Stanisław Tosza
Uniwersytet w Luksemburgu, Luksemburg
stanislaw.tosza@uni.lu
ORCID: 0000-0002-3265-1460

https://doi.org/10.26881/gsp.2024.2.03

W poszukiwaniu dowodów elektronicznych – europejski nakaz wydania dowodów elektronicznych oraz inne narzędzia międzynarodowego pozyskiwania danych dla potrzeb postępowania karnego[1]

Wprowadzenie

Nie ma takiego przestępstwa, którego współcześnie nie można by potencjalnie udowodnić przy pomocy dowodów elektronicznych. Nie tylko cyberprzestępstwa, lecz wszelka przestępcza aktywność pozostawia ślady cyfrowe. Nawet w przypadku przestępstw niemających żadnego związku z cyberprzestrzenią dane elektroniczne mogą okazać się kluczowym materiałem dowodowym. Może to być zdjęcie lub nagranie z miejsca przestępstwa zarejestrowane na telefonie (np. zarejestrowane przez samego sprawcę i wysłane do innej osoby), może to być fragment komunikacji, w ramach której sprawca chwali się przestępstwem lub dzieli obawami wynikającymi z jego popełnienia. Może to być również rejestracja lokalizacji miejsca połączenia z siecią telefonu lub działającej w momencie popełnienia czynu zabronionego aplikacji. Skuteczność postępowania karnego zależy dziś więc od posiadania efektywnych sposobów uzyskiwania takich danych na potrzeby dowodowe w postępowaniu karnym.

Ponieważ dane te są w rękach dostarczycieli różnego rodzaju usług, kluczowe dla tej skuteczności będą instytucje karnoprocesowe umożliwiające żądanie tego rodzaju danych od usługodawców. Krajowe przepisy postępowania karnego pozwalają organom na żądanie tych danych od krajowych usługodawców, przy jednoczesnym zagwarantowaniu podejrzanym ochrony ich gwarancji procesowych. Jednakże stosunkowo często usługodawcy – zwłaszcza ci najwięksi i najpopularniejsi (jak Google czy Meta) – są zlokalizowani w innym państwie, a nierzadko przechowują dane jeszcze w innym kraju bądź w chmurze cyfrowej. Z tego wynika, według tradycyjnego podejścia do

[1] W artykule wykorzystano fragmenty wcześniejszych publikacji autora: S. Tosza, *Cross-Border Gathering of Electronic Evidence: Mutual Legal Assistance, Its Shortcomings and Remedies* [w:] *Société numérique et droit pénal: Belgique, France, Europe*, sous la direction de V. Franssen, D. Flore, Bruxelles 2019 oraz *idem*, *The E-Evidence Package is Adopted: End of a Saga or Beginning of a New One?*, „European Data Protection Law Review" 2023, no. 2.

pojęcia terytorialności, konieczność posłużenia się instrumentami współpracy międzynarodowej, aby uzyskać dostęp do przywoływanych tu danych.

Jednakże instrumenty te wydłużają i komplikują postępowanie w sprawach, które same z siebie nie zawierają koniecznie żadnego komponentu międzynarodowego. W sytuacjach, gdy istnieje konieczność zwrócenia się o pomoc prawną do Stanów Zjednoczonych (a najwięksi usługodawcy podlegają prawu właśnie tego kraju), średnia długość procedury pomocy prawnej dla celów uzyskania dowodów elektronicznych będących w posiadaniu amerykańskich dostarczycieli usług wynosi prawie rok[2]. Jeśli zachodzi konieczność współpracy z innym państwem członkowskim Unii Europejskiej, można dziś zastosować europejski nakaz dochodzeniowy (dalej: END). Jednak standardowy termin jego wykonania to 120 dni[3].

Zastosowanie wzajemnej pomocy prawnej wymaga poświęcenia czasu przez szereg funkcjonariuszy organów wymiaru sprawiedliwości obu krajów. Europejski nakaz dochodzeniowy jest w porównaniu z międzynarodową pomocą prawną prostszy, ale dalej angażuje organy w kraju, który bardzo często nie ma nic wspólnego ze sprawą, której dotyczy prośba, poza faktem, przypadkowym w kontekście rzeczonego postępowania karnego, że dostarczyciel usług lub dane znajdują się na terytorium tego kraju.

Stąd powstaje pytanie, czy nie można dopuścić, by organ poszukujący dowodów elektronicznych mógł – transgranicznie – zwrócić się bezpośrednio do dostarczyciela usług o wydanie tych dowodów. Od wielu lat obserwuje się tendencję, by taką możliwość stworzyć. Stoi ona jednak w sprzeczności z uświęconą i rozwiniętą w prawie międzynarodowym po pokoju westfalskim z 1648 r. zasadą ograniczającą możliwość działania organów ścigania do granic ich własnego kraju. Zasada ta jednak nie wytrzymuje konfrontacji z realiami cyberprzestrzeni, która lekko traktuje barierę, jaką jest fizyczna granica państwa.

Celem niniejszego artykułu jest przedstawienie problemów, jakie zbieraniu dowodów elektronicznych stwarza zasada terytorialności, oraz rozwiązań, które próbuje się zastosować, żeby przełamać ograniczenia wynikające z niej dla skuteczności postępowania karnego. W opracowaniu zaprezentowano obowiązujące obecnie rozwiązania, takie jak międzynarodowa pomoc prawna, dobrowolna współpraca, próby rozszerzenia jurysdykcji krajowej i europejski nakaz dochodzeniowy, oraz przeanalizowano ich mankamenty. Odpowiedzią na niedostatki tych rozwiązań ma być przyjęty w lipcu 2023 r. europejski nakaz wydania dowodów elektronicznych, który w ciągu

---

[2] J. Daskal, *A New UK-US Data Sharing Agreement: A Tremendous Opportunity, If Done Right*, justsecurity.org, February 2016, https://www.justsecurity.org/29203/british-searches-america-tremendous-opportunity/ [dostęp: 24.07.2023].

[3] Commission Staff Working Document, Impact Assessment, Accompanying the document 'Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings' (Brussels, 17.4.2018 SWD (2018) 118 final) 23.

najbliższych trzech lat stanie się kluczowym instrumentem transgranicznego uzyskania dowodów elektronicznych. Zostanie on tu poddany bardziej szczegółowej krytycznej analizie.

1. Zbieranie dowodów elektronicznych w zderzeniu z zasadą terytorialności – niepraktyczność międzynarodowej pomocy prawnej

Konieczność sprawnego dostępu do dowodów elektronicznych na potrzeby postępowania karnego wydaje się dziś niekwestionowana i postępujący rozwój technologii – takich jak Internet rzeczy czy światy wirtualne (*metaverse*) – będą tę potrzebę jedynie zwiększać. Mamy do czynienia z sytuacją bez precedensu. Tradycyjna poczta nie rejestrowała całości korespondencji, jaka przechodziła przez jej ręce. Nie posiadała też dostępu do treści listów, które przesyłała. Otwarcie korespondencji wymagało użycia specjalnych instrumentów procesowych. Obecna komunikacja odbywająca się przy pomocy narzędzi elektronicznych zakłada, choćby z przyczyn biznesowych, dostęp do danych, jakie są przesyłane, i ich rejestrację, czy mówimy o metadanych (np. kto do kogo wysłał wiadomość, kiedy, skąd i dokąd), czy o samej treści korespondencji. Dane te to naturalnie prawdziwy skarb dla organów ścigania, a fakt, że są w posiadaniu osób trzecich, czyli dostarczycieli usług, jest prawdziwym błogosławieństwem, gdyż dostęp do nich nie jest ograniczony przez zasady procesowe, jak choćby przywilej *nemo tenetur*.

Ograniczeniem w dostępie do tych danych powinna być głównie troska o prawo do prywatności. Jednak, jak się okazuje, dostępu do tego skarbu nie broni prawo, a zasada terytorialności.

Zgodnie z tą zasadą, wyrażoną w wyroku Stałego Trybunału Sprawiedliwości Międzynarodowej w sprawie Lotus[4], jurysdykcja do egzekwowania prawa jest ograniczona ściśle do terytorium państwa. Innymi słowy, organy ścigania nie mogą podejmować żadnych działań poza fizycznymi granicami własnego kraju. Ograniczenie to koliduje z naturą cyberprzestrzeni i Internetu, które takich fizycznych granic nie znają, a dane przepływają swobodnie po (niemal)[5] całym świecie[6]. W rezultacie organy ścigania mają do czynienia ze stosunkowo prostymi sprawami (np. krajowymi, w których ofiary i sprawcy są mieszkańcami tego kraju, w którym również miało miejsce przedmiotowe przestępstwo i którego organy prowadzą postępowanie), w których niezbędne są dowody elektroniczne znajdujące się w rękach usługodawcy podlegającego obowiązkom innego kraju i potencjalnie na serwerach w ramach centrum danych zlokalizowanym

4 S.S. Lotus (Fr. *v.* Turk.), 1927 P.C.I.J. (ser. A) No. 10 (Sept. 7).

5 Wyjątek należy tu uczynić dla krajów ograniczających swobodę korzystania z cyberprzestrzeni.

6 W tym zakresie szczególnie zob. analizę: U. Sieber, C.-W. Neubert, *Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty* [w:] *Max Planck Yearbook of United Nations Law*, vol. 20 (2016), eds. F. Lachenmann, T.J. Röder, R. Wolfrum, Leiden 2017, s. 241–321.

w jeszcze innym kraju. Co więcej, niektórzy dostawcy usług, jak np. Google, nie umieszczają danych na statycznym serwerze, lecz krążą one pomiędzy centrami danych, stąd jeden mail może być podzielony na kilka fragmentów pozostających w danym momencie w kilku różnych krajach[7]. Zjawisko to znane jako utrata lokalizacji (*loss of location*) dodatkowo komplikuje zadanie organów ścigania[8].

Z zasady terytorialności wynika, że za każdym razem, gdy organy ścigania potrzebują dowodów elektronicznych w powyżej opisanych sytuacjach transgranicznych, aby nie naruszać suwerenności kraju usługodawcy bądź kraju, gdzie dane się znajdują, muszą posłużyć się one instrumentami współpracy międzynarodowej bądź transgranicznej. W ramach Unii Europejskiej od 2017 r. podstawowym instrumentem jest dyrektywa dotycząca europejskiego nakazu dochodzeniowego przyjęta w 2014 r., która zostanie omówiona bardziej szczegółowo poniżej[9]. Jednak częścią dyrektywy END nie jest Irlandia (oraz Dania, co ma mniejsze znaczenie), będąca siedzibą wielu istotnych usługodawców na potrzeby ich europejskiej aktywności (np. Google i Meta). W przypadku konieczności uzyskania danych z Irlandii właściwym instrumentem współpracy międzynarodowej jest Europejska konwencja o pomocy prawnej w sprawach karnych z 1959 r.[10] Jeżeli dane mają być uzyskane spoza Unii Europejskiej, traktaty o wzajemnej pomocy prawnej będą stanowiły podstawę zwrócenia się o nie, co jest kluczowe w szczególności, jeśli chodzi o dane będące w posiadaniu amerykańskich dostarczycieli usług.

Głównym mankamentem wzajemnej pomocy prawnej jest długi czas jej trwania[11]. Procedura ta trwa średnio 10 miesięcy[12]. Drugą poważną trudność stanowi amerykański standard dowodowy – tzw. *probable cause*, z którego wynika konieczność przekonania amerykańskiego sędziego, że dowód, jaki się chce uzyskać, prawdopodobnie przyczyni się do udowodnienia przestępstwa[13]. Wymóg ten, wynikający z czwartej

---

7 V. Krishnamurthy, *Cloudy with a Conflict of Laws: How Cloud Computing Has Disrupted the Mutual Legal Assistance Treaty System and Why It Matters*, Berkman Klein Center Research Publication No. 2016-3, https://ssrn.com/abstract=2733350 [dostęp: 24.07.2023].

8 J. Daskal, *The Un-Territoriality of Data*, „Yale Law Journal" 2015, vol. 125, no. 2, s. 365–375.

9 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).

10 Europejska konwencja o pomocy prawnej w sprawach karnych, sporządzona w Strasburgu dnia 20 kwietnia 1959 r. (Dz. U. z 1999 r. Nr 76, poz. 854).

11 Zob. również analizę dotyczącą mankamentów tej procedury: G. Kent, *The Mutual Legal Assistance Problem Explained*, The Center for Internet and Society, 23 February 2015, http://cyberlaw.stanford.edu/blog/2015/02/mutual-legal-assistance-problem-explained [dostęp: 24.07.2023].

12 R.A. Clarke, M.J. Morell, G.R. Stone, C.R. Sunstein, P. Swire, *Liberty and Security in a Changing World. Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies*, 12 December 2013, s. 227, https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf [dostęp: 24.07.2023]. Por. też krytykę tej analizy: G. González Fuster, S. Vázquez Maymir, *Cross-border Access to E-Evidence: Framing the Evidence*, CEPS Papers series, Brussels 2020, https://www.ceps.eu/wp-content/uploads/2020/03/LSE2020-02_Cross-border-Access-to-E-Evidence.pdf [dostęp: 24.07.2023].

13 Oświadczenie Jennifer Daskal na forum Committee on the Judiciary Subcommittee on Crime and Terrorism United States Senate. Hearing on Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights (May 10, 2017), s. 3.

poprawki do Konstytucji Stanów Zjednoczonych, jest przedmiotem obszernego orzecznictwa amerykańskiego[14], jednak nie jest znany europejskim sędziom, więc nierzadko zdarza się, że mają oni trudności z jego spełnieniem, co znacznie opóźnia procedurę[15]. Problem ten został już dostrzeżony przez Komisję Europejską, która przeznaczyła znaczne środki na szkolenie europejskich sędziów w tym zakresie[16]. Ze względu na wyżej opisaną uciążliwą procedurę angażującą różne organy obu państw uważa się ją za zbyt skomplikowaną i wymagającą zbyt dużych zasobów[17].

W rezultacie można było obserwować postępującą frustrację organów ścigania, wynikającą z konieczności zaangażowania nieproporcjonalnych środków do uzyskania danych na potrzeby dowodowe, gdzie komplikacja postępowania nie ma uzasadnienia, a meritum postępowania czy konieczności efektywnej ochrony praw osób, których dane te dotyczą, wynika z przypadkowej (z punktu widzenia przedmiotowego postępowania) lokalizacji dostarczyciela usług bądź danych. Dobrą ilustracją tej frustracji jest sprawa Microsoft Ireland, w której rząd USA domagał się na mocy prawa krajowego wydania danych przez Microsoft[18]. Firma odmówiła wydania danych, argumentując to tym, że dane były przechowywane w centrum danych w Dublinie, i zażądała wysłania wniosku o wzajemną pomoc prawną do Irlandii. Sąd Apelacyjny rozpoznający sprawę przyznał rację Microsoftowi[19], jednak rozstrzygnięcie to zostało zaskarżone do Sądu Najwyższego. Ten wprawdzie przeprowadził nawet posiedzenie w tym zakresie, jednak sprawa została ostatecznie umorzona ze względu na zmiany legislacyjne, które nastąpiły w międzyczasie.

Kluczową dla rozstrzygnięcia kwestią było pytanie, czy w sprawie miało miejsce eksterytorialne zastosowanie prawa amerykańskiego (tj. ustawy o przechowywanej komunikacji – Stored Communications Act), czy też sytuacja ta pod kątem stosowania prawa miała charakter *stricte* krajowy. Pierwsze spośród wskazanych wyżej stanowisk było prezentowane przez Microsoft, który argumentował na podstawie miejsca przechowywania danych, a więc przy zastosowaniu zasady terytorialności, wskazując, że wniosek złożony przez rząd amerykański wykraczał poza granice USA, ponieważ żądane dane były przechowywane za granicą. W swojej argumentacji rząd amerykański skupił się na możliwościach Microsoftu, by z terytorium USA pozyskiwać dostęp

---

[14] W.R. LaFave, *Search and Seizure: A Treatise on the Fourth Amendment*, 5th ed., St. Paul (oct. 2017 update), § 3.1 i nn.

[15] Technical Document: Measures to improve cross-border access to electronic evidence for criminal investigations following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace, s. 8–9, https://home-affairs.ec.europa.eu/system/files/2020-09/20170522_technical_document_electronic_evidence_en.pdf [dostęp: 24.07.2023].

[16] EU Commission Non-paper: Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward, s. 3, https://home-affairs.ec.europa.eu/system/files/2017-05/20170522_non-paper_electronic_evidence_en.pdf [dostęp: 24.07.2023].

[17] EU Commission, Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace, s. 5, http://data.consilium.europa.eu/doc/document/ST-15072-2016-REV-1/en/pdf [dostęp: 24.07.2023].

[18] United States v. Microsoft Corp., 584 U.S. ___, 138 S. Ct. 1186 (2018).

[19] Zob. pozew oraz rozstrzygnięcie Sądu Apelacyjnego dla Drugiego Okręgu: https://www.scotusblog.com/wp-content/uploads/2017/07/17-2-petition.pdf [dostęp: 25.07.2023].

i kontrolować dane. Wskazywał w ten sposób, iż sytuacja w istocie ma charakter krajowy w tym sensie, że Microsoft był w stanie pozyskać dostęp i kontrolować dane z terytorium USA, a zatem wydanie danych dokonywałoby się z terytorium tego kraju, co nadawało sprawie krajowy, a nie eksterytorialny charakter.

Ostatecznie problem ten rozwiązano poprzez zmianę legislacyjną (tym samym czyniąc wyrok Sądu Najwyższego zbędnym)[20]. Uchwalony w kwietniu 2018 r. tzw. CLOUD Act rozstrzygnął po myśli rządu amerykańskiego kwestię zasięgu działania amerykańskich organów ścigania w odniesieniu do danych przechowywanych przez amerykańskich dostawców poza terytorium Stanów Zjednoczonych. CLOUD Act jest również kluczowy dla sytuacji europejskich organów ścigania i w tym kontekście zostanie omówiony poniżej.

2. Alternatywy dla międzynarodowej pomocy prawnej

Innym przykładem frustracji organów ścigania, które zakończyły się próbami szukania rozwiązań poza międzynarodową pomocą prawną, są belgijskie sprawy dotyczące Yahoo[21] i Skype'a[22]. W pierwszej z tych spraw Yahoo odmówiło udostępnienia danych niedotyczących treści (danych subskrybentów, a także dynamicznych adresów IP oraz daty i godziny utworzenia kont)[23], o które zwróciły się belgijskie organy ścigania w sprawie *stricte* krajowej. Yahoo odmowę tę argumentowało faktem, iż będąc spółką amerykańską, nie może przekazać tych danych, i zwróciło się do władz belgijskich o skorzystanie z mechanizmu wzajemnej pomocy prawnej. Belgijski prokurator, zamiast wdrożyć sugerowaną przez Yahoo procedurę, zdecydował się oskarżyć spółkę o brak współpracy, co w ostateczności zaowocowało jej ukaraniem. Główna kwestia prawna dotyczyła tego, czy można uznać, że Yahoo powinno być traktowane jako podmiot belgijski i tym samym podlegać obowiązkom wynikającym z belgijskiego Kodeksu postępowania karnego. Podczas gdy usługodawca wskazywał na brak fizycznej obecności w kraju (tj. brak siedziby lub brak jakiejkolwiek infrastruktury), organy ścigania skupiły się na wirtualnej obecności wynikającej z kierowania usług do lokalnych klientów (np. używanie lokalnych języków, publikowanie lokalnych reklam)[24]. Sądy prowadzące postępowanie w tej sprawie, w tym Sąd Najwyższy, podzieliły stanowisko prokuratury[25].

Inna przełomowa sprawa, która znalazła podobny finał, dotyczyła Skype'a. Usługodawca ten, mający swoją siedzibę w Luksemburgu, również odmówił wydania żądanych danych (dotyczących ruchu i lokalizacji, ale co istotniejsze, również treści

---

20 J. Daskal, *Unpacking the CLOUD Act*, „eucrim" 2018, issue 4, s. 221.

21 Cour de cassation (Belgijski Sąd Najwyższy), wyrok z dnia 1 grudnia 2015 r., P.13.2082.N.

22 Cour de cassation (Belgijski Sąd Najwyższy), wyrok z dnia 19 lutego 2019 r., P.17.229.N.

23 V. Franssen, *The Belgian Internet Investigatory Powers Act – A Model to Pursue at European Level?*, „European Data Protection Law Review" 2017, vol. 3, issue 4, s. 538.

24 *Ibidem*, s. 538–539.

25 Cass. 18 January 2017, No P.10.1347/N, cyt. za: *ibidem*, s. 538.

komunikacji prowadzonej na żywo), powołując się na brak fizycznej obecności spółki na terytorium Belgii. Odmowa ta skutkowała nałożeniem na Skype'a grzywny za brak współpracy w toku prowadzonego postępowania, która została utrzymana na etapie apelacji[26]. Rozstrzygnięcie, jakie przyjęto w tej sprawie, potwierdziło podejście użyte wobec Yahoo. Tym samym zastosowano to samo rozwiązanie na gruncie wewnątrzunijnym co w sprawie transatlantyckiej. Ponadto belgijski ustawodawca przyjął niniejsze podejście wypracowane w orzecznictwie, włączając je do przepisów belgijskiego Kodeksu postępowania karnego i nakładając obowiązki współpracy na usługodawców bez względu na brak ich fizycznej obecności w Belgii[27].

Z omawianym rozwiązaniem wiążą się co najmniej trzy problemy. Po pierwsze, eksterytorialne stosowanie prawa krajowego budzi wątpliwości w świetle standardów prawa międzynarodowego. Co więcej, o ile można uznać takie rozwiązanie za uzasadnione w sprawach czysto krajowych (jak w przypadku Yahoo i Skype'a), to biorąc również pod uwagę ochronę zapewnianą przez krajową procedurę karną, nic nie stałoby na przeszkodzie zastosowania tego podejścia w sytuacjach, w których lokalne powiązanie byłoby mniej oczywiste[28]. Rezultat ten mógłby być również mniej niż zadowalający, gdyby podejście to było stosowane przez kraje o niskim standardzie ochrony praw człowieka. Po drugie, egzekwowanie takiego rozwiązania mogłoby doprowadzić do swoistej bitwy na skuteczność między organami ścigania różnych krajów (kto przestraszy usługodawcę bardziej), co również należy uznać za skutek wysoce niepożądany. Po trzecie, konsekwencją dwóch poprzednich argumentów jest to, że takie podejście okazało się bardzo uciążliwe dla środowiska biznesowego, ponieważ zrodziło niepewność w zakresie obowiązujących zasad i sprzecznych obowiązków. Z tych powodów to właśnie rozstrzygnięcia we wspomnianych belgijskich sprawach dotyczących Yahoo i Skype'a unaoczniły w skali międzynarodowej problematykę dostępu do dowodów elektronicznych i doprowadziły do rozpoczęcia prac nad rozwiązaniem, jakim są przyjęte w lipcu 2023 r. rozporządzenie i dyrektywa w sprawie dostępu do dowodów elektronicznych. Zanim to się jednak stało, organy ścigania szukały innych – bardziej pragmatycznych – sposobów na uzyskanie danych na potrzeby postępowań karnych.

Takim rozwiązaniem, które znalazło zastosowanie w praktyce, jest bezpośrednia dobrowolna współpraca usługodawców z organami ścigania[29]. Polega ona na wysyłaniu przez organy żądań bezpośrednio do dostawców usług zlokalizowanych za granicą i poleganiu na ich dobrej woli w zakresie dostarczania danych na potrzeby prowadzonego postępowania[30].

---

[26] *Ibidem*, s. 539.

[27] *Ibidem*, s. 539–540.

[28] *Ibidem*, s. 539.

[29] EU Commission Non-paper: Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward s. 1 i 3–4; EU Commission, Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace, s. 4.

[30] Według badania przeprowadzonego przez Komisję Europejską siedem państw członkowskich uważa takie wnioski za obowiązkowe – EU Commission, Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace, s. 4.

W szczególności amerykańscy usługodawcy, zgodnie z ustawą o prywatności w komunikacji elektronicznej (Electronic Communication and Privacy Act) z 1986 r., mogą dobrowolnie dostarczać zagranicznym organom ścigania dane, pod warunkiem, że nie dotyczą one treści. Sytuacja jest odmienna w odniesieniu do danych dotyczących treści, które ze względu na tzw. przepis blokujący nie mogą być dostarczane przez amerykańskich usługodawców zagranicznym organom ścigania[31]. W konsekwencji wnioski o udostępnienie danych niedotyczących treści mogą być wysyłane, a odpowiedzi na nie udzielane bez uciekania się do mechanizmów wzajemnej pomocy prawnej, a tym samym bez angażowania amerykańskich organów sądowych.

O ile współpraca ta zapewnia większą elastyczność i pozwala na ominięcie problemów związanych z mechanizmem wzajemnej pomocy prawnej, o tyle budzi wątpliwości co do ochrony praw osób, których dotyczy, z powodu braku jasnych ram prawnych. Poza tym, po stronie usługodawców trudność polega na ocenie autentyczności wniosków oraz ich legalności[32]. Wreszcie mogą się pojawić problemy z dopuszczalnością w postępowaniu karnym dowodów zebranych w taki właśnie sposób[33].

3. Europejski nakaz dochodzeniowy

W ramach Unii Europejskiej głównym instrumentem transgranicznej współpracy w sprawie zbierania dowodów wszelkiego rodzaju jest obecnie europejski nakaz dochodzeniowy. Przyjęty w 2014 r. z trzyletnim okresem na implementację do porządków krajowych END ma na celu znaczne usprawnienie transgranicznej wymiany dowodów poprzez bazowanie na zasadzie wzajemnego uznawania i zapewnienie znacznie krótszych w porównaniu z międzynarodową pomocą prawną terminów na zaakceptowanie i wykonanie nakazu.

Instrument ten może również służyć do ułatwienia pozyskiwania danych przechowywanych przez firmy w państwie członkowskim innym niż miejsce prowadzonego postępowania. Jednak uważa się, że END nie jest idealnym instrumentem do uzyskania danych elektronicznych[34]. Krytycy podkreślają, że przy jego przygotowywaniu nie wzięto pod uwagę realiów gromadzenia dowodów cyfrowych. W treści nakazu nie wspomina się o zbieraniu tego rodzaju dowodów, a jego rozwiązania ukierunkowane są na gromadzenie „dowodów ze świata rzeczywistego", danych finansowych bądź bankowych lub na przechwytywanie komunikacji prowadzonej „na żywo".

Aspekt ten uwidacznia się przede wszystkim w tym, że europejski nakaz dochodzeniowy nie uwzględnia bezpośredniej współpracy między organami ścigania a dostawcami usług. Europejski nakaz dochodzeniowy opiera się na wzajemnym uznawaniu i w praktyce działa w taki sam sposób, jak inne przewidziane w Unii Europejskiej

31 18 U.S.C. §§ 2702; *ibidem*, s. 6.
32 *Ibidem*, s. 9.
33 *Ibidem*, s. 5 i 10.
34 Commission Staff Working Document, Impact Assessment…, s. 23.

instrumenty wzajemnego uznawania – np. europejski nakaz aresztowania. W tym przypadku procedura wymaga kontaktu między organami sądowymi i tylko właściwy organ państwa wykonującego może nakazać dostawcy usług internetowych dostarczenie danych[35].

Ponadto, pomimo że END skraca czas uzyskania dowodów w ramach współpracy transgranicznej, to jednak terminy, jakie przewiduje, są wciąż za długie jak na realia cyberprzestrzeni ze względu na ryzyko zmodyfikowania lub utracenia danych. Termin 90 dni przewidziany na wykonanie nakazu jest rzeczywiście dość długi, a ponadto jest poprzedzany terminem 30-dniowym na podjęcie decyzji w zakresie uznania lub wykonania nakazu (art. 12 ust. 3 i 4 dyrektywy END)[36]. Trzeba jednak zaznaczyć, że inicjatywa w sprawie pakietu legislacyjnego dotyczącego dowodów elektronicznych została wydana zaledwie rok po upływie terminu na implementację END. Nie miał więc on szansy zaistnieć jako podstawowy instrument transgranicznego uzyskiwania dowodów, a tym samym potwierdzić lub obalić powyższą krytykę.

Innym problemem jest to, że w END nie uczestniczy Irlandia, co do której właściwym instrumentem, jak już wspomniano, jest Europejska konwencja o pomocy prawnej w sprawach karnych z 1959 r.[37] Ze względu na wagę Irlandii na mapie dostarczycieli usług funkcjonujących w ramach Unii Europejskiej niemożność skorzystania w tym przypadku z END jest dużym mankamentem. Europejski nakaz dochodzeniowy nie oferuje również żadnego rozwiązania w kwestii dopuszczalności wydania dowodów przez usługodawców amerykańskich ograniczonych przepisem blokującym.

4. Europejski nakaz wydania oraz zabezpieczenia dowodów

Sposobem na rozwiązanie obu problemów – dostępu do dowodów elektronicznych w ramach UE i odblokowania możliwości współpracy przez amerykańskich usługodawców – jest przyjęty w lipcu 2023 r. tzw. pakiet w sprawie dowodów elektronicznych (*E-evidence Package*) składający się z rozporządzenia w sprawie europejskiego nakazu wydania oraz zabezpieczenia dowodów i towarzyszącej mu dyrektywy.

---

[35] Warto zwrócić uwagę na terminologię w języku angielskim – w nakazie nie użyto znanych z dyrektywy END wyrażeń: *executing State* i *executing authority* (po polsku odpowiednio: „państwo wykonujące" i „organ wykonujący"), lecz *enforcing State* i *enforcing authority*, zwracając uwagę, że rolą tego drugiego państwa nie jest wykonanie nakazu, lecz przymuszenie usługodawcy, żeby mu się poddał. To rozróżnienie tylko częściowo oddało polskie tłumaczenie 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) (dalej: rozporządzenie 2023/1543), które posługuje się wyrażeniami: „państwo wykonujące" i „organ przymuszający do wykonania nakazu".

[36] Szerzej na temat europejskiego nakazu dochodzeniowego oraz jego mankamentów zob. M. Kusak, *Europejski nakaz dochodzeniowy – przełom w dziedzinie europejskiego ścigania karnego?*, RPEiS 2012, t. 74, z. 4, s. 93–105.

[37] Zob. https://www.gov.ie/en/policy-information/e5f87-mutual-legal-assistance/ [dostęp: 25.07.2023].

Akty te przyjęto po bardzo długim procesie legislacyjnym, w trakcie którego pojawiły się różne wersje tekstu. W tym zakresie warto wyróżnić szczególnie stanowisko Parlamentu Europejskiego znacznie odbiegające od pierwotnej treści wniosku Komisji Europejskiej[38]. Intensywna debata co do tej propozycji dotyczyła kluczowych pytań, spośród których jedynie przykładowo można wskazać samą potrzebę niniejszej regulacji, a także te odnoszące się do fundamentalnych kwestii dotyczących prywatności[39], charakteru i przyszłości transgranicznej współpracy w sprawach karnych[40] oraz roli podmiotów prywatnych w egzekwowaniu prawa[41]. Kilka prezydencji podjęło wysiłki w celu znalezienia kompromisu podczas przedłużającego się okresu impasu[42]. Obserwatorom wydawało się nawet, że pakiet nie zostanie nigdy przyjęty. Jednak potrzeba stworzenia nowych ram prawnych wzięła górę, a ostateczna wersja tekstu rozporządzenia nie odbiega zasadniczo od treści wniosku przedstawionego przez Komisję w kwietniu 2018 r.

Celem tych dwóch powiązanych ze sobą aktów prawnych jest zapewnienie skutecznego i szybkiego instrumentu dostępu do danych elektronicznych w ramach UE oraz rozwiązanie problemu wynikającego z amerykańskiego przepisu blokującego. Osiągnięcie tego drugiego celu jest możliwe dzięki wspomnianemu CLOUD Act[43].

---

38 Komisja Europejska, Wniosek z dnia 17 kwietnia 2018 r. odnośnie do Rozporządzenia Parlamentu Europejskiego i Rady 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, COM(2018) 225 final, 2018/0108 (COD) oraz Komisja Europejska, Wniosek z dnia 17 kwietnia 2018 r. odnośnie do Dyrektywy Parlamentu Europejskiego ustanawiającej zharmonizowane przepisy dotyczące mianowania przedstawicieli prawnych w celu gromadzenia dowodów na potrzeby postępowań karnych, COM(2018) 226 final, 2018/0107 (COD); Sprawozdanie Parlamentu Europejskiego odnośnie do 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, 11.12.2020, COM(2018)0225; Raport w sprawie wniosku odnośnie do Dyrektywy Parlamentu Europejskiego ustanawiającej zharmonizowane przepisy dotyczące mianowania przedstawicieli prawnych w celu gromadzenia dowodów na potrzeby postępowań karnych, 11.12.2020, COM(2018)0226.

39 G. González Fuster, S. Vázquez Maymir, *Cross-border Access to E-Evidence…*; M. Corhay, *Private Life, Personal Data Protection and the Role of Service Providers: The EU e-Evidence Proposal*, „European Papers" 2021, vol. 6, no. 1, s. 441–471.

40 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, issue 2, s. 161–183; K. Ligeti, G. Robinson, *Sword, Shield and Cloud: Toward a European System of Public-Private Orders for Electronic Evidence in Criminal Matters?* [w:] *Surveillance and Privacy in the Digital Age: European, Transatlantic and Global Perspectives*, eds. V. Mitsilegas, N. Vavoula, Oxford–New York 2021, s. 27–70.

41 S. Tosza, *Internet service providers as law enforcers and adjudicators. A public role of private actors*, „Computer Law & Security Review" 2021, vol. 43, s. 1–17; V. Mitsilegas, *The Privatisation of Mutual Trust in Europe's Area of Criminal Justice: The Case of E-evidence*, „Maastricht Journal of European and Comparative Law" 2018, vol. 25, issue 3, s. 263–265.

42 Zob. np. starania prezydencji francuskiej z dnia 16 czerwca 2022 r.: Nota prezydencji (Council doc. 10271/22, LIMITE, 16 June 2022), https://data.consilium.europa.eu/doc/document/ST-10271-2022-INIT/en/pdf [dostęp: 25.06.2023].

43 M. Rojszczak, *CLOUD act agreements from an EU perspective*, „Computer Law & Security Review" 2020, vol. 3.

Umożliwia on zniesienie obowiązywania przepisu blokującego, ale pod warunkiem podpisania ze Stanami Zjednoczonymi porozumienia międzyrządowego. Takie porozumienia USA podpisało już z Wielką Brytanią i Australią[44]. Ponieważ kwestia dostępu do e-dowodów była problemem krajowym, istniało ryzyko, że USA będą negocjować z każdym z państw członkowskich UE z osobna. Byłoby to nie tylko bardzo czasochłonne, ale też stworzyłoby ryzyko, że tak wynegocjowane umowy będą się od siebie różnić co do szczegółów, tym samym dodatkowo komplikując pejzaż reguł rządzących uzyskiwaniem dowodów elektronicznych w UE[45]. Uchwalenie pakietu w sprawie dowodów elektronicznych zapobiega temu ryzyku. Oznacza bowiem, że to UE będzie negocjować jedno porozumienie i będzie ono jednakowe w ramach całej przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Negocjacje z USA rozpoczęte już w czerwcu 2019 r. uległy zamrożeniu na czas przedłużających się prac legislacyjnych dotyczących pakietu. Kiedy jednak stało się jasne, że jego ostateczny kształt został uzgodniony zimą 2023 r., natychmiast je odmrożono[46].

Pakiet legislacyjny w zakresie dowodów elektronicznych składa się z dwóch instrumentów: przywołanego już wcześniej rozporządzenia 2023/1543 oraz dyrektywy[47].

Dyrektywa 2023/1544 ustanawiająca zharmonizowane przepisy dotyczące mianowania przedstawicieli prawnych w celu gromadzenia dowodów na potrzeby postępowań karnych odgrywa w tym tandemie rolę pomocniczą. Jej celem jest zapewnienie, aby dla każdego usługodawcy, którego dotyczy zakres obowiązków opisanych w rozporządzeniu, istniał co najmniej jeden potencjalny adresat europejskiego nakazu wydania lub zabezpieczenia dowodów. Dyrektywa 2023/1544 jest więc warunkiem *sine qua non* (choć nie jedynym) skuteczności nowego systemu. Usługodawcy mający siedzibę w Unii Europejskiej muszą wyznaczyć co najmniej jeden zakład (czyli oddział), do którego należy kierować wnioski w tej kwestii. Ci, którzy nie mają siedziby w UE, muszą wyznaczyć co najmniej jednego przedstawiciela prawnego w Unii, odpowiedzialnego za odbieranie i wykonywanie decyzji i nakazów właściwych organów państw członkowskich wydanych w celu uzyskania dowodów (art. 3 dyrektywy 2023/1544). Państwa członkowskie będą zobowiązane zapewnić, aby dostawcy usług internetowych wyznaczyli właściwy oddział lub przedstawiciela w ciągu trzech lat od wejścia w życie tej dyrektywy. Bedą musiały również ustanowić przepisy wprowadzające sankcje dla

---

[44] Porozumienie z Wielką Brytanią: https://www.justice.gov/criminal-oia/cloud-act-agreement-between-governments-us-united-kingdom-great-britain-and-northern [dostęp: 25.06.2023]; porozumienie z Australią: https://www.homeaffairs.gov.au/nat-security/files/cloud-act-agreement-signed.pdf [dostęp: 25.06.2023].

[45] Bardziej szczegółowo o rozwiązaniach krajowych w tej kwestii zob. V. Franssen, S. Tosza, *Cambridge Handbook of Digital Evidence in Criminal Matters*, Cambridge 2023.

[46] Zob. https://commission.europa.eu/news/eu-us-announcement-resumption-negotiations-eu-us-agreement-facilitate-access-electronic-evidence-2023-03-02_en [dostęp: 25.06.2023].

[47] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2023/1544 z dnia 12 lipca 2023 r. w sprawie zharmonizowanych przepisów dotyczących wskazywania wyznaczonych zakładów i ustanawiania przedstawicieli prawnych w celu gromadzenia dowodów elektronicznych w postępowaniach karnych (Dz. Urz. UE L 191 z 28.07.2023, s. 181) (dalej: dyrektywa 2023/1544).

usługodawców nieprzestrzegających obowiązków przewidzianych w tym akcie prawnym (art. 5 dyrektywy 2023/1544).

Z kolei rozporządzenie 2023/1543 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 stanowi główny element tego duetu. To ono kreuje oba nakazy, określa zasady ich wydawania, przekazywania usługodawcom, ich wykonywania i wreszcie egzekwowania w razie odmowy wykonania.

Rozporządzenie 2023/1543 ustanawia dwa nakazy: europejski nakaz wydania dowodów elektronicznych, tj. danych posiadanych przez usługodawcę, które mogą służyć jako dowód w postępowaniu karnym, oraz europejski nakaz zabezpieczenia dowodów, który jest instrumentem szybkiego zamrażania takich dowodów. Europejski nakaz wydania oraz europejski nakaz zabezpieczenia dowodów mogą być stosowane „wyłącznie w ramach i do celów postępowania karnego", jak również w celu wykonania „kary pozbawienia wolności lub środka zabezpieczającego polegającego na pozbawieniu wolności w wymiarze co najmniej czterech miesięcy". Postępowania te mogą dotyczyć osób fizycznych lub prawnych, jeżeli w przypadku tych ostatnich krajowy porządek prawny przewiduje odpowiedzialność karną osób prawnych (art. 2 pkt 2 rozporządzenia 2023/1543). Ponadto nakazy te nie mogą być wykorzystywane wyłącznie w celu zapewnienia wzajemnej pomocy prawnej innemu państwu członkowskiemu lub państwu trzeciemu (art. 2 pkt 4 rozporządzenia 2023/1543).

Rozporządzenie to ma zastosowanie do usługodawców, którzy oferują usługi w Unii Europejskiej (art. 2 pkt 1). W art. 3 pkt 3 zawarto szczegółową definicję usług objętych zakresem rozporządzenia, którymi zgodnie z treścią tego przepisu są usługi łączności elektronicznej lub inne usługi społeczeństwa informacyjnego umożliwiające ich użytkownikom komunikację, usługi w zakresie nazw domen internetowych i numeracji IP lub usługi przechowywania lub przetwarzania danych. Usługodawcy świadczący te usługi nie muszą być fizycznie obecni w Unii Europejskiej (nie jest wymagane, aby mieli siedzibę lub centra danych w UE), by podlegać obowiązkom z rozporządzenia. Będą oni objęci zakresem pakietu legislacyjnego w zakresie dowodów elektronicznych, jeśli będą posiadać istotny związek z państwem członkowskim, w którym można korzystać z ich usług. Taki związek będzie określany na podstawie kryteriów faktycznych, np. „istnieje znaczna liczba użytkowników w co najmniej jednym państwie członkowskim lub gdy działalność jest ukierunkowana na co najmniej jedno państwo członkowskie" (art. 3 pkt 4b rozporządzenia 2023/1543).

Analizowane rozporządzenie ma zastosowanie do czterech rodzajów przechowywanych danych (komunikacja prowadzona na żywo jest wyłączona z jego zakresu), które można zebrać w dwie kategorie: z jednej strony „dane abonenta" oraz „dane, których zażądano wyłącznie w celu identyfikacji użytkownika", które postrzegane są za mniej inwazyjne, a z drugiej strony – „dane o ruchu" oraz „dane dotyczące treści" (art. 3 pkt 9–12 rozporządzenia 2023/1543). Kategoryzacja danych jest bezpośrednio związana z warunkami wydawania europejskich nakazów wydania dowodów oraz uprawnieniem organów do wydawania tych nakazów. Pierwsza kategoria danych może być

przedmiotem wniosku wydanego zarówno przez sędziego, sąd, sędziego śledczego (w krajach, gdzie taka instytucja istnieje), jak i prokuratora. Nakaz może być ponadto wydany przez każdy inny właściwy organ zgodnie z prawem krajowym, jednak wówczas wniosek ten musi zostać zatwierdzony przez jeden z organów wymienionych powyżej. Jeśli chodzi o dane o ruchu (ale nie takie, które należałyby do kategorii danych wymaganych wyłącznie w celu identyfikacji użytkownika) i dane dotyczące treści, to nakaz nie może być wydany samodzielnie przez prokuratora, lecz jedynie przez sędziego bądź sąd. Prokurator może wydać taki nakaz, jednak musi on następnie zostać zatwierdzony przez sędziego lub sąd (art. 4 rozporządzenia 2023/1543). Zakres europejskiego nakazu wydania dowodów dotyczących danych o ruchu lub danych dotyczących treści jest ograniczony do „przestępstw zagrożonych w państwie wydającym karą pozbawienia wolności o górnej granicy ustawowego zagrożenia w wysokości co najmniej trzech lat" oraz ponadto niektórych przestępstw wymienionych w art. 5 ust. 4 rozporządzenia 2023/1543. Ograniczenie to wyeliminuje niektóre przestępstwa z zakresu stosowania nakazów mających za przedmiot dane o ruchu i dane dotyczące treści, jednak prawdopodobnie nie ograniczy ich stosowania tylko do poważnych przestępstw, gdyż próg ten, zwłaszcza w odniesieniu do bardziej represyjnych systemów prawa karnego, jest stosunkowo niski.

Europejski nakaz zabezpieczenia dowodów, jako środek *per se* mniej inwazyjny, nie podlega takim ograniczeniom i może być wydawany w odniesieniu do każdego przestępstwa i przez wszystkie wymienione organy, w tym przez prokuratorów (art. 4 ust. 3 oraz art. 5 rozporządzenia 2023/1543). Może on zostać wydany nie tylko w związku z późniejszym europejskim nakazem wydania dowodów, ale także w związku z wnioskami o wydanie danych w ramach wzajemnej pomocy prawnej lub w ramach europejskiego nakazu dochodzeniowego (art. 6 ust. 2 rozporządzenia 2023/1543).

Wnioski są przekazywane usługodawcom w formie standardowych zaświadczeń zgodnie z załącznikami do rozporządzenia 2023/1543 (art. 9, Załączniki I i II). Po otrzymaniu zaświadczenia usługodawca powinien przede wszystkim szybko zabezpieczyć dane. W przypadku europejskiego nakazu wydania dowodów dane są przekazywane organowi wnioskującemu w ciągu 10 dni od otrzymania zaświadczenia, a w przypadkach nagłych w ciągu 8 godzin. Usługodawcy mogą odmówić wydania danych, powołując się tylko na ograniczony katalog powodów, głównie dlatego, że zaświadczenie „jest niekompletn[e], zawiera oczywiste błędy lub nie zawiera informacji wystarczających do jego wykonania" bądź z powodu faktycznej niemożności wydania danych wynikającej z okoliczności niezawinionych przez adresata. Usługodawcy są zobowiązani poinformować organ wydający, jeśli uznają, że nakaz mógłby „kolidować z przewidzianymi w prawie państwa wykonującego immunitetami lub przywilejami lub z przepisami dotyczącymi ustalania lub granic odpowiedzialności karnej związanymi z wolnością prasy lub wolnością wypowiedzi w innych mediach" (art. 11 ust. 4 rozporządzenia 2023/1543).

W sytuacji, gdy usługodawca zdecyduje się na odmowę wykonania wniosku, jest on zobowiązany udzielić odpowiedzi na formularzu znajdującym się w Załączniku III do rozporządzenia 2023/1543. Z treści Załącznika można wywnioskować, że dostawcy

usług mogą również kwestionować inne aspekty niż te wymienione w art. 11, a mianowicie, czy wniosek został wydany lub zatwierdzony przez właściwy organ, czy wniosek o udostępnienie danych o ruchu lub treści został wydany w związku z przestępstwami, do których ograniczony jest zakres możliwości wydania nakazu dotyczącego tego rodzaju danych, oraz czy usługa świadczona przez usługodawcę jest objęta zakresem europejskiego nakazu.

Rozporządzenie 2023/1543 przewiduje szczególną procedurę, gdy wniosek stawia usługodawcę w sytuacji sprzecznych obowiązków prawnych ze względu na obowiązujące prawo państwa trzeciego (art. 17). Usługodawca powinien zasygnalizować ten konflikt w formularzu zawartym w Załączniku III, a organ wydający nakaz musi zbadać przedstawioną sytuację. Pierwotna wersja tego przepisu według propozycji Komisji Europejskiej przewidywała procedurę dialogu między organami państwa wydającego a organami państwa trzeciego, której wynik zależał od odpowiedzi lub milczenia organów tego ostatniego (art. 15–16 rozporządzenia 2023/1543 w brzmieniu zaproponowanym przez Komisję). Nie wydawało się jednak wykonalne sformułowanie oczekiwania współpracy organów państwa trzeciego na podstawie rozporządzenia 2023/1543. Podobnie nie było sprawiedliwe uzależnianie losu usługodawcy od reakcji tego organu lub jej braku. Obecne rozwiązanie również nie jest idealne, ponieważ nie gwarantuje wyeliminowania konfliktu obowiązków, gdyż organ może utrzymać w mocy nakaz niezależnie od tego, że pozostaje on w konflikcie z zakazem w państwie trzecim. Artykuł 17 przewiduje natomiast procedurę badania tego konfliktu oraz kryteria, wedle których podejmowana powinna być decyzja o podtrzymaniu lub uchyleniu wniosku.

Od ogólnej zasady, iż organy państwa wykonującego nie są informowane o wniosku, przewidziany został jeden wyjątek. Mianowicie, jeżeli wniosek dotyczy danych o ruchu lub treści, powiadomienie organu wykonującego powinno zostać wysłane jednocześnie z zaświadczeniem skierowanym do usługodawcy. Na pierwszy rzut oka wydaje się, że jest to znaczący wyjątek od zasady bezpośredniej współpracy, jednak jego efekt będzie znacznie ograniczony przez zasadę wyłączającą z tego obowiązku sprawy krajowe, czyli takie, gdzie „a) przestępstwo zostało popełnione, jest popełniane lub istnieje prawdopodobieństwo jego popełnienia w państwie wydającym; oraz b) osoba, której dane są objęte nakazem, ma miejsce pobytu w państwie wydającym" – oraz przez fakt, iż to organ wydający jest uprawniony do oceny, czy zachodzą uzasadnione podstawy, by sądzić, że sprawa ma charakter krajowy (art. 8 ust. 2 rozporządzenia 2023/1543). Należy zauważyć, że to właśnie ten organ jest zainteresowany tym, aby dane zostały uzyskane bez dalszych komplikacji, które mogą zostać spowodowane przez takie powiadomienie.

W wyniku powiadomienia organ państwa wykonującego może w ciągu 10 dni (częściowo lub całkowicie) zablokować przekazanie danych lub ograniczyć ich wykorzystanie (art. 12 rozporządzenia 2023/1543) na podstawie enumeratywnie wskazanych kryteriów, takich jak: istnienie immunitetów lub przywilejów, zasada *ne bis in idem*, brak podwójnej karalności (z wyjątkiem przestępstw wymienionych w Załączniku IV do rozporządzenia 2023/1543) oraz – prawdopodobnie najważniejszego – oczywiste naruszenie istotnego prawa podstawowego wskazanego w art. 6 Traktatu o Unii

Europejskiej lub w Karcie praw podstawowych[48]. Ta podstawa odmowy może być przywołana tylko „w sytuacjach wyjątkowych". Wyrażenie to wydaje się wprowadzać problematyczną logikę, zakładającą, że jeśli naruszenie jest systematyczne, to wówczas ta podstawa odmowy nie może zostać wykorzystana (art. 12 ust. 1 rozporządzenia 2023/1543).

Elementem dodanym stosunkowo późno w trakcie negocjacji jest tzw. zdecentralizowany system teleinformatyczny, za pośrednictwem którego ze względów bezpieczeństwa ma się odbywać cała komunikacja i wymiana danych między organami a dostawcami usług (art. 19–26 rozporządzenia 2023/1543). W tym celu państwa członkowskie mogą zaoferować krajowy system informatyczny. Mogą się również zdecydować na zastosowanie systemu stworzonego na te potrzeby przez Komisję Europejską, który będzie przez nią utrzymywany i rozwijany (art. 22 rozporządzenia 2023/1543).

Odmowa wydania danych przez usługodawcę będącego adresatem wniosku powoduje wszczęcie postępowania przymuszającego, które przekształca nakaz w „klasyczny" instrument wzajemnego uznawania: organ wydający może zwrócić się do organu państwa członkowskiego usługodawcy (zwanego w tym kontekście organem przymuszającym) o wykonanie nakazu[49]. W takim przypadku organ przymuszający będzie miał do dyspozycji podstawy odmowy, które dotyczą ważności wydania nakazu, immunitetów i przywilejów, niemożności wykonania oraz względów dotyczących praw podstawowych sformułowanych w ten sam sposób, jak w przypadku procedury powiadamiania (art. 16 rozporządzenia 2023/1543). W celu przymuszenia usługodawcy, który nie spełnia nałożonych przez nakaz obowiązków, będzie można zastosować kary pieniężne. Jednak analizowane rozporządzenie nie wyznacza precyzyjnie ich wysokości, to państwa członkowskie muszą określić ich poziom w prawie krajowym. Treść rozporządzenia 2023/1543 w tej kwestii ogranicza się do żądania, aby wśród dostępnych sankcji znalazła się kara pieniężna „o wysokości nieprzekraczającej 2% całkowitego światowego rocznego obrotu usługodawcy w poprzednim roku obrotowym" (art. 15 ust. 1).

Rozporządzenie 2023/1543 przewiduje też w art. 18 podstawowe reguły dotyczące środków prawnych dostępnych osobom, których dane są objęte europejskim nakazem wydania dowodów. Jednak szczegółowe reguły odnośnie do dochodzenia tych praw będą wynikać z praw krajów członkowskich. Tym samym w tym aspekcie rozporządzenie to również wymaga dostosowania prawa krajowego.

---

[48] Traktat o Unii Europejskiej (wersja skonsolidowana) (Dz. Urz. UE C 202 z 7.06.2016, s. 1); Karta praw podstawowych Unii Europejskiej (wersja skonsolidowana) (Dz. Urz. UE C 202 z 7.06.2016, s. 1).

[49] O problemach z rozumieniem zasady wzajemnego uznawania w kontekście europejskich nakazów wydania dowodów zob. S. Tosza, *Mutual Recognition by Private Actors in Criminal Justice? Service Providers as Gatekeepers of Data and Human Rights Obligations*, September 19, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3517878 [dostęp: 25.06.2023].

Uwagi końcowe

Skuteczność europejskiego nakazu wydania dowodów elektronicznych będzie uzależniona od kilku czynników, których ostateczny kształt wciąż pozostaje otwarty. Niektóre z nich są nieodłącznie związane z pakietem legislacyjnym w zakresie dowodów elektronicznych. Są to w szczególności system sankcji (i praktyka ich nakładania) wobec dostawców usług nieprzestrzegających przepisów, a także skuteczność środków prawnych służących ochronie praw osób, których dane zostały objęte nakazem. Rozporządzenie 2023/1543 będzie stosowane dopiero od sierpnia 2026 r. Ten trzyletni okres przewidziany jest na dostosowanie porządków krajowych i stworzenie systemu teleinformatycznego. Kluczowy wpływ na nowy system będą miały również czynniki zewnętrzne w stosunku do tych przepisów. Najważniejszą kwestią w tym zakresie jest powodzenie negocjacji z USA w celu zniesienia przepisu blokującego zgodnie z CLOUD Act.

Rozporządzenie 2023/1543 nie porusza szeregu zagadnień istotnych dla zbierania danych elektronicznych, takich jak retencja danych, problem szyfrowania, czy wreszcie kwestii dopuszczalności dowodów uzyskanych transgranicznie od podmiotów prywatnych. Będą one jednak miały kluczowe znaczenie dla możliwości pozyskiwania i wykorzystywania danych jako dowodów. Co do problemu dopuszczalności dowodów grupa naukowców skupiona wokół Europejskiego Instytutu Prawa w Wiedniu sformułowała propozycję harmonizacji przepisów dotyczących dopuszczalności dowodów, ale to, czy Komisja Europejska zaproponuje przepisy w tym obszarze, pozostaje niejasne[50].

Ponadto należy wspomnieć o instrumencie, który był przygotowywany równolegle z pakietem w zakresie dowodów elektronicznych – jest nim Drugi protokół dodatkowy do konwencji budapesztańskiej o cyberprzestępczości[51]. Jego art. 6 i 7 również przewidują międzynarodową bezpośrednią współpracę między organami ścigania a dostawcami usług, jednak możliwości oferowane przez Protokół ograniczają się tylko do informacji o rejestracji nazw domen i informacji o abonentach. W tym sensie rozporządzenie 2023/1543 idzie o wiele dalej i w ramach UE Drugi protokół nie będzie stanowił dla niego większej konkurencji. Może on jednak mieć znacznie bardziej globalny wpływ, jeśli, podobnie jak to się stało w przypadku samej Konwencji, zostanie on ratyfikowany przez znaczącą liczbę państw również spoza Europy.

---

[50] Zob. Propozycja Europejskiego Instytutu Prawa dotycząca Dyrektywy Parlamentu Europejskiego i Rady w sprawie wzajemnego dopuszczania dowodów oraz dowodów elektronicznych w postępowaniu karnym (ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings, 2023), https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Proposal_for_a_Directive_on_Mutual_Admissibility_of_Evidence_and_Electronic_Evidence_in_Criminal_Proceedings_in_the_EU.pdf [dostęp: 26.07.2023].

[51] Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz. U. z 2005 r., poz. 728); 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).

Jeśli chodzi o kluczowe aspekty pakietu w zakresie dowodów elektronicznych, to można się spodziewać sporów sądowych. Już podczas debat prowadzących do jego przyjęcia kwestionowano wykorzystaną podstawę prawną pakietu[52]. Nie będzie więc zaskoczeniem, jeśli Trybunał Sprawiedliwości Unii Europejskiej zostanie zaangażowany do oceny jego ważności.

Ważnym pytaniem jest również to, jaki wpływ będzie mieć pojawienie się ułatwionego sposobu uzyskiwania dowodów elektronicznych na wykorzystanie dowodów w postępowaniach karnych w ogóle. W tym sensie istotne będzie, czy organy ścigania będą coraz chętniej korzystać z możliwości uzyskiwania dowodów elektronicznych od usługodawców kosztem innych dostępnych metod. Innym zagadnieniem o fundamentalnym znaczeniu dla współpracy ponadnarodowej w sprawach karnych, a w szczególności dla rozumienia zasady wzajemnego uznawania jest kwestia, czy ten model bezpośredniej współpracy zostanie rozszerzony na inne sposoby zbierania dowodów, np. te dotyczące komunikacji na żywo[53].

Literatura

Clarke R.A., Morell M.J., Stone G.R., Sunstein C.R., Swire P., *Liberty and Security in a Changing World. Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies*, 12 December 2013, https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

Corhay M., *Private Life, Personal Data Protection and the Role of Service Providers: The EU e-Evidence Proposal*, „European Papers" 2021, vol 6, no. 1.

Daskal J., *A New UK-US Data Sharing Agreement: A Tremendous Opportunity, If Done Right*, justsecurity.org, February 2016, https://www.justsecurity.org/29203/british-searches-america-tremendous-opportunity/.

Daskal J., *The Un-Territoriality of Data*, „Yale Law Journal" 2015, vol. 125, no. 2.

Daskal J., *Unpacking the CLOUD Act*, „eucrim" 2018, issue 4.

Franssen V., *The Belgian Internet Investigatory Powers Act – A Model to Pursue at European Level?*, „European Data Protection Law Review" 2017, vol. 3, issue 4.

Franssen V., Tosza S., *Cambridge Handbook of Digital Evidence in Criminal Matters*, Cambridge 2023.

González Fuster G., Vázquez Maymir S., *Cross-border Access to E-Evidence: Framing the Evidence*, CEPS Papers series, Brussels 2020, https://www.ceps.eu/wp-content/uploads/2020/03/LSE2020-02_Cross-border-Access-to-E-Evidence.pdf.

Kent G., *The Mutual Legal Assistance Problem Explained*, The Center for Internet and Society, 23 February 2015, http://cyberlaw.stanford.edu/blog/2015/02/mutual-legal-assistance-problem-explained.

[52] Szerzej na temat podstawy prawnej pakietu zob. S. Tosza, *Mutual Recognition by Private Actors in Criminal Justice? E-Evidence Regulation and Service Providers as the New Guardians of Fundamental Rights*, „Common Market Law Review" 2023, vol. 61, s. 1–28.

[53] S. Tosza, *All evidence is equal…*, s. 181–182.

Krishnamurthy V., *Cloudy with a Conflict of Laws: How Cloud Computing Has Disrupted the Mutual Legal Assistance Treaty System and Why It Matters*, Berkman Klein Center Research Publication No. 2016-3, https://ssrn.com/abstract=2733350.

Kusak M., *Europejski nakaz dochodzeniowy – przełom w dziedzinie europejskiego ścigania karnego?*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2012, t. 74, z. 4.

LaFave W.R., *Search and Seizure: A Treatise on the Fourth Amendment*, 5th ed., St. Paul (oct. 2017 update).

Ligeti K., Robinson G., *Sword, Shield and Cloud: Toward a European System of Public-Private Orders for Electronic Evidence in Criminal Matters?* [w:] *Surveillance and Privacy in the Digital Age: European, Transatlantic and Global Perspectives*, eds. V. Mitsilegas, N. Vavoula, Oxford–New York 2021.

Mitsilegas V., *The Privatisation of Mutual Trust in Europe's Area of Criminal Justice: The Case of E-evidence*, „Maastricht Journal of European and Comparative Law" 2018, vol. 25, issue 3.

Rojszczak M., *CLOUD act agreements from an EU perspective*, „Computer Law & Security Review" 2020, vol. 3.

Sieber U., Neubert C.-W., *Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty* [w:] *Max Planck Yearbook of United Nations Law*, vol. 20 (2016), eds. F. Lachenmann, T.J. Röder, R. Wolfrum, Leiden 2017.

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, issue 2.

Tosza S., *Cross-Border Gathering of Electronic Evidence: Mutual Legal Assistance, Its Shortcomings and Remedies* [w:] *Société numérique et droit pénal: Belgique, France, Europe*, sous la direction de V. Franssen, D. Flore, Bruxelles 2019.

Tosza S., *Internet service providers as law enforcers and adjudicators. A public role of private actors*, „Computer Law & Security Review" 2021, vol. 43.

Tosza S., *Mutual Recognition by Private Actors in Criminal Justice? E-Evidence Regulation and Service Providers as the New Guardians of Fundamental Rights*, „Common Market Law Review" 2023, vol. 61.

Tosza S., *Mutual Recognition by Private Actors in Criminal Justice? Service Providers as Gatekeepers of Data and Human Rights Obligations*, September 19, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3517878.

Tosza S., *The E-Evidence Package is Adopted: End of a Saga or Beginning of a New One?*, „European Data Protection Law Review" 2023, no. 2.

Streszczenie

Stanisław Tosza

W poszukiwaniu dowodów elektronicznych – europejski nakaz wydania dowodów elektronicznych oraz inne narzędzia międzynarodowego pozyskiwania danych dla potrzeb postępowania karnego

W lipcu 2023 r., po ponad pięcioletnich negocjacjach przyjęto rozporządzenie w sprawie europejskich nakazów wydania i europejskich nakazów zabezpieczenia dowodów elektronicznych. Rozporządzenie to wprowadza nowy paradygmat współpracy europejskiej w sprawach karnych

pozwalający na bezpośrednie wiążące żądanie przez organ jednego państwa członkowskiego wydania danych przez usługodawcę w innym państwie członkowskim, co do zasady bez udziału organów tego ostatniego. Rozwiązanie to, niepozbawione kontrowersji, jest odpowiedzią na coraz bardziej palącą potrzebę efektywnych sposobów na zdobywanie danych elektronicznych na potrzeby postępowania karnego. Celem niniejszego artykułu jest przedstawienie, dlaczego zbieranie dowodów elektronicznych nastręcza wielu prawnych i praktycznych problemów, a także jak próbowano sobie z nimi radzić. Ponadto w opracowaniu przeanalizowano zapisy nowego rozporządzenia i omówiono jego najważniejsze konsekwencje.

Słowa kluczowe: dowody elektroniczne, postępowanie karne, europejska współpraca w sprawach karnych, dostarczyciele usług elektronicznych, zasada terytorialności, europejski nakaz dochodzeniowy, zasada wzajemnego uznawania.

Summary

Stanisław Tosza

In Search of Electronic Evidence – European Production Order and Other Instruments for International Obtaining of Data for Criminal Proceedings

In July 2023, after more than five years of negotiations, the EU adopted the Regulation on European Production Orders and European Preservation Orders for electronic evidence. The regulation introduces a new paradigm for European cooperation in criminal matters, allowing authorities in one Member State to issue a direct binding order to a service provider in another Member State to produce data, in principle without the involvement of the latter's authorities. This solution, not without controversy, responds to the increasingly pressing need for effective means of obtaining electronic data for criminal proceedings. The purpose of the article is to outline why the collection of electronic evidence poses several legal and practical problems, how they have been attempted to be dealt with and to analyse the new regulation and its key implications.

Keywords: electronic evidence, criminal proceedings, European cooperation in criminal matters, Internet service providers, principle of territoriality, European Investigation Order, principle of mutual recognition.