POZYSKIWANIE DOWODÓW ELEKTRONICZNYCH

przez organy ścigania i wymiaru sprawiedliwości

Karolina Kiejnich-Kruk

Wolters Kluwer

POZYSKIWANIE DOWODÓW ELEKTRONICZNYCH

przez organy ścigania i wymiaru sprawiedliwości

Karolina Kiejnich-Kruk

Wolters Kluwer

WARSZAWA 2026

Stan prawny na 1 stycznia 2026 r.

Karolina Kiejnich-Kruk, nr ORCID: 0000-0003-1551-5448

Publikacja częściowo finansowana przez Wydział Prawa i Administracji
Uniwersytetu im. Adama Mickiewicza w Poznaniu

Recenzent
Dr hab. Dariusz Świecki, prof. Uniwersytetu Łódzkiego

Wydawczyni
Monika Pawłowska

Redaktorka prowadząca
Katarzyna Gierłowska

Opracowanie redakcyjne
Joanna Ośka

Projekt okładek serii
Wojtek Janikowski, Przemek Dębowski

prawolubni

Ta książka jest wspólnym dziełem twórcy i wydawcy. Prosimy, byś przestrzegał przysługujących im praw. Książkę możesz udostępnić osobom bliskim lub osobiście znanym, ale nie publikuj jej w internecie. Jeśli cytujesz fragmenty, nie zmieniaj ich treści i koniecznie zaznacz, czyje to dzieło. A jeśli musisz skopiować część, rób to jedynie na użytek osobisty.

Szanujmy prawo i własność
Więcej na www.legalnakultura.pl
Polska Izba Książki

© Copyright by Wolters Kluwer Polska Sp. z o.o., 2026

ISBN 978-83-8438-127-4 *ISBN PDF-a: 978-83-8438-236-3*

Wolters Kluwer Polska Sp. z o.o.
Dział Zarządzania Prawami Autorskimi i Treściami
01-208 Warszawa, ul. Przyokopowa 33
tel. +48 692 477 076
e-mail: PL-ksiazki@wolterskluwer.com
księgarnia internetowa www.profinfo.pl

SPIS TREŚCI

WYKAZ SKRÓTÓW

BEREC	– Organ Europejskich Regulatorów Łączności Elektronicznej
DSA	– rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z 19.10.2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych) (Dz.Urz. UE L 277, s. 1)
EKŁE	– dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z 11.12.2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (wersja przekształcona) (Dz.Urz. UE L 321, s. 36)
EKPC	– Konwencja o ochronie praw człowieka i podstawowych wolności, sporządzona w Rzymie 4.11.1960 r., zmieniona następnie Protokołami nr 3, 5, 8 oraz uzupełniona Protokołem nr 2 (Dz.U. z 1993 r. Nr 61, poz. 284 ze zm.)
END	– europejski nakaz dochodzeniowy
EPO	– europejski nakaz wydania dowodów
EPOC	– zaświadczenie europejskiego nakazu wydania dowodów
ETPC	– Europejski Trybunał Praw Człowieka
k.p.k.	– ustawa z 6.06.1997 r. – Kodeks postępowania karnego (Dz.U. z 2025 r. poz. 46 ze zm.)
Karta	– Karta praw podstawowych Unii Europejskiej (Dz.Urz. UE C 202 z 2016 r., s. 389)
LED	– dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z 27.04.2016 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, s. 89)

OSINT	– *open-source intelligence*, tzw. biały wywiad
p.k.e.	– ustawa z 12.07.2024 r. – Prawo komunikacji elektronicznej (Dz.U. poz. 1221)
rozporządzenie w sprawie e-dowodów	– rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1543 z 12.07.2023 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, s. 118)
RPO	– Rzecznik Praw Obywatelskich
SOP	– standardowa procedura operacyjna
TOC	– rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/784 z 29.04.2021 r. w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym (Dz.Urz. UE L 172, s. 79)
TSUE	– Trybunał Sprawiedliwości Unii Europejskiej
u.o.d.o.z.z.p.	– ustawa z 14.12.2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2023 r. poz. 1206 ze zm.)
u.ś.u.d.e.	– ustawa z 18.07.2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2024 r. poz. 1513 ze zm.)

WSTĘP

Dowody elektroniczne występują obecnie w ok. 85% postępowań karnych prowadzonych w Europie[1]. Dotyczy to nie tylko postępowań z zakresu tzw. cyberprzestępstw, lecz także tych prowadzonych w sprawach przestępstw tradycyjnych. Pozyskanie i analiza dowodów elektronicznych są często niezbędne dla realizacji celów postępowania karnego, w szczególności wykrycia sprawcy przestępstwa i ustalenia relewantnych okoliczności sprawy. Jednocześnie, zarówno pozyskanie, jak i analiza tych dowodów przedstawiają nierzadko znaczną trudność dla organów ścigania oraz sądu. Wynika to przede wszystkim z szybkiego rozwoju nowych technologii, braku odpowiednich kompetencji cyfrowych po stronie uczestników postępowań, rozproszenia źródeł prawa i informacji o dostępnych instrumentach pozyskiwania owych dowodów.

Na potrzeby niniejszej publikacji zdecydowano się na posłużenie pojęciem dowodów elektronicznych, rozumianych jako dane związane z aktywnością użytkowników w sieci Internet, gromadzonych na potrzeby procesu karnego, na które składają się dane o treści, o ruchu i abonencie. Pojęcie to nie odnosi się więc do formy, w jakiej prezentowane czy przechowywane są owe dane. W ramach prezentowanych w doktrynie stanowisk

[1] Rada Europejska, *Łatwiejszy dostęp do e-dowodów – skuteczniejsza walka z przestępczością*, https://www.consilium.europa.eu/en/policies/e-evidence/ (dostęp: 4.07.2023); R. Stoykova, *Digital evidence: Unaddressed threats to fairness and the presumption of innocence*, „Computer Law & Security Review" 2021/42, s. 1 (dostęp: 4.07.2023 r.); L. Geddes, *Digital forensics experts prone to bias, study shows*, „Guardian" (31.05.2021), https://www.theguardian.com/science/2021/may/31/digital-forensics-experts-prone-to-bias-study-shows (dostęp: 4.07.2023 r.).

co do terminologii w tym zakresie odwołać się można do kompleksowej analizy przedstawionej przez P. Lewulisa[2]. Wskazać również można na wątpliwości terminologiczne, które pojawiły się na etapie unijnych prac legislacyjnych nad regulacją o e-dowodach[3].

Dowody elektroniczne na gruncie europejskim ujmowane są w trzech kategoriach[4]:

1) dane dotyczące treści (*content data*),
2) dane dotyczące abonenta (*subscriber data*) oraz
3) dane dotyczące ruchu (*traffic data*).

W ślad za unijnym rozporządzeniem w sprawie e-dowodów[5], które stanowi najnowszą regulację prawną w interesującym nas obszarze, wskazać należy, że:

1) dane dotyczące treści oznaczają wszelkie dane w formacie cyfrowym takie jak tekst, głos, wideo, obrazy i dźwięk, inne niż dane abonenta lub dane o ruchu;

---

[2] P. Lewulis, *Dowody cyfrowe – teoria i praktyka kryminalistyczna w polskim postępowaniu karnym*, Warszawa 2021, s. 30–37.

[3] T. Christakis, *From Mutual Trust to the Gordian Knot of Notificatio*n [w:] *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, red. V. Franssen, S. Tosza, Cambridge 2025, s. 181.

[4] Por. rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1543 z 12.07.2023 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, s. 118); Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23.11.2001 r. (Dz.U. z 2015 r. poz. 728); Drugi protokół dodatkowy do Konwencji o cyberprzestępczości dotyczący wzmocnionej współpracy i ujawniania elektronicznego materiału dowodowego (Dz.Urz. UE L 63, s. 28); zob. także propozycje alternatywnych podziałów rodzaju danych: 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" 2020/34, s. 44–64.

[5] Zob. art. 3 pkt 9–12 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/1543 z 12.07.2023 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, s. 118).

2) dane abonenta oznaczają dane dotyczące:
   a) tożsamości abonenta, takie jak imię i nazwisko, data urodzenia, adres pocztowy lub geograficzny, dane rozliczeniowe i dotyczące 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, z wyjątkiem haseł i innych środków uwierzytelnienia stosowanych zamiast hasła;
3) dane o ruchu oznaczają dane związane ze świadczeniem usługi oferowanej przez usługodawcę, takie jak dane dotyczące źródła i miejsca przeznaczenia wiadomości lub interakcji innego rodzaju, dane na temat lokalizacji urządzenia, daty, czasu, czasu trwania, rozmiaru, trasy, formatu, wykorzystanego protokołu i typu kompresji, a także inne metadane i dane pochodzące z łączności elektronicznej, inne niż dane abonenta, dotyczące rozpoczęcia i zakończenia sesji dostępu użytkownika do usługi, takie jak data i czas korzystania z usługi, logowanie do i wylogowanie z usługi.

Rozporządzenie w sprawie e-dowodów wyróżnia również czwartą kategorię danych, tj. dane, których zażądano wyłącznie w celu identyfikacji użytkownika. Oznacza to dane takie jak adresy IP oraz, w razie potrzeby, odpowiednie porty źródłowe i znaczniki czasu lub techniczne odpowiedniki tych identyfikatorów i związanych z nimi informacji, jeżeli zażądały ich organy wyłącznie w celu identyfikacji użytkownika w konkretnym postępowaniu karnym. Jest to więc podkategoria danych o ruchu. Podział ten obecnie nie jest znany polskim ustawom, niemniej jednak z powodzeniem może być wykorzystywany na potrzeby omawiania również regulacji krajowych. Tak też uczyniono na potrzeby tej książki.

Mając na uwadze, że obecnie komunikacja tradycyjna zastępowana jest komunikacją internetową, powstają uzasadnione wątpliwości w zakresie możliwości pozyskania danych jej dotyczących. Odnoszą się one w szczególności do następujących obszarów:
1) jakie dane można pozyskać,
2) od kogo,

3) w jaki sposób i na jakiej podstawie,
4) w jakim okresie czasowym,
5) jakie wnioski można wyciągnąć z analizy owych danych,
6) jak ocenić wiarygodność, autentyczność i rzetelność owych danych.

Celem niniejszej publikacji jest przedstawienie schematów pozyskania dowodów elektronicznych na etapie postępowania karnego (brak odwołań do tzw. ustaw policyjnych i etapu przedprocesowego) od usługodawców internetowych, tj. podmiotów świadczących usługi drogą elektroniczną, dostawców Internetu, dostawców komunikatorów internetowych. Jednocześnie, dokonano rozróżnienia na procesy pozyskiwania danych od podmiotów krajowych oraz od podmiotów zagranicznych. Jest to o tyle istotne, że często występujący w omawianych postępowaniach element transgraniczny przesuwa punkt ciężkości rozważań w kierunku prawodawstwa międzynarodowego, przede wszystkim unijnego. Jednocześnie, analiza ograniczona została do kwestii pozyskiwania danych w sytuacji braku dostępu do urządzeń elektronicznych. Pozyskiwanie danych z takich urządzeń przez organy ścigania jest bowiem co do zasady zagadnieniem z dziedziny kryminalistyki[6] i zostało już wielokrotnie omówione w doktrynie[7]. W przeciwieństwie więc do sytuacji braku dostępu do urządzenia, jest to zagadnienie dobrze rozpoznane przez praktykę organów ścigania i wymiaru sprawiedliwości.

---

[6] D. Pawlaszczyk, *Mobile Forensics – The End of a Golden Age?*, „Journal of Forensic Sciences & Criminal Investigation" 2022/15(4), s. 1, https://juniperpublishers.com/jfsci/pdf/JFSCI.MS.ID.555917.pdf (dostęp: 6.10.2025 r.).

[7] Rada Europy, *Standard Operating Procedures for the collection, analysis and presentation of electronic evidence*, 2019, https://rm.coe.int/3692-sop-electronic-evidence/168097d7cb (dostęp: 6.10.2025 r.); CEN, *Requirements and Guidelines for a complete end-to-end mobile forensic investigation chain*, 2022, https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::FSP_PROJECT,FSP_ORG_ID:75304,2780164&cs=1D3C72A411BB5C37394D9CECD56A5F57F (dostęp: 6.10.2025 r.); D. Pawlaszczyk, Ch. Hummert (red.), *Mobile Forensics – The File Format Handbook. Common File Formats and File Systems Used in Mobile Devices*, Monachium 2022; D. Pawlaszczyk, Ch. Hummert, *Making the Invisible Visible – Techniques for Recovering Deleted SQLite Data Records*, „International Journal of Cyber Forensics and Advanced Threat Investigations" 2020/1(1–3), s. 27.

W pierwszej części tekstu omówiono dwa podstawowe zagadnienia związane z pozyskiwaniem dowodów na potrzeby procesu karnego: kwestię dostępu do danych oraz kwestię subsydiarną, tj. obowiązki i warunki retencji owych danych przez usługodawców internetowych. W drugiej części publikacji przedstawiono omówienie przykładowych spraw karnych, w których dowody elektroniczne stanowiły istotny dowód w sprawie. Dalej wskazano na przykłady dobrych i złych praktyk w zakresie postępowania z danymi, jak również na kwestię standardowych procedur operacyjnych w tym zakresie. W trzeciej części książki znajdują się schematy graficzne pozyskania dowodów elektronicznych przez organy ścigania oraz sądy w różnych układach procesowych. Należy mieć jednak na uwadze, że schematy te nie przewidują wszystkich możliwych scenariuszy procesowych (np. postępowań w przypadku tajemnic prawnie chronionych) – obrazują natomiast standardowe procedury w danym zakresie.

Rozdział I

INSTRUMENTY POZWALAJĄCE NA POZYSKIWANIE DOWODÓW ELEKTRONICZNYCH DLA CELÓW POSTĘPOWANIA KARNEGO

1. Instrumenty przewidziane w prawie krajowym

1.1. Uwagi ogólne

W zakresie gromadzenia dowodów elektronicznych znaczenie mają przede wszystkim ustawy: ustawa o świadczeniu usług drogą elektroniczną[1], Prawo komunikacji elektronicznej[2] oraz Kodeks postępowania karnego[3]. Pierwsza z nich reguluje obowiązki i uprawnienia podmiotów świadczących usługi drogą elektroniczną, tj. usługi świadczone na odległość, poprzez przekaz danych na indywidualne żądanie usługobiorcy, przesyłanej i otrzymywanej za pomocą urządzeń do elektronicznego przetwarzania i przechowywania danych (art. 2 pkt 4 u.ś.u.d.e.). Takimi usługodawcami są podmioty oferujące usługę poczty e-mail, komunikatory internetowe, ale też fora internetowe czy serwisy sprzedażowe (marketplace). Prawo komunikacji

[1] Ustawa z 18.07.2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2024 r. poz. 1513).

[2] Ustawa z 12.07.2024 r. – Prawo komunikacji elektronicznej (Dz.U. poz. 1221 ze zm.).

[3] Ustawa z 6.06.1997 r. – Kodeks postępowania karnego (Dz.U. z 2025 r. poz. 46 ze zm.).