. 1(f) dyrektywy END)[34]. Organ wykonujący dysponuje również ciekawym (choć wątpliwym w świetle zasady wzajemnego uznawania) rozwiązaniem zastosowania czynności innej niż wskazana w END, jeżeli będzie miała taki sam rezultat jak czynność dochodzeniowa wskazana w END przy

---

30 Wynika to z zakresu END, który wydaje się w celu przeprowadzenia czynności dochodzeniowej lub w celu uzyskania materiału dowodowego, którym właściwe organy państwa wykonującego już dysponują (art. 1 dyrektywy END).

31 Wyrażonej na posiedzeniu Rady Europejskiej w 1999 r. w Tampere: „Evidence lawfully gathered by one Member State's authorities should be admissible before the courts of other Member States, taking into account the standards that apply there" – Tampere European Council 15 and 16 October 1999 Presidency Conclusions, s. 36.

32 M. Rojszczak, *e-Evidence Cooperation in Criminal Matters from an EU Perspective*, „Modern Law Review" 2022, vol. 85, issue 4, s. 998–999, https://onlinelibrary.wiley.com/doi/10.1111/1468-2230.12749 [dostęp: 19.04.2024]. Określone w rozdziale IV dyrektywy END przepisy szczegółowe dotyczące niektórych czynności dochodzeniowych odnoszą się do tymczasowego przekazania osób pozbawionych wolności, przesłuchania w formie wideokonferencji lub z wykorzystaniem innej formy przekazu audiowizualnego, przesłuchania w formie konferencji telefonicznej, przekazywania informacji o transakcjach bankowych i innych transakcjach finansowych, czynności dochodzeniowych wymagających gromadzenia materiału dowodowego na bieżąco, w sposób ciągły i przez konkretny okres, oraz dochodzeń niejawnych.

33 Traktat o funkcjonowaniu Unii Europejskiej (wersja skonsolidowana; Dz. Urz. UE C 326 z 26.10.2012, s. 47). M. Kusak, *Common EU Minimum Standards for Enhancing Mutual Admissibility of Evidence Gathered in Criminal Matters*, „European Journal on Criminal Policy and Research", Springer 2017, s. 337–352, http://link.springer.com/article/10.1007/s10610-017-9339-0 [dostęp: 19.04.2024].

34 Traktat o Unii Europejskiej (wersja skonsolidowana; Dz. Urz. UE C 202 z 7.06.2016, s. 1) (dalej: TUE); Karta praw podstawowych Unii Europejskiej (wersja skonsolidowana; Dz. Urz. UE C 202 z 7.06.2016, s. 1). W polskim Kodeksie postępowania karnego przepis ten wdrożono jako obligatoryjną przesłankę odmowy, jeżeli wykonanie END naruszyłoby wolności i prawa człowieka i obywatela (art. 589zj § 1 pkt 5 k.p.k.).

użyciu mniej inwazyjnych środków (art. 10 ust. 3 dyrektywy END). Jeżeli zaś czynność dochodzeniowa wskazana w END nie istnieje w prawie państwa wykonującego lub nie byłaby dopuszczalna w podobnej sprawie krajowej, a brak jest innej czynności dochodzeniowej, która miałaby ten sam skutek co żądana czynność dochodzeniowa, organ wykonujący powiadamia organ wydający, że udzielenie żądanej pomocy nie było możliwe (art. 10 dyrektywy END). Jest to więc *de facto* przesłanka odmowy możliwa do zastosowania w przypadku różnic krajowych w gromadzeniu dowodów pomiędzy współpracującymi państwami. Wydawana na tej podstawie odmowa wykonania END z uwagi na krajowe różnice w podejściu do gromadzenia dowodów elektronicznych wydaje się być bardzo prawdopodobna, o czym będzie jeszcze mowa niżej.

Europejski nakaz wydania dowodów to z kolei śmiały krok w kierunku ułatwienia gromadzenia danych elektronicznych od podmiotów oferujących na terenie UE usługi łączności elektronicznej, społeczeństwa informacyjnego oraz nazw domen internetowych i numeracji IP. Projekt, którego pierwsza wersja została opublikowana w 2018 r.[35], spotkał się z potężną dezaprobatą, zwłaszcza ze strony środowiska związanego z ochroną prywatności i danych osobowych[36]. W ogniu krytyki znalazły się przede wszystkim istota proponowanego modelu współpracy organu wydającego bezpośrednio z dostawcą usługi oraz rezygnacja z udziału organu wykonującego. Model taki ma w założeniu przyspieszyć procedurę gromadzenia danych. Całkowite poleganie na organie wydającym oraz pominięcie organu wykonującego (który w projekcie określa się jako „organ przymuszający", ponieważ jego rolę widzi się raczej w prowadzeniu

[35] Zob. https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52018PC0225 [dostęp: 19.04.2024].

[36] European Data Protection Supervisor, *Opinion 7/2019, EDPS Opinion on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters*, 2019, https://edps.europa.eu/sites/default/files/publication/19-11-06_opinion_on_e_evidence_proposals_en.pdf [dostęp: 19.04.2024]; European Data Protection Board, *Opinion of the EDPB on Commission proposals of the EP and of the Council on European production and preservation orders for electronic evidence in criminal matters*, 2018, https://data.consilium.europa.eu/doc/document/ST-13317-2018-INIT/EN/pdf [dostęp: 19.04.2024]; European Digital Rights, *Recommendations on cross-border access to data. Position paper on the European Commission's proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters*, 2019, https://edri.org/files/e-evidence/20190425-EDRi_PositionPaper_e-evidence_final.pdf [dostęp: 19.04.2024]; *E-evidence Coalition Remarks on the Rapporteur Package Proposal*, 2022, https://www.ebu.ch/files/live/sites/ebu/files/News/Position_Papers/open/2022/Coalition's%20remarks%20on%20EP%20package%20deal.pdf [dostęp: 19.04.2024]; European Judicial Network's Working Group on E-evidence, *Conclusions of the 4th online meeting on the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters*, https://www.statewatch.org/media/1867/eu-council-ejn-e-evidence-ep-position-paper-6035-21.pdf [dostęp: 19.04.2024]; M.D. Cole, T. Quintel, *Transborder Access to e-Evidence by Law Enforcement Agencies* (May 11, 2018), University of Luxembourg Law Working Paper No. 2018-010, https://ssrn.com/abstract=3278780 [dostęp: 19.04.2024]; M. Rogalski, *The European Commission's e-Evidence Proposal – Critical Remarks and Proposals for Changes*, „European Journal of Crime, Criminal Law and Criminal Justice" 2020, vol. 28, issue 4, https://doi.org/10.1163/15718174-BJA10018 [dostęp: 19.04.2024].

dialogu z dostawcą usługi odmawiającym wykonania nakazu) nie wydaje się być jednak kompatybilne ze stanem wzajemnego zaufania w UE[37].

Trwająca przeszło sześć lat gorąca dyskusja nad projektem wynika nie tylko z nowego pomysłu na współpracę, ale oddaje również klimat polityczny, w jakim debata ta była prowadzona. Projekt rozporządzenia powstał bowiem krótko po serii ataków terrorystycznych w UE w latach 2015–2016, w atmosferze rozszerzania uprawnień organów ścigania na rzecz zwiększenia bezpieczeństwa publicznego. Kolejne lata przyniosły jednak nowe wyzwania, które ostudziły wiarę we wzajemne zaufanie pomiędzy państwami członkowskimi. Przykładem są zarówno naruszenia praworządności w państwach członkowskich[38], jak i wątpliwe działania w sferze dowodów elektronicznych w państwach unijnych (czego przykładem jest sprawa EncroChat[39]). Impas w pracach nad modelem dostępu do danych elektronicznych starał się przełamać Parlament Europejski, który uzupełnił projekt o mechanizm notyfikacji[40] mający w określonych przypadkach zapewnić, że „organ przymuszający" będzie posiadał wiedzę o wydanym przez organ innego państwa nakazie i, w przypadku wątpliwości, będzie mógł zareagować, w tym odmówić wykonania nakazu w sytuacjach określonych w rozporządzeniu. „Organ przymuszający" może odmówić wykonania nakazu, jeśli: a) jego wykonanie naruszałoby immunitety i przywileje w państwie przymuszającym; b) byłoby sprzeczne z zasadą *ne bis in idem*; c) przestępstwo, którego dotyczy nakaz, nie jest penalizowane w państwie przymuszającym, z wyjątkiem przestępstw określonych w rozporządzeniu, o ile przekraczają minimalny próg karalności trzech lat; d) istnieją – w wyjątkowych sytuacjach – uzasadnione powody, by przyjąć, że na podstawie konkretnych i obiektywnych dowodów wykonanie nakazu będzie prowadziło do poważnego naruszenia praw fundamentalnych określonych w art. 6 TUE oraz w Karcie praw podstawowych UE[41]. Notyfikacja odnosi się tylko do nakazu w sprawie danych dotyczących ruchu (z wyjątkiem danych służących jedynie identyfikacji użytkownika) oraz danych dotyczących treści – a zatem w sprawach pozyskiwania danych o najwyższym stopniu ingerencji w prawa jednostki. Efektywność mechanizmu notyfikacji jest jednak wątpliwa. Po pierwsze, polega on w pełni na woli organu wydającego. Po drugie, rozporządzenie ENWD zawęża sytuacje, w których notyfikacja jest wskazana, i jeśli przestępstwo zostało popełnione (lub jest to prawdopodobne) na terenie pań-

37 M. Kusak, *Mutual trust to obtain electronic evidence in the EU: Is the bar low or high?* [w:] *Current Issues of EU Criminal Law*, eds. A.H. Ochnio, H. Kuczyńska, Warsaw 2022, s. 73–88.

38 L. Pech, P. Wachowiec, D. Mazur, *Poland's Rule of Law Breakdown: A Five-Year Assessment of EU's (In) Action*, „Hague Journal on the Rule of Law" 2021, vol. 13, s. 1–43, https://doi.org/10.1007/s40803-021-00151-9 [dostęp: 19.04.2024].

39 Por. sprawę toczącą się przed TSUE dotyczącą przepływu dowodów zgromadzonych niezgodnie z prawem wobec użytkowników usługi EncroChat, C-670/22.

40 W uzgodnionej wersji rozporządzenia przyjęto tylko część zmian proponowanych przez Parlament Europejski, w tym związanych z notyfikacją. Więcej informacji: https://www.europarl.europa.eu/legislative-train/theme-a-new-push-for-european-democracy/file-jd-cross-border-access-to-e-evidence-production-and-preservation-orders [dostęp: 19.04.2024].

41 Rozwinięcie tej ostatniej przesłanki znajduje się w pkt 42d preambuły finalnej wersji rozporządzenia ENWD.

stwa wydającego nakaz, lub osoba, której dane dotyczą, przebywa na terenie państwa wydającego – notyfikacja nie ma zastosowania. Mechanizm notyfikacji wydaje się być zatem wąski i kruchy, z uwagi na oparcie go w dużej mierze na standardzie i etyce działania organu wydającego.

Oba omawiane wyżej unijne instrumenty przyjmują skrajne wobec siebie podejścia w gromadzeniu dowodów: o ile END zawiera serię przepisów dających organowi wykonującemu możliwość odmowy wykonania nakazu, w tym w celu ochrony praw podstawowych (ale w sposób „bierny", uwalniając od współpracy, ale nie zmierzając do ogólnego zwiększenia ochrony praw podstawowych w postępowaniu dowodowym), tak w ENWD nacisk położono na efektywność w dostępie do danych, a ochrona praw jednostki wydaje się pozostawać na dalszym planie. Natomiast wspólnym zarzutem zarówno wobec END, jak i ENWD jest obojętność obu instrumentów na potencjalne krajowe różnice w podejściu do dowodów elektronicznych, która może się przekładać na ich gromadzenie oraz wzajemną dopuszczalność. W celu głębszego zweryfikowania tego problemu w latach 2020–2021 prowadzono w ramach grantu Narodowego Centrum Nauki[42] badanie porównawcze siedmiu państw członkowskich: Austrii (AT), Bułgarii (BG), Cypru (CY), Włoch (IT), Litwy (LT), Polski (PL) i Portugali (PT)[43]. Państwa te wybrano ze względu na różne obszary geograficzne, a także różnorodność modeli postępowania karnego. Dane porównawcze zostały zebrane za pomocą kwestionariusza, który rozesłano do odpowiednich ekspertów krajowych, a także na podstawie informacji z EJN Fiches Belges on Electronic Evidence – które składają się z krajowych informacji dostarczonych przez punkty kontaktowe[44]. Wykorzystano również profile wiki zawierające przegląd przepisów w zakresie cyberprzestępczości i elektronicznego materiału dowodowego[45].

Badanie potwierdziło hipotezę o różnicach w standardzie dostępu do elektronicznych danych dotyczących treści. W odniesieniu do danych gromadzonych w czasie rzeczywistym zasadniczą różnicą jest ujęcie tej czynności w krajowym porządku prawnym. O ile ustawy karnoprocesowe w niektórych krajach (AT, PT) wprost regulują przechwytywanie rozmów prowadzonych drogą elektroniczną, to inne kraje (w tym PL, IT, LT) stosują w takich sprawach odpowiednio przepisy o podsłuchu telefonicznym[46]. Różne podejścia nie przekładają się jednak na kluczowe gwarancje związane z kontrolowaniem rozmów. We wszystkich państwach czynność tę zawężono do poważnych przestępstw, ujętych jednak w inny sposób – w formie katalogu przestępstw lub progiem karalności. Wszędzie konieczna jest również autoryzacja *ex ante* lub *ex post*

---

42 Projekt nr 2016/23/D/HS5/00182.

43 Wyniki badań w druku.

44 https://www.ejn-crimjust.europa.eu/ejn2021/ContentDetail/EN/6/88 [dostęp: 19.04.2024].

45 Country Wiki, https://www.coe.int/en/web/octopus/country-wiki [dostęp: 19.04.2024].

46 Z państw objętych badaniem Bułgaria dopuszcza przechwytywanie danych elektronicznych tylko w ramach czynności służb specjalnych, a Cypr nie przewiduje takiej możliwości w ogóle. Wniosek ten potwierdzają również badania komparatystyczne prowadzone przez naukowców z Uniwersytetu im. Adama Mickiewicza w Poznaniu w ramach projektu unijnego „Improving the application of the presumption of innocence when applying electronic evidence" (INNOCENT, Agreement no. 101056685).

(w szczególnych wypadkach) przez organ sądowy. Podobieństwa wykazało także badanie czasu trwania czynności – jasne reguły czasu trwania oraz warunków przedłużania określono we wszystkich państwach, choć ramy te dość mocno się od siebie różnią.

Znacznie większe różnice ujawniło porównanie dostępu do przechowywanej treści komunikacji. W trzech państwach (AT, IT i PT)[47] przepisy krajowe zabraniają dostępu do przechowywanej treści komunikacji, która jest osiągalna wyłącznie za pomocą przechwytywania komunikacji w czasie rzeczywistym. W pozostałych krajach (poza Cyprem) czynność ta jest dopuszczalna w trybie dostępu do urządzenia lub za pośrednictwem dostawcy usług. W państwach, gdzie dostęp jest dopuszczalny, stosuje się zaś standard podobny do podsłuchu rozmów telefonicznych, w szczególności udział organu sądowego. Wyjątkiem w tym zakresie jest Polska.

Główny wniosek płynący z badania komparatystycznego jest więc następujący: o ile w przypadku dostępu do danych dotyczących treści w czasie rzeczywistym stosuje się podobny standard oparty zasadniczo na podsłuchu rozmów, o tyle dostęp do danych przechowywanych wykazuje skrajne podejścia – od wyraźnego ujęcia przez ustawodawcę, że ingerencja w przechowywaną treść komunikacji nie jest możliwa, przez dostęp do danych już istniejących na warunkach podobnych do podsłuchu, po stosowanie przepisów dotyczących przeszukania. Różnice krajowe będą zapewne źródłem wątpliwości we współpracy w dostępie do elektronicznych danych dotyczących treści zarówno w odniesieniu do END, jak i do ENWD.

Wnioski i postulaty *de lege ferenda*

W obecnym stanie rozwoju technologii wpływającej na sposoby komunikowania się konieczne jest przesądzenie w sposób jednoznaczny, w jakim trybie ma się odbywać dostęp do elektronicznych danych dotyczących treści, niezależnie od tego, czy są one przechwytywane „na żywo", czy też na podstawie dostępu do przechowywanych danych. Gromadzenie danych dotyczących treści za pomocą czynności „tradycyjnych" nie sprawdza się, prowadzi do wątpliwości interpretacyjnych i różnic w standardzie ochrony praw jednostki. Przepisy o kontroli i utrwalaniu rozmów nie odnoszą się do problemów szyfrowania, a art. 241 k.p.k. jest źle sformułowany i od momentu wprowadzenia budzi wątpliwości co do znaczenia pojęcia „treści innych rozmów lub przekazów informacji"[48]. Natomiast czynność tak głęboko ingerująca w prawa i wolności człowieka, jak kontrola treści rozmów nie może w demokratycznym państwie prawa być niedookreślona i nieprecyzyjna[49]. Przepisy powinny również pozostawić jak najmniej wątpliwości co do tego, czy dane należy pozyskiwać czynnościami procesowymi czy

[47] Przepisy na Cyprze zabraniają dostępu do treści komunikacji w ogóle – Police *v.* Georghiades (1983) 2 CLR 33, http://www.cylaw.org/cgi-bin/open.pl?file=/apofaseis/aad/meros_2/1983/rep/1983_2_0033.htm [dostęp: 19.04.2024].

[48] M. Rogalski, *Kontrola i utrwalanie*…, s. 4057–4058.

[49] Por. wyroki ETPC z dnia: 29 czerwca 2006 r. w sprawie Weber i Saravia *v.* Niemcy, skarga nr 54934/00, § 96 oraz 15 stycznia 2015 r. w sprawie Dragojević *v.* Chorwacja, skarga nr 68955/11, § 83.

operacyjnymi. Obecnie, z uwagi na niewystarczający charakter trybów kodeksowych, dostęp do treści może być w praktyce prostszy w ramach czynności pozaprocesowych, które z zasady charakteryzują się niższym stopniem gwarancyjności.

Argumentem za opracowaniem odrębnych zasad umożliwiających uzyskanie tak dalece wrażliwych informacji jak elektroniczne dane dotyczące treści są również instrumenty unijne regulujące dostęp do takich danych w drodze współpracy pomiędzy państwami członkowskimi. Niski, krajowy standard w gromadzeniu takich danych może utrudniać wykonanie lub być przesłanką do odmowy wykonania zarówno END, jak i ENWD. Tymczasem, na co wskazuje badanie komparatystyczne, większość państw członkowskich dostrzega specyfikę elektronicznych danych dotyczących treści, w tym ich „dwufazowość" i wynikające z niej z różne progi dostępu przez organy.

De lege ferenda procesowy dostęp do elektronicznych danych dotyczących treści, niezależnie od fazy, w której się znajdują, powinien się opierać na konstrukcji kontroli i utrwalania rozmów. Jest to bowiem czynność skrojona na potrzeby ochrony komunikacji, w której chodzi przecież o to, aby uniemożliwić przejęcie wiadomości przez osoby nieuprawnione[50]. Dostęp do treści, niezależnie, czy tej „na żywo", czy tej przechowywanej, wymaga ograniczenia zakresu przedmiotowego[51], podmiotowego, kontroli sądu oraz określenia granic temporalnych (w przypadku danych przechowywanych zasadne byłoby więc określenie, jak daleko wstecz możliwy jest wgląd w treści). Z badania komparatystycznego wynika zresztą, że właśnie taka konstrukcja prawna jest często stosowana w innych krajach. Z uwagi na realne trudności w dostępie do danych oraz potencjalne ryzyko nadużyć uzasadnione byłoby ujęcie w Kodeksie postępowania karnego warunków instalowania oprogramowania z kluczem do szyfrowanych wiadomości lub zdalnego przeszukania urządzenia. Poza specyficznymi dla treści rozwiązaniami Kodeks powinien również określać standard typowy dla wszystkich rodzajów danych elektronicznych, tj. kompetencje osób dokonujących ingerencji w dane, warunki ochrony integralności danych, tworzenia kopii i ich udostępniania stronom, udział biegłego w procesie ingerencji w dane i ich interpretacji. Takie ujęcie dostępu do elektronicznych danych dotyczących treści uporządkowałoby reguły dostępu przez organy, zlikwidowało dychotomię w standardzie ochrony osób, których dane dotyczą, oraz wyeliminowało prawne i techniczne wątpliwości w zakresie nieefektywnego i nieprzystającego do realiów odpowiedniego stosowania przepisów.

Literatura

Cole M.D., Quintel T., *Transborder Access to e-Evidence by Law Enforcement Agencies* (May 11, 2018), University of Luxembourg Law Working Paper No. 2018-010, https://ssrn.com/abstract=3278780.

[50] M. Rogalski, *Tajemnica komunikowania się w prawie polskim* [w:] *idem*, *Podsłuch procesowy i pozaprocesowy. Kontrola i utrwalanie rozmów na podstawie kpk oraz ustaw szczególnych*, Warszawa 2019.

[51] Tak: wyroki ETPC z dnia: 4 grudnia 2015 r. w sprawie Roman Zakharov *v.* Rosja, skarga nr 47143/06, § 243 i nn. oraz 10 lutego 2009 r. w sprawie Iordachi i inni *v.* Mołdawia, skarga nr 25198/02, § 41 i nn.

Dudka K., *Podsłuch komputerowy w polskim procesie karnym – wybrane zagadnienia praktyczne*, „Prokuratura i Prawo" 1999, nr 1.

Grzelak A., *Trybunał Sprawiedliwości ponownie o relacji między koniecznością zwalczania przestępczości a prawem do prywatności – glosa do wyroku TS z 21.12.2016 r. w sprawach połączonych C-203/15 Tele2 Sverige AB oraz C-698/15 Watson, Brice, Lewis*, „Europejski Przegląd Sądowy" 2017, nr 3.

Grzelak A., Zielińska K., *Między prawem do prywatności i ochrony danych osobowych a zapewnieniem bezpieczeństwa publicznego i walką z przestępczością. Problemu retencji danych ciąg dalszy – glosa do wyroków Trybunału Sprawiedliwości z 6.10.2020 r.: C-623/17, Privacy International, oraz w sprawach połączonych C-511/18, C-512/18, C-520/18, La Quadrature du Net i in.*, „Europejski Przegląd Sądowy" 2021, nr 8.

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

Lach A., *Gromadzenie dowodów elektronicznych po nowelizacji k.p.k.*, „Prokuratura i Prawo" 2003, nr 10.

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

Lewulis P., *Dowody cyfrowe – teoria i praktyka kryminalistyczna*, Warszawa 2021.

Kremens K., *O znaczeniu prawa porównawczego dla nauki polskiego procesu karnego na przykładzie przeszukań telefonów komórkowych* [w:] *W pogoni za rzetelnym procesem karnym. Księga dedykowana Profesorowi Stanisławowi Waltosiowi*, red. D. Szumiło-Kulczycka, Warszawa 2022.

Kusak M., *Common EU Minimum Standards for Enhancing Mutual Admissibility of Evidence Gathered in Criminal Matters*, „European Journal on Criminal Policy and Research", Springer 2017, http://link.springer.com/article/10.1007/s10610-017-9339-0.

Kusak M., *Mutual trust to obtain electronic evidence in the EU: Is the bar low or high?* [w:] *Current Issues of EU Criminal Law*, eds. A.H. Ochnio, H. Kuczyńska, Warsaw 2022.

Pech L., Wachowiec P., Mazur D., *Poland's Rule of Law Breakdown: A Five-Year Assessment of EU's (In)Action*, „Hague Journal on the Rule of Law" 2021, vol. 13, https://doi.org/10.1007/s40803-021-00151-9.

Rojszczak M., *e-Evidence Cooperation in Criminal Matters from an EU Perspective*, „Modern Law Review" 2022, vol. 85, issue 4, https://onlinelibrary.wiley.com/doi/10.1111/1468-2230.12749.

Rogalski M., *Kontrola i utrwalanie treści innych rozmów lub przekazów informacji* [w:] *System prawa karnego procesowego*, t. 8, *Dowody*, cz. 3, red. J. Skorupka, Warszawa 2019.

Rogalski M., *Potrzeba zmiany przepisów Kodeksu postępowania karnego w zakresie kontroli korespondencji oraz kontroli i utrwalania rozmów telefonicznych* [w:] *W pogoni za rzetelnym procesem karnym. Księga dedykowana Profesorowi Stanisławowi Waltosiowi*, red. D. Szumiło-Kulczycka, Warszawa 2022.

Rogalski M., *Tajemnica komunikowania się w prawie polskim* [w:] *idem*, *Podsłuch procesowy i pozaprocesowy. Kontrola i utrwalanie rozmów na podstawie kpk oraz ustaw szczególnych*, Warszawa 2019.

Rogalski M., *The European Commission's e-Evidence Proposal – Critical Remarks and Proposals for Changes*, „European Journal of Crime, Criminal Law and Criminal Justice" 2020, vol. 28, issue 4, https://doi.org/10.1163/15718174-BJA10018.

Siwicki M., *Przetwarzanie danych informatycznych w chmurach obliczeniowych. Wybrane aspekty prawnokarne i procesowe*, „Palestra" 2005, nr 1–2.

Szumiło-Kulczycka D., *Wolność i tajemnica komunikowania się* [w:] *eadem*, *Czynności operacyjno-rozpoznawcze i ich relacje do procesu karnego*, Warszawa 2012.

Tosza S., *All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order*, „New Journal of European Criminal Law" 2020, vol. 11, no. 2.

Tosza S., *Internet service providers as law enforcers and adjudicators. A public role of private actors*, „Computer Law & Security Review" 2021, no. 43, https://doi.org/10.1016/j.clsr.2021.105614.

Warken C., van Zwietenband L., Svantesson D., *Re-thinking the categorisation of data in the context of law enforcement cross-border access to evidence*, „International Review of Law, Computers & Technology" 2020, vol. 34, https://doi.org/10.1080/13600869.2019.1600871.

Wiliński P., *Ochrona tajemnicy komunikowania się (art. 49 Konstytucji RP)* [w:] *System prawa karnego procesowego. Tom I. Zagadnienia ogólne*, red. P. Hofmański, Warszawa 2013.

Streszczenie

Martyna Kusak

Dostęp do danych elektronicznych dotyczących treści w postępowaniu karnym – wyzwania krajowe i międzynarodowe

Komunikacja na odległość nie sprowadza się już do rozmów telefonicznych, ale obejmuje również wiadomości tekstowe, głosowe czy zdjęcia przesyłane za pomocą aplikacji, komunikatorów internetowych, poczty elektronicznej, portali społecznościowych, a także korzystanie z telefonii internetowej. Nowe formy komunikowania się generują treść, do której dostęp może okazać się potrzebny w postępowaniu karnym. Pomimo wszechobecności elektronicznych danych dotyczących treści ich pozyskiwanie na podstawie Kodeksu postępowania karnego jest nieoczywiste i nieprzystające ani do prawnych standardów ingerencji w tajemnicę komunikacji, ani realiów technicznych związanych z tego rodzaju danymi. W artykule przedstawiono tryby *de lege lata* gromadzenia treści elektronicznych zarówno na poziomie krajowym, jak i w ramach współpracy międzynarodowej, a także postulaty *de lege ferenda*, opierające się na postulacie stosowania do takich danych modelu podobnego do kontroli i utrwalania rozmów.

Słowa kluczowe: dane elektroniczne, dane dotyczące treści, inwigilacja, dowody elektroniczne, europejski nakaz dochodzeniowy, europejski nakaz wydania dowodów.

Summary

Martyna Kusak

Access to Electronic Content Data in Criminal Proceedings – National and International Challenges

Modern distant communication is no longer limited to telephone calls. It also includes text messages, voice messages or photos sent via applications, instant messaging, e-mail, social networking sites, and VoIP channels. These new forms of communication generate content that may need to be accessed in criminal proceedings. Despite the ubiquity of electronic content data, its acquisition under the Code of Criminal Procedure is non-obvious and complies neither

with the legal standards of interference with the secrecy of communication nor with the technical realities associated with such data. Therefore, the article presents *de lege lata* modes of collecting electronic content both at the national level and within the framework of international cooperation, as well as *de lege ferenda* postulates for applying a model similar to the telephone tapping.

Keywords: electronic data, content data, surveillance, electronic evidence, European investigation order, European production order.