



Młody Jurysta

Pozyskiwanie danych informatycznych w postępowaniu karnym a elementy prawa do prywatności w europejskich systemach ochrony praw człowieka

Jonasz Szpoton¹

19–36

Streszczenie: Artykuł omawia problematykę dopuszczalności pozyskiwania danych informatycznych na potrzeby postępowania karnego w kontekście wybranych elementów prawa do prywatności. Przedstawia podstawowe zagadnienia związane z ochroną życia prywatnego, rodzinnego i korespondencji oraz jej ograniczenia w europejskich systemach ochrony praw człowieka. Autor dokonuje analizy wybranych wyroków Europejskiego Trybunału Praw Człowieka w Strasburgu dotyczących naruszeń w zakresie prawa do poszanowania życia prywatnego, rodzinnego i korespondencji w ramach procedur pozyskiwania danych informatycznych oraz formułuje konkluzje z nich wynikające. W dalszej części oceniana jest kwestia zgodności prawa polskiego z wypracowanymi w orzecznictwie Trybunału standardami, ich wpływ na realizację podstawowych funkcji prawa karnego oraz przedstawiane są propozycje zmian w tym zakresie.

Słowa kluczowe: prawo do prywatności, prawo do poszanowania życia prywatnego, korespondencja, dane informatyczne, klauzula limitacyjna, postępowanie karne, cyberprzestępczość, prawa człowieka

¹ Absolwent prawa stacjonarnego na Wydziale Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie. Słuchacz na studiach podyplomowych z inżynierii danych (Big Data) w Szkole Głównej Handlowej w Warszawie. Zainteresowania badawcze – dane w prawie, prawo karne, a także wpływ technologii na tworzenie i stosowanie prawa; ochrona praw człowieka w kontekście zmian technologicznych.

Abstract: Collection of computer data in the criminal proceedings and the elements of the right to privacy in the European systems for the protection of human rights

The article discusses the issue of admissibility of collecting computer data for the purposes of criminal trial in conjunction with selected elements of the right to privacy. It presents basic issues related to the protection of private and family life, protection of correspondence and their limitations in the European systems for the protection of human rights. The author analyzes selected judgments of the European Court of Human Rights in Strasbourg regarding the violations of the right to respect for private and family life and the right to correspondence in the context of computer data collection procedures. Furthermore, the issue of compliance of Polish law with the standards developed in the case law of the Court is assessed, as well as their impact on the implementation of the criminal law's basic principles, and proposals for changes in this area are presented.

Keywords: right to privacy, right to respect for one's private life, correspondence, computer data, limitation clauses, criminal trial, cybercrime, human rights

1. Wprowadzenie

Postępująca informatyzacja życia społecznego, a co za tym idzie zwiększona liczba tzw. cyberprzestępstw², ma bez wątpienia szeroki i wieloaspektowy wpływ na funkcjonowanie procedury karnej. Jednym z jej skutków jest wzrost znaczenia zagadnień związanych z pozyskiwaniem danych informatycznych na potrzeby postępowania, które mogą niejednokrotnie stanowić wyłączne dowody w sprawie. Ze względu na charakter i specyfikę danych informatycznych wykonywanie czynności procesowych polegających na zabezpieczeniu i zatrzymaniu tego rodzaju dowodów sprzyja powstawaniu sytuacji kolizyjnych w zakresie takich wartości jak dążenie do ustalenia prawdy materialnej i dobro wymiaru sprawiedliwości, a prawo do prywatności oraz swoboda komunikowania się jednostek.

Dyskrecjonalność organów państwowych w ramach stosowanych metod, ich intensyfikacji oraz dopuszczalnego zakresu pozyskiwanych danych

² Def. przestępstwa w zakresie czynów skierowanych przeciwko systemowi komputerowemu i czynów dokonanych przy użyciu komputera jako narzędzia (Międzynarodowa Organizacja Policji Kryminalnych „Interpol”, <https://www.interpol.int> [dostęp 14.6.2023]).

informatycznych ogranicza m.in. Konwencja o ochronie praw człowieka i podstawowych wolności z dnia 4 listopada 1950 r.³, która w art. 8 gwarantuje prawo do poszanowania życia prywatnego i rodzinnego, mieszkania oraz wolność korespondencji. Wprowadza jednak szeroki katalog ustępstw w ramach tzw. klauzuli limitacyjnej (ust. 2). Ich wykładnia w kontekście cyfrowym jest często niejednoznaczna i bywa przedmiotem orzecznictwa Europejskiego Trybunału Praw Człowieka w Strasburgu⁴.

Celem przeprowadzonej analizy było m.in. określenie dopuszczalnego stopnia ekstensywności ingerencji organów państwowych (w odniesieniu do organów postępowania karnego) w prawo do poszanowania życia prywatnego i rodzinnego oraz korespondencji (art. 8 Konwencji) w ramach procedur pozyskiwania danych informatycznych na potrzeby postępowania karnego.

Dominującą metodą badań jest analiza orzecznictwa Trybunału, a następnie podjęcie próby ujednolicenia wynikających z niego standardów dotyczących zakresu dopuszczalności metod pozyskiwania danych informatycznych na gruncie systemu Rady Europy.

Niniejsze opracowanie jest ponadto próbą odpowiedzi na pytanie, czy obecnie obowiązująca krajowa procedura w zakresie pozyskiwania danych informatycznych pozostaje zgodna z nakreślonym w orzecznictwie Trybunału. Postawiona w artykule hipoteza badawcza zakłada, że polskie regulacje prawne dotyczące pozyskiwania danych informatycznych nie spełniają w pełni standardów wypracowanych przez Trybunał związanych z dopuszczalnym zakresem ingerencji w prawo do poszanowania życia prywatnego, rodzinnego i korespondencji. Z drugiej strony, kwestią wymagającą ustalenia jest ocena czy obowiązujące standardy wynikające z orzecznictwa Trybunału wystarczają do pełnej realizacji podstawowych założeń krajowego prawa karnego, a więc w szczególności do skutecznego działania organów wykonawczych wymiaru sprawiedliwości w zakresie ścigania przestępstw.

2. Prawo do prywatności w systemach ochrony praw człowieka Rady Europy i Unii Europejskiej

³ Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie 4.11.1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz. U. z 1993 r. Nr 61, poz. 284 z późn. zm.), dalej jako: „Konwencja”, „EKPC”.

⁴ Europejski Trybunał Praw Człowieka z siedzibą w Strasburgu, dalej jako: „Trybunał”.

Jako pierwowzór dzisiejszego rozumienia prawa do prywatności uznaje się ukształtowane pod koniec XIX w. w Stanach Zjednoczonych m.in. za sprawą prac T.M. Colleya prawo do pozostawienia w spokoju (*the right to be left alone*)⁵. Choć historycznie powstałe później niż klasyczne prawa osobiste i polityczne, bywa dziś zaliczane przedmiotowo do tzw. praw pierwszej generacji⁶. Jest zasadniczo objęte wysokim, ale nie bezwzględnym standardem ochrony. W strukturach europejskich ochrony prawa do prywatności bezpośrednio dotyczą zarówno konwencyjne postanowienia w ramach systemu Rady Europy (tutaj w kontekście prawa do poszanowania życia prywatnego i rodzinnego, mieszkania i korespondencji) oraz w sensie poszanowania życia prywatnego i rodzinnego, domu i komunikowania się systemie Unii Europejskiej – w Karcie Praw Podstawowych Unii Europejskiej⁷.

Zgodnie z art. 8 ust. 1 Konwencji, każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji. Powyższy przepis wprowadza jednocześnie sformułowaną negatywnie klauzulę limitacyjną znajdującą się w ust. 2 rzeczonego artykułu. Dopuszcza ona ingerencję władzy publicznej w korzystanie obywateli z tych praw w przypadkach, gdy ingerencja taka jest przewidziana przez ustawę i konieczna w demokratycznym społeczeństwie z uwagi na:

- 1) bezpieczeństwo państwowe;
- 2) bezpieczeństwo publiczne;
- 3) dobrobyt gospodarczy kraju;
- 4) ochronę porządku i zapobieganie przestępstwom;
- 5) ochronę zdrowia i moralności;
- 6) ochronę praw i wolności innych osób.

Konwencja wprowadza tym samym katalog pojęć autonomicznych, których definiowanie przez Trybunał ma charakter dynamiczny⁸. W kontekście tematyki niniejszego opracowania istotne jest przede wszystkim pojęcie „korespondencji”, które to – zgodnie z dotychczasową praktyką orzeczniczą Trybunału – oprócz klasycznego rozumienia może odnosić się również do wiadomości elektronicznych,

⁵ J. Sieńczyło-Chlabowicz, *O prawie i jego dziejach. Księga II*, Białystok 2010, s. 1050.

⁶ M. Pryciak, *Prawo do prywatności*, Studia Erasmiانا Wratislaviensia 4/2010, s. 212–214.

⁷ Karta praw podstawowych Unii Europejskiej (Dz.U.UE.C.2007.303.1), dalej jako: „Karta Praw Podstawowych UE”, „Karta”.

⁸ K. Strzępek, *Zakres ochrony Artykułu 8 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności – uwagi ogólne na tle orzecznictwa Europejskiego Trybunału Praw Człowieka*, *Prawo i Więź* 33/2020, s. 279.

danych internetowych, danych przechowywanych na serwerach komputerowych i dyskach twardych oraz dyskiecie⁹.

Klauzula ograniczająca z art. 8 ust. 2 Konwencji posługuje się katalogiem przesłanek o dwojakim charakterze: formalnym oraz materialnym. Pod pojęciem przesłanki formalnej rozumie się tzw. wymóg legalności¹⁰, tj. obowiązek ustanowienia ograniczenia w prawie państwowym (ustawie). Pozostałe przesłanki, w tym wymóg „konieczności w demokratycznym społeczeństwie” mają charakter materialny.

W orzecznictwie (m.in. w sprawach *S. i Marper v. Wielka Brytania*¹¹ i *Malone v. Wielka Brytania*¹²) oraz w doktrynie¹³ wskazuje się, że najważniejsze obowiązki prawodawcy krajowego determinujące spełnienie wymogu legalności to przede wszystkim istnienie podstawy prawnej ingerencji w danym czasie w prawie krajowym. Jednocześnie spełnione muszą zostać wymogi jakościowe, czyli: powszechna dostępność źródła prawa, które formułuje ograniczenie, jego przewidywalność, tj. sytuacja, w której jednostka może dokonać samodzielnej oceny konsekwencji prawnych z jego wynikających oraz istnienie systemu ochrony przed arbitralną ingerencją. Łączne spełnienie tych przesłanek stanowi podstawę do uznania, że został spełniony warunek legalności ingerencji.

Innym rodzajem przesłanek klauzuli ograniczającej są kryteria materialne. Należy do nich wymóg „konieczności w demokratycznym społeczeństwie”, na który – zgodnie z utrwalonym orzecznictwem Trybunału – składają się elementy proporcjonalności i pilnej potrzeby społecznej ingerencji¹⁴. Kryterium proporcjonalności oznacza, że interes państwa-strony powinien zostać przeciwstawiony interesowi jednostki¹⁵. Konieczne jest więc, aby ingerencja w prawa jednostki przybierała możliwie najmniejszą intensywność wystarczającą

⁹ K. Strzępek, *op. cit.*, s. 285.

¹⁰ B. Latos, *Klauzula derogacyjna i limitacyjna w europejskiej konwencji o ochronie praw człowieka i podstawowych wolności*, Warszawa 2008, s. 165–168.

¹¹ Wyrok Europejskiego Trybunału Praw Człowieka z 4.12.2008 r., [WI], skarga nr 30562/04 i 30566/04, § 66–67.

¹² Wyrok Europejskiego Trybunału Praw Człowieka z 2.8.1984 r., skarga nr 8691/79, § 66.

¹³ Z. Kulińska-Kępa, *Prawa Obywatelskie i polityczne a prawa gospodarcze, społeczne i kulturalne. Porównanie systemów ochrony*, pkt 5.2.2.

¹⁴ Zob. np. wyroki Europejskiego Trybunału Praw Człowieka: z dnia 7.12.1976 r., *Handyside v. Wielka Brytania*, skarga nr 5493/72, § 48–49; z dnia 22.10.1981 r., *Dudgeon v. Wielka Brytania*, skarga nr 7525/76, § 53.

¹⁵ Wyrok Europejskiego Trybunału Praw Człowieka z dnia 8.4.2021 r., *Vavříčka i inni v. Republika Czeska* [WI], skarga nr 47621/13, § 273–275.

jednocześnie do osiągnięcia zamierzonego celu. Kryterium konieczności zakłada ponadto wystąpienie pilnej potrzeby społecznej danej ingerencji¹⁶. Zgodnie z regułą szerszego marginesu oceny, regularnie stosowaną w orzeczeniach Trybunału, to do władz krajowych należy wstępna ocena zaistnienia pilnej potrzeby społecznej, jednak taka decyzja potencjalnie podlega następcej kontroli dokonywanej przez Trybunał przy rozpatrywaniu skargi¹⁷.

Drugim rodzajem kryterium materialnego przesłanek klauzuli ograniczającej zawartej w art. 8 ust. 2 Konwencji jest kryterium celowości (nazywane również warunkiem legalności materialnej)¹⁸. Zgodnie z nim działania ograniczające możliwość korzystania z prawa muszą służyć realizacji jednego z celów wymienionych w postanowieniach dotyczących praw podlegających ograniczeniom. Powyższe cele mają różnoraki charakter w zależności od tego, którego prawa przyznanego przez Konwencję dotyczą. W ramach art. 8 Konwencji są one wskazane w ust. 2 *in fine*. Wszystkie konwencyjne przesłanki ograniczeń prawa do poszanowania życia prywatnego, rodzinnego i korespondencji podlegają jednak pewnym nadrzędnym zasadom wypracowanym w orzecznictwie Trybunału. Po pierwsze, wykładnia ograniczeń, podobnie jak innego rodzaju regulacji zawartych w Konwencji powinna być przeprowadzana zgodnie z koncepcją „*living instrument*”, stanowiącą, że Konwencja jest instrumentem żywym, który należy interpretować w świetle warunków dnia dzisiejszego¹⁹.

Kolejną z wytycznych dla wykładni ograniczeń jest zasada ochrony realnej związana z zasadą rzeczywistości i skuteczności praw zawartych w Konwencji, która stanowi, że Konwencja gwarantuje (chroni) prawa nie teoretyczne i iluzoryczne, ale rzeczywiste (praktyczne) i skuteczne²⁰. Gwarancje muszą być ponadto możliwe do wyegzekwowania, należy więc stworzyć w tym celu środki wykonawcze, przepisy prawne i mechanizmy kontrolne²¹. W kontekście ograniczeń prawa

¹⁶ Europejski Trybunał Praw Człowieka, *Guide on Article 8 of the European Convention on Human Rights*, wersja z 31.8.2022, 13/172.

¹⁷ Wyrok Europejskiego Trybunału Praw Człowieka z dnia 7.12.1976 r., *Handyside v. Wielka Brytania*, skarga nr 5493/72, § 48.

¹⁸ Zob. np. L. Garlicki (red.), *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności. Tom I. Komentarz do artykułów 1-18*, Warszawa 2010, s. 488 [w: Z. Kulińska-Kępa, op. cit.].

¹⁹ Wyrok Europejskiego Trybunału Praw Człowieka z dnia 25.4.1978 r., *Tyrer v. Wielka Brytania*, nr skargi 5856/72, § 31.

²⁰ Zob. np. wyrok Europejskiego Trybunału Praw Człowieka z dnia 9.10.1979 r., *Airey v. Irlandia*, nr skargi 6289/73, § 24.

²¹ Zob. np. wyrok Europejskiego Trybunału Praw Człowieka z dnia 4.12.2015 r., *Zakharov v. Rosja*, [WI], nr skargi 47143/06, § 232.

do poszanowania życia prywatnego, rodzinnego i korespondencji oznacza to konieczność zastosowania pogłębionego badania możliwości zastosowania ograniczeń oraz wykazania istnienia rzeczywistych podstaw do ingerencji przez państwo²².

Mimo obszernego zakresu ochrony wybranych aspektów prawa do prywatności (takich jak np. prawo do poszanowania życia prywatnego) Trybunał w swoich orzeczeniach wielokrotnie zezwalał w tej sferze na odstępstwa, zwłaszcza w przypadkach, kiedy przeciwstawianą im wartością było dobro wymiaru sprawiedliwości państwa członkowskiego. Jak zaznaczył Trybunał w sprawie *L.L. v. Francja*²³, „w pewnych sytuacjach tajemnica danych medycznych oraz interesy pacjenta muszą ustąpić przed interesem śledztwa i ścigania przestępstw oraz zachowania publicznego charakteru procesu sądowego, jeśli te okażą się istotniejsze”. Z kolei we wspomnianej już sprawie *S. i Marper v. Wielka Brytania*²⁴ Trybunał wskazał na obowiązek zapewnienia przez prawo krajowe, aby dane osobowe były zbierane wyłącznie w celach istotnych, przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, i nie dłużej niż przez okres wymagany ze względu na taki cel. Zwrócił również uwagę na konieczność zapewnienia odpowiednich gwarancji ich skutecznej ochrony przed niewłaściwym użyciem lub nadużyciami. Co jednak warto zauważyć, wskazał również, że sama obawa jednostki o to, że w przyszłości możliwe będzie posłużenie się jej prywatnymi danymi przez władze jest istotna przy ocenie, czy doszło do ingerencji w jej życie prywatne.

W Karcie Praw Podstawowych UE regulacje dotyczące ochrony prywatności zostały ustanowione w ramach art. 7. Zgodnie z nim każdy ma prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się. Pod względem językowym, pomimo zasadniczo tożsamer do art. 8 Konwencji przedmiotu ochrony wyodrębnić można w ich treści kilka różnic.

Karta posługuje się pojęciem autonomicznym „komunikowania się”, podczas gdy w Konwencji użyte zostało bardziej konserwatywne określenie „korespondencja”. Brak jest ponadto w art. 7 Karty wyrażonych *explicite* przesłanek ograniczających zakres ochrony wynikających z niego praw. Ogólnie sformułowaną klauzulę limitacyjną w stosunku do praw zawartych w Karcie określa jednak art. 52

²² Wyrok Europejskiego Trybunału Praw Człowieka z dnia 10.12.2007 r., *Stoll v. Szvajcaria*, [WI], nr skargi 69698/01, § 128.

²³ Wyrok Europejskiego Trybunału Praw Człowieka z dnia 10.10.2006 r., nr skargi 7508/02.

²⁴ Wyrok Europejskiego Trybunału Praw Człowieka z dnia 4.12.2008 r., [WI], nr skargi 30562/04 i 30566/04, § 103.

ust. 1 Karty, który dopuszcza stosowanie ograniczeń pod warunkiem, że są one przewidziane ustawą i szanują istotę tych praw i wolności. Mogą być one wprowadzone tylko z poszanowaniem zasady proporcjonalności oraz wyłącznie wtedy, gdy są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób.

Warto zauważyć, że ze względu na obecność art. 8 Karty dotyczącego ochrony danych osobowych w orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej²⁵ art. 7 Karty jest często pomocniczo uwzględniany w tego rodzaju sprawach. Jak zaznacza TSUE „art. 7 Karty musi być należycie wzięty pod uwagę przy dokonywaniu wykładni stosownych przepisów dyrektywy, która wymaga od państw członkowskich szczególnie ochrony prawa do prywatności”²⁶. Ponadto, w sprawie *Volker i Markus Schecke GbR i Hartmut Eifert v. Land Hessen*²⁷ TSUE stwierdził, że „ograniczenia prawa do ochrony danych osobowych mogą być uzasadnione, jeżeli odpowiadają tym, które są tolerowane w ramach art. 8 EKPC”.

Zgodnie z art. 52 Karty w zakresie, w jakim zawiera ona prawa, które odpowiadają prawom zagwarantowanym w Konwencji, ich znaczenie i zakres są takie same jak praw z Konwencji. Znajduje to również potwierdzenie w wyjaśnieniach dotyczących art. 7 Karty²⁸, stanowiącym, że prawa zagwarantowane w art. 7 Karty odpowiadają prawom zagwarantowanym na mocy art. 8 Konwencji. Aby uwzględnić rozwój technologiczny, określenie „korespondencja” zostało zastąpione określeniem „komunikowanie się”. W ramach wyjaśnień zaznacza się również, że taka sama jak w Konwencji jest wykładnia dozwolonych ograniczeń dotyczących chronionych elementów prawa do prywatności zawartych w art. 52 ust. 1 Karty. Należy więc uznać art. 7 Karty i art. 8 Konwencji za przepisy o tożsamym znaczeniu i traktować tak również prawa z nich wynikające, a także ograniczenia ochrony tych praw, co oznacza, że standardy orzecznicze wypracowane przez Trybunał powinny być stosowane również przy wykładni art. 7 Karty.

²⁵ Trybunał Sprawiedliwości Unii Europejskiej z siedzibą w Luksemburgu, dalej jako: „TSUE”.

²⁶ Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 13.5.2014 r., *Google Spain SL i Google Inc. v. Agencia Española de Protección de Datos (AEPD) i Mario Costeja González*, C-131/12, pkt 69.

²⁷ Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 9.11.2010 r., C-92/09, pkt 52.

²⁸ Zob. Wyjaśnienia dotyczące Karty praw podstawowych, Dz.U. UE C 303 z 14.12.2007 r., s. 17; wyjaśnienie do art. 7 Karty.

3. Wyrok Trybunału w sprawie *Kirdok i inni v. Turcja*²⁹

Orzecznictwo Trybunału odgrywa – poza sferą normatywną – kluczową rolę w systemach ochrony praw człowieka Rady Europy i Unii Europejskiej w kształtowaniu modelu ochrony aspektów prawa do prywatności, jakimi są m.in. prawo do poszanowania życia prywatnego, rodzinnego i korespondencji. Zakres przedmiotowy niniejszej tematyki jest obszerny, a w niniejszym opracowaniu przeanalizowane zostaną jedynie wybrane orzeczenia w tym zakresie. Jednym z takich wyroków, odnoszącym się w szczególności do poszanowania korespondencji oraz obowiązków organów wykonawczych jest sprawa *Kirdok i inni v. Turcja*. Skarżącymi w omawianej sprawie byli prawnicy, którzy zarzucali organom władzy publicznej naruszenie tajemnicy zawodowej wynikającej z poufności ich relacji z klientami poprzez skopiowanie podczas przeszukania należących do nich danych informatycznych. Zgromadzone przez organy dane miały zostać wykorzystane dla celów postępowania karnego prowadzonego przeciwko innemu prawnikowi, z którym wnioskodawcy dzielili biuro. Zdaniem skarżących uzyskane w ten sposób kopie nie miały znaczenia dla rzeczonego śledztwa. W związku z objęciem przejętych danych tajemnicą zawodową skarżący złożyli odwołanie w tej sprawie do sądu krajowego, żądając zwrócenia lub zniszczenia rzeczonych danych. Odwołanie zostało jednak oddalone przez sąd krajowy w konsekwencji uznania powyższych działań za zgodne z prawem. Zarzut naruszenia art. 8 Konwencji był przez Trybunał rozpatrywany zarówno samodzielnie jak i związku z art. 13 Konwencji (prawo do skutecznego środka odwoławczego).

Argumentacja rządu w ramach art. 8 Konwencji polegała na negowaniu przynależności plików do skarżących w związku z niemożnością ostatecznego ustalenia własności skonfiskowanych danych w postępowaniu krajowym. Zdaniem rządu, aby doszło do naruszenia art. 8 Konwencji konieczne było całkowite odszyfrowanie, transkrypcja i oficjalne przypisanie wspomnianych danych skarżącym. Ponadto, rząd wskazywał również na niewyczerpanie krajowych środków odwoławczych proponując wniesienie powództwa o odszkodowanie za szkodę poniesioną w wyniku przeszukania przeprowadzonego w sposób nieproporcjonalny.

Trybunał wskazał, że – w świetle ugruntowanego orzecznictwa – czynności realizowane w kancelariach prawnych jako objęte tajemnicą zawodową zasadniczo stanowią ingerencję w prawo do poszanowania życia prywatnego

²⁹ Wyrok Europejskiego Trybunału Praw Człowieka z dnia 3.12.2019 r., skarga nr 14704/12.

chronione na mocy art. 8 Konwencji³⁰. Co istotne, odniósł się również do wykładni pojęcia „korespondencji” użytego w ramach art. 8 Konwencji wskazując – w myśl koncepcji „*living instrument*” – że naruszenie prawa do korespondencji obejmuje również fakt przeszukania i zatrzymania komputerowych dysków twardych oraz danych informatycznych, takich jak pliki komputerowe i wiadomości³¹.

Trybunał zaznaczył ponadto, że aby doszło do naruszenia art. 8 Konwencji w kontekście prawa do korespondencji nie jest konieczne ostateczne ustalenie własności skonfiskowanych danych informatycznych. Do naruszenia prawa do korespondencji wystarczy sama ingerencja w tego rodzaju dane i nie jest ono uzależnione od dalszego toku czynności podjętych przez organy.

W ramach weryfikacji spełnienia warunku legalności Trybunał uznał, że ingerencja organów nie miała podstawy w prawie krajowym, w tym sensie, że prawo krajowe nakładało na organy postępowania obowiązek zwrotu skarżącym lub zniszczenia danych informatycznych przejętych podczas przeszukania w razie późniejszego poinformowania ich o fakcie, że dane te są objęte tajemnicą zawodową. Ponadto – jak zaznaczył Trybunał – zastosowana procedura nie była wyraźnie przewidziana przez prawo krajowe oraz była sprzeczna z istotą tajemnicy zawodowej.

Konkluzja Trybunału w ramach badania wymogu „konieczności ingerencji w demokratycznym społeczeństwie” polegała po pierwsze na wskazaniu, że na organy nakłada się obowiązek dostatecznie precyzyjnej regulacji zakresu zatrzymywanych danych informatycznych. Ingerencja może być więc uznana za uzasadnioną jedynie w przypadku, kiedy postanowienie dotyczące zatrzymania takich danych dokładnie wymienia dane podlegające zatrzymaniu oraz jest związane z zaspokojeniem pilnej potrzeby społecznej. Postanowienie takie nie może opierać się więc jedynie na ogólnie określonym celu podejmowanych działań, np. wykazaniu, że podejrzany prowadzi działalność w ramach organizacji terrorystycznej.

Ponadto Trybunał nakazał przestrzeganie procedury filtrowania w razie zatrzymywania danych informatycznych objętych tajemnicą zawodową nakładając obowiązek zawarcia w postanowieniu wyraźnego zakazu przejmowania

³⁰ Zob. m.in. wyrok Europejskiego Trybunału Praw Człowieka z dnia 28.4.2005 r., *Buck v. Niemcy*, skarga nr 41604/98, § 31–32.

³¹ Zob. szerzej Przeszukanie i zatrzymanie komputerowych dysków twardych: wyrok Europejskiego Trybunału Praw Człowieka z dnia 27.9.2005 r., *Petri Sallinen i inni v. Finlandia*, skarga nr 50882/99, § 71; przeszukanie i zatrzymanie danych informatycznych: wyrok Europejskiego Trybunału Praw Człowieka z dnia 16.10.2007 r., *Wieser i Bicos Beteiligungen GmbH v. Austria*, skarga nr 74336/01, § 66–68.

takich danych. Wskazał również, że ingerencji nie usprawiedliwia sam fakt zaszyfrowania czy ukrycia danych objętych tajemnicą zawodową mimo ich zatrzymania. W razie zatrzymania danych objętych tajemnicą zawodową Trybunał wskazał na obowiązek zapewnienia szczególnie rygorystycznego monitorowania środków odwoławczych dotyczących takich danych. Nawiązując do obowiązku interpretacji ograniczeń zgodnie z zasadą ochrony realnej wskazał, że taki środek odwoławczy powinien mieć skuteczny charakter (fr. „*contrôle efficace*”), a co za tym idzie zapobiegać potencjalnie popełnionemu naruszeniu. Zdaniem Trybunału propozycja rządu dotycząca wniesienia powództwa o odszkodowanie za szkodę poniesioną w wyniku przeszukania przeprowadzonego w sposób nieproporcjonalny nie miała takiego charakteru.

Omawiana sprawa jest więc szczególnie istotna w kontekście gromadzenia danych informatycznych przez organy postępowania karnego z kilku względów. Po pierwsze, należy docenić jej wagę z punktu widzenia rozszerzenia znaczenia pojęcia „korespondencji” użytego w art. 8 Konwencji również do komputerowych dysków twardych oraz danych informatycznych. Po drugie, statuuje ona regułę, w myśl której do stwierdzenia naruszenia art. 8 Konwencji wystarczy sama ingerencja organów w prywatną korespondencję jednocześnie uniezależniając takowe od jakichkolwiek innych podjętych przez organy czynności, takich jak ich późniejsze odszyfrowanie, transkrypcja czy oficjalne przypisanie osobie skarżącej. Po trzecie, nakłada na organy wydające postanowienie o zatrzymaniu danych informatycznych obowiązek precyzyjnego określenia zakresu dokonywanych czynności. Wyklucza tym samym możliwość zastosowania nieproporcjonalnie szerokiego przejęcia danych. Istotny z punktu widzenia poszanowania prawa do korespondencji jest ponadto wspomniany nakaz przestrzegania procedury filtrowania w razie zatrzymywania danych informatycznych objętych tajemnicą zawodową.

4. Wyrok Trybunału w sprawie *Benedik v. Słowenia*³²

W przeciwieństwie do sprawy *Kirdok i inni v. Turcja*, kreującej obowiązki przede wszystkim po stronie organów wykonawczych konkluzje z wyroku *Benedik v. Słowenia* adresowane są już bezpośrednio do ustawodawcy. Skarga w niniejszej sprawie jest konsekwencją działań szwajcarskich organów ścigania polegających na nadzorowaniu użytkowników, w wyniku których ustalono, że byli oni w posiadaniu

³² Wyrok Europejskiego Trybunału Praw Człowieka z dnia 24.7.2018 r., skarga nr 62357/14.

oraz wymieniali się materiałami zawierającymi pornografię dziecięcą w postaci zdjęć lub nagrań wideo. Jednym z jej użytkowników był późniejszy skarżący w omawianej sprawie obywatel Słowenii, którego adres IP został ujawniony w toku działań organów, przekazany słoweńskiej policji, a następnie skierowany bez uzyskania postanowienia sądu do słoweńskiego dostawcy usługi internetowej w celu ujawnienia jego danych użytkownika (w tym m.in. danych osobowych).

Postanowienie sądowe pozwalające na ujawnienie danych osobowych abonenta oraz danych o ruchu zostało wydane kilka miesięcy po faktycznym uzyskaniu danych. Późniejszy skarżący w omawianej sprawie wielokrotnie kwestionował legalność czynności podjętych przed sądami krajowymi, podnosząc m.in. zarzut bezprawnego uzyskania materiału dowodowego dotyczącego tożsamości użytkownika używanego przez niego adresu IP, a następnie wnioskując o wyłączenie uzyskanego bezprawnie materiału dowodowego. Jego żądania nie zostały jednak uwzględnione, zgodnie bowiem z argumentacją organów krajowych – niemożliwa była kwalifikacja adresu IP, za pomocą którego doszło do skierowania do operatora usługi internetowej prośby oraz późniejszego ujawnienia danych użytkownika jako danych o ruchu, zatem zgodnie ze słoweńskim porządkiem prawnym dopuszczalne było jego uzyskanie, a następnie identyfikacja użytkownika bez postanowienia sądu. Sprawa trafiła do słoweńskiego Trybunału Konstytucyjnego, który mimo odejścia od – jak się zresztą wydaje mylnej – interpretacji sądów krajowych wyłączającej adresy IP użytkowników z kategorii danych o ruchu – również oddalił skargę. Wskazał jednak, że w ramach analizy, czy doszło do naruszenia prawa do poszanowania życia prywatnego użytkownika konieczne jest ustalenie jego uzasadnionego oczekiwania prywatności. Zdaniem Trybunału Konstytucyjnego powyższa przesłanka również nie została spełniona w omawianej sprawie, ponieważ skarżący umyślnie rzekł się swojej prywatności dokonując publicznej wymiany przedmiotowych plików.

Trybunał analizując kwestię potencjalnego naruszenia art. 8 Konwencji w kontekście prawa do poszanowania życia prywatnego uznał – podobnie do słoweńskiego Trybunału Konstytucyjnego – że konieczne jest ustalenie, czy skarżący miał uzasadnione oczekiwanie, że jego działalność w sieci pozostanie anonimowa. Wskazał również, że uzasadnione oczekiwanie prywatności jest czynnikiem istotnym, choć niekonieczne determinującym zastosowanie art. 8 Konwencji³³. Odmienne jednak do słoweńskiego Trybunału Konstytucyjnego uznał,

³³ Zob. wyrok Europejskiego Trybunału Praw Człowieka z dnia 5.9.2017 r., *Bărbulescu v. Rumunia*, [WI], skarga nr 61496/08, § 73.

że w omawianej sprawie oczekiwanie prywatności należy oceniać w stosunku do tożsamości skarżącego, nie natomiast jak orzekł Trybunał Konstytucyjny – co do jego dynamicznego adresu IP. Biorąc pod uwagę powyższe stwierdził, że oczekiwania skarżącego w odniesieniu do jego aktywności online należy uznać za uzasadnione. Wydaje się, że jest to słuszna interpretacja – przyjęcie bowiem odmiennego stanowiska mogłoby prowadzić do wykształcenia się praktyki polegającej na maskowaniu dynamicznych adresów IP przez sprawców wyłącznie w celu spełnienia wymogu uzasadnionego oczekiwania prywatności, co zredukowałoby jednocześnie w wielu przypadkach ich wykrywalność.

Wskazano ponadto, że zakres przedmiotowy art. 8 Konwencji obejmuje dane takie jak dynamiczne adresy IP. Przywołano w tym kontekście utrwalone orzecznictwo, z którego wynika, że jeżeli doszło do kompilacji danych o danej osobie, przetwarzania lub wykorzystania danych osobowych lub opublikowania materiału w sposób lub w stopniu wykraczającym poza przewidywalny w normalnych okolicznościach, powstaje wówczas kwestia życia prywatnego³⁴.

W ramach badania realizacji warunku legalności Trybunał stwierdził, że do jej spełnienia konieczne jest m.in., aby prawo krajowe było zgodne z rządami prawa, tj. by przewidywało odpowiednią ochronę przed arbitralną ingerencją w prawa z art. 8 Konwencji. Ochrona taka, analogicznie do sformułowanej w wyroku *Kirdok i inni v. Turcja* zasady skuteczności środka odwoławczego powinna w sposób odpowiedni i efektywny zapobiegać potencjalnym nadużyciom. Jako kryteria oceny środków ochrony wskazał wszystkie okoliczności sprawy, takie jak charakter, zakres i okres trwania określonych środków, podstawy ich zarządzenia oraz organy właściwe do wydania zezwolenia na zastosowanie środków, ich przeprowadzenie i nadzorowanie jak również rodzaj tych środków³⁵. Trybunał uznał w omawianej sprawie, że czynności podjęte przez organy krajowe były w sposób oczywisty niewłaściwe, a ponadto nie zapewniono żadnej ochrony przed arbitralną ingerencją. Stwierdził jednocześnie, że w czasie istotnym dla sprawy nie istniały uregulowania określające warunki zatrzymywania danych informatycznych ani zabezpieczające przed nadużyciami po stronie funkcjonariuszy państwowych w toku wspomnianej procedury.

Powyższa sprawa jest istotna z punktu widzenia omawianej tematyki zwłaszcza w kontekście pozytywnie sformułowanego obowiązku spoczywającego

³⁴ Zob. wyrok Europejskiego Trybunału Praw Człowieka z dnia 27.6.2017 r., *Satakunnan Markkinapörssi Oy i Satamedia v. Finlandia*, [WI], skarga nr 931/13, § 136.

³⁵ Zob. wyrok Europejskiego Trybunału Praw Człowieka z dnia 28.6.2007 r., *Association for European Integration and Human Rights i Ekimdzhev v. Bułgaria*, skarga nr 62540/00, § 77.

na prawodawcy państwowym dotyczącego ustanowienia przewidywalnej procedury zatrzymywania danych informatycznych oraz zapewnienia ochrony jednostce przed arbitralną ingerencją organów w tym zakresie. Wydaje się, że do jego spełnienia niezbędne jest uchwalenie przepisów dotyczących w szczególności zatrzymywania danych dotyczących pochodzenia komunikatów, takich jak imienia i nazwiska oraz adresu abonenta, któremu przypisano określony adres IP oraz ustanowienia procedury uzyskiwania dostępu do danych i ich przekazywania. Takie regulacje powinny ponadto gwarantować odpowiednie i efektywne środki chroniące przed arbitralną ingerencją w dane informatyczne.

5. Kwestia zgodności krajowej procedury ze standardami Rady Europy

Obecny kształt krajowych unormowań może okazać się niewystarczający do spełnienia standardów orzeczniczych Trybunału, przede wszystkim w kontekście warunku legalności z art. 8 Konwencji³⁶. Wspomniana potencjalna niezgodność objawia się przede wszystkim poprzez niewystarczająco szeroki zakres podmiotowy Rozporządzenia Ministra Sprawiedliwości z dnia 18 czerwca 2021 r. w sprawie sposobu technicznego przygotowania systemów i sieci służących do przekazywania informacji do gromadzenia danych informatycznych oraz danych niestanowiących treści rozmowy telefonicznej lub innego przekazu informacji, a także sposobów ich zabezpieczania w urządzeniach zawierających te dane oraz w systemach i na informatycznych nośnikach danych³⁷, które ustanawia procedurę pozyskiwania danych informatycznych na potrzeby postępowania karnego (delegacja ustawowa z art. 218b ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego³⁸). Podmioty, do których odnosi się ww. rozporządzenie w kontekście gromadzenia (zatrzymania) danych (§ 1 ust. 1 pkt 1 rozporządzenia) są bowiem ograniczone do tych wymienionych w art. 218 § 1 k.p.k., czyli jedynie urzędów, instytucji i podmiotów prowadzących działalność w dziedzinie

³⁶ Zob. szerzej J. Szpoton, *Zabezpieczanie i zatrzymywanie danych informatycznych w polskim postępowaniu karnym*, Młody Jurysta 2/2023, s. 29–30.

³⁷ Rozporządzenie Ministra Sprawiedliwości z dnia 18 czerwca 2021 r. w sprawie sposobu technicznego przygotowania systemów i sieci służących do przekazywania informacji do gromadzenia danych informatycznych oraz danych niestanowiących treści rozmowy telefonicznej lub innego przekazu informacji, a także sposobów ich zabezpieczania w urządzeniach zawierających te dane oraz w systemach i na informatycznych nośnikach danych (Dz. U. poz. 1101), dalej jako: „rozporządzenie”, „rozporządzenie 218b”.

³⁸ Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (t.j. Dz. U. z 2024 r. poz. 37 z późn. zm.), dalej jako: „k.p.k.”.

poczty lub działalność telekomunikacyjną, urzędów celno-skarbowych oraz instytucji i przedsiębiorstw transportowych.

Powyższe ograniczenie może skutkować niezgodnością formalną, w szczególności w przypadku wydania postanowienia o zatrzymaniu danych informatycznych w stosunku do dysponenta niewymienionego w ramach zakresu podmiotowego art. 218 § 1 k.p.k., bez ich uprzedniego zabezpieczenia (procedura zabezpieczania danych informatycznych jest bowiem uregulowana w § 1 ust. 1 pkt 2 i 3 rozporządzenia i odnosi się do znacznie szerszego zakresu podmiotów). Dokonanie tego rodzaju czynności bez wyraźnej podstawy prawnej mogłoby potencjalnie zostać przez Trybunał uznane – w kontekście wspomnianych konkluzji z orzecznictwa Trybunału – jako naruszenie w zakresie prawa do poszanowania życia prywatnego, rodzinnego i korespondencji, związane m.in. z brakiem ustanowienia przewidywalnej procedury zatrzymywania danych informatycznych w prawie krajowym. *De lege lata* wydaje się zatem, że kluczowa jest kwestia zachowania w tym zakresie jasności terminologicznej.

Należy ponadto uznać, że nakreślone przez Trybunał wymogi nie umniejszają znacząco kompetencji uprawnionych organów wymiaru sprawiedliwości państw członkowskich w zakresie ścigania przestępstw. Obowiązujące standardy nakładają jedynie pewne fundamentalne obowiązki formalne na ustawodawcę i organy wykonawcze, po których spełnieniu zachowują one swoje dotychczasowe uprawnienia. Zarzuty sugerujące, że implementacja standardów Trybunału może osłabić skuteczność ścigania przestępstw, opierają się często na fałszywym przeciwstawieniu funkcji ochronnej i gwarancyjnej. Tymczasem efektywność prawa karnego nie powinna być mierzona wyłącznie przez pryzmat represji, lecz również przez jakość gwarancji procesowych, jakie oferuje jednostce. Na pierwszy rzut oka mogłoby się wydawać, że zastosowanie tego rodzaju wytycznych mogłoby bowiem stanowić poważne zagrożenie właśnie dla funkcji ochronnej prawa karnego.

Tymczasem jest dokładnie odwrotnie – stosowanie wytycznych wypracowanych przez Trybunał nie tylko nie ogranicza możliwości realizacji fundamentalnych celów prawa karnego, ale wręcz je wzmacnia. Wynika to przede wszystkim z obecności funkcji gwarancyjnej prawa karnego, której istotą jest ochrona jednostki przed nadużyciami władzy publicznej. Pominięcie wskazanych przez Trybunał standardów proceduralnych skutkowałoby jej istotnym osłabieniem na rzecz jednostronnego uprzywilejowania funkcji ochronnej, co pozostaje w sprzeczności z zasadą proporcjonalności. Z tego względu – jak się wydaje – spełnienie wymogów dotyczących dopuszczalności pozyskiwania danych informatycznych, a w szczególności tych wynikających z pozytywnych obowiązków

legislacyjnych, stanowi warunek *sine qua non* prawidłowej realizacji celów prawa karnego.

6. Wnioski

W ramach konkluzji z przeprowadzonej analizy należy wskazać, że Trybunał – co do zasady – konsekwentnie przyznaje prymat konwencyjnemu prawu do poszanowania życia prywatnego, rodzinnego i korespondencji. Istotne jest jednak, że mimo tak zdecydowanego stanowiska (bezwzględność Trybunału w analizowanych sprawach wynikała m.in. z powagi oraz wysokiego stopnia społecznej szkodliwości niektórych czynów, dotyczących m.in. posiadania i obrotu pornografią dziecięcą), Trybunał jednocześnie formułuje przesłanki, których spełnienie może prowadzić do uznania ingerencji w te prawa za uzasadnioną. Do przesłanek tych należą przede wszystkim:

- 1) obowiązek dostatecznie precyzyjnej regulacji zakresu zatrzymywanych danych informatycznych;
- 2) obowiązek zawarcia w postanowieniu wyraźnego zakazu przejmowania danych objętych tajemnicą zawodową (tzw. procedura filtrowania);
- 3) konieczność zbadania, czy skarżący miał uzasadnione oczekiwanie, że jego tożsamość w sieci pozostanie anonimowa (uzasadnione oczekiwanie prywatności);
- 4) sformułowane pozytywne obowiązki prawodawcze: obowiązek ustanowienia przewidywalnej procedury zatrzymywania i przekazywania danych informatycznych oraz zapewnienie skutecznych środków odwoławczych.

Należy wyraźnie zaznaczyć, że Trybunał w żadnym z badanych przypadków nie uznał, że do naruszenia doszło wyłącznie z uwagi na niedostateczne spełnienie przesłanki materialnej zawartej w klauzuli limitacyjnej. Podstawą wyroków stwierdzających naruszenia art. 8 Konwencji w analizowanych sprawach były natomiast w każdym przypadku uchybienia o charakterze formalnym, związane z warunkiem legalności, obciążające państwa członkowskie.

Mając to na uwadze, tym bardziej należy zwrócić uwagę na nakreślone we wcześniejszej części artykułu braki podmiotowe w polskiej procedurze w tym zakresie. Zatem *de lege ferenda*, pożądana jest przede wszystkim modyfikacja zakresu adresatów art. 218 § 1 k.p.k. w ten sposób, aby obejmował również inne grupy podmiotów, jak np. podmioty świadczące usługi drogą elektroniczną, dostawców usług cyfrowych, czy administratora treści publikowanych lub udostępnianych drogą elektroniczną. Wprowadzenie powyższych nowelizacji zminimalizuje ryzyko naruszeń art. 8 Konwencji, ponieważ pełen zakres potencjalnych adresatów

postanowień o zatrzymaniu danych informatycznych będzie wówczas objęty procedurą, którą przewiduje rozporządzenie 218b k.p.k., gwarantując posiadanie przez nią przymiotu przewidywalności oraz wykluczając ewentualne wątpliwości co do przysługujących adresatom postanowień środków odwoławczych.

Bibliografia:

- M. A. Nowicki [w:] *Komentarz do Konwencji o ochronie praw człowieka i podstawowych wolności [w:] Wokół Konwencji Europejskiej. Komentarz do Europejskiej Konwencji Praw Człowieka*, wyd. VIII, Warszawa 2021, art. 8
- B. Liżewski, *Klauzule generalne i ich funkcje w Europejskiej Konwencji Praw Człowieka*, Annales Universitatis Mariae Curie-Skłodowska. Sectio G. Ius, 63/2/2016, s. 191-207
- B. Latos, *Klauzula derogacyjna i limitacyjna w europejskiej konwencji o ochronie praw człowieka i podstawowych wolności*, Warszawa 2008
- L. Garlicki (red.), *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności. Tom I. Komentarz do artykułów 1-18*, Warszawa 2010
- M. Barański, *Ochrona danych osobowych pracowników w orzecznictwie Trybunału Konstytucyjnego oraz Trybunału Sprawiedliwości*, PiP 1/2022, s. 46-65
- T. Jurczyk, 2.3. *Prawa podstawowe zawarte w Karcie Praw Podstawowych Unii Europejskiej i Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności (analiza porównawcza) [w:] Prawa jednostki w orzecznictwie Europejskiego Trybunału Sprawiedliwości*, Warszawa 2009
- Z. Kulińska-Kępa, 5.2.2. *Ograniczenie praw ustanowionych w Konwencji o ochronie praw człowieka i podstawowych wolności [w:] Prawa Obywatelskie i polityczne a prawa gospodarcze, społeczne i kulturalne. Porównanie systemów ochrony*, Warszawa 2017
- J. Sieńczyło-Chlabowicz, *O prawie i jego dziejach. Księga II*, Białystok 2010
- M. Pryciak, *Prawo do prywatności*, Studia Erasmianna Wratislaviensia 4/2010 s. 211-229
- K. Strzępek, *Zakres ochrony Artykułu 8 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności – uwagi ogólne na tle orzecznictwa Europejskiego Trybunału Praw Człowieka*, Prawo i Więź 33/2020, s. 279-294
- J. Szpoton, *Zabezpieczanie i zatrzymywanie danych informatycznych w polskim postępowaniu karnym*, Młody Jurysta, 2/2023, s. 15-31
- Wyjaśnienia dotyczące Karty praw podstawowych, Dz.U. UE C 303 z 14 grudnia 2007 r.
- Europejski Trybunał Praw Człowieka, *Guide on Article 8 of the European Convention on Human Rights*, wersja z 31.8.2022, 13/172

Orzecznictwo:

- Wyrok Europejskiego Trybunału Praw Człowieka z dnia 3.12.2019 r., skarga nr 14704/12
- Wyrok Europejskiego Trybunału Praw Człowieka z dnia 24.7.2018 r., skarga nr 62357/14



- Wyrok Europejskiego Trybunału Praw Człowieka z dnia 4.12.2008 r., [WI], skarga nr 30562/04 i 30566/04
- Wyrok Europejskiego Trybunału Praw Człowieka z dnia 2.8.1984 r., skarga nr 8691/79
- Wyrok Europejskiego Trybunału Praw Człowieka z dnia 7.12.1976 r., skarga nr 5493/72
- Wyrok Europejskiego Trybunału Praw Człowieka z dnia 22.10.1981 r., skarga nr 7525/76
- Wyrok Europejskiego Trybunału Praw Człowieka z dnia 8.4.2021 r., [WI], skarga nr 47621/13
- Wyrok Europejskiego Trybunału Praw Człowieka z dnia 25.4.1978 r., nr skargi 5856/72
- Wyrok Europejskiego Trybunału Praw Człowieka z dnia 9.10.1979 r., nr skargi 6289/73
- Wyrok Europejskiego Trybunału Praw Człowieka z dnia 4.12.2015 r., [WI], nr skargi 47143/06
- Wyrok Europejskiego Trybunału Praw Człowieka z dnia 10.12.2007 r., [WI], nr skargi 69698/01
- Wyrok Europejskiego Trybunału Praw Człowieka z dnia 10.10.2006 r., nr skargi 7508/02
- Wyrok Europejskiego Trybunału Praw Człowieka z dnia 28.4.2005 r., skarga nr 41604/98
- Wyrok Europejskiego Trybunału Praw Człowieka z dnia 27.9.2005 r., skarga nr 50882/99
- Wyrok Europejskiego Trybunału Praw Człowieka z dnia 16.10.2007 r., skarga nr 74336/01
- Wyrok Europejskiego Trybunału Praw Człowieka z dnia 5.9.2007 r., [WI], skarga nr 61496/08
- Wyrok Europejskiego Trybunału Praw Człowieka z dnia 27.6.2017 r., [WI], skarga nr 931/13
- Wyrok Europejskiego Trybunału Praw Człowieka z dnia 28.6.2007 r., skarga nr 62540/00
- Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 13.5.2014 r., C-131/12
- Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 9.11.2010 r., C-92/09

Akty prawne:

- Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie dnia 4.11.1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz. U. z 1993 r. Nr 61, poz. 284 z późn. zm.)
- Karta praw podstawowych Unii Europejskiej (Dz.U.U.E.C.2007.303.1)
- Ustawa z dnia 6.6.1997 r. Kodeks postępowania karnego (t.j. Dz. U. z 2024 r. poz. 37 z późn. zm.)
- Rozporządzenie Ministra Sprawiedliwości z dnia 18.6.2021 r. w sprawie sposobu technicznego przygotowania systemów i sieci służących do przekazywania informacji do gromadzenia danych informatycznych oraz danych niestanowiących treści rozmowy telefonicznej lub innego przekazu informacji, a także sposobów ich zabezpieczania w urządzeniach zawierających te dane oraz w systemach i na informatycznych nośnikach danych (Dz. U. poz. 1101)

Propozycja cytowania: J. Szpoton, Pozyskiwanie danych informatycznych w postępowaniu karnym a elementy prawa do prywatności w europejskich systemach ochrony praw człowieka, Młody Jurysta 2025, nr 1, s. 19–36.