Warszawa, 07-04-2026 r.

BIURO
RZECZNIKA PRAW OBYWATELSKICH

Zespół Prawa Karnego

II.519.1068.2022.DC

Wykonanie wyroku Europejskiego Trybunału Praw Człowieka w sprawie Pietrzak i Bychawska-Siniarska i inni przeciwko Polsce (sprawa nr 72038/17 i 25237/18), cz. 2.

Raport w przedmiocie retencji danych i dostępu do danych retencyjnych w świetle konstytucyjnych, unijnych i konwencyjnych standardów ochrony praw jednostki

dr Dominika Czerniak

Wydział ds. Legislacyjnych i Ustrojowych

Spis treści

Słowniczek pojęć

Definicje poniżej nie zastępują definicji ustawowych, przytoczonych w dalszej części opracowania i mają charakter pomocniczy, ułatwiający zorientowanie się w siatce terminologicznej.

- **Dane dotyczące treści** – informacje, które obejmują treść komunikacji przesyłanej drogą elektroniczną/treść komunikacji „na odległość (treść maila, SMSa, rozmowy telefoniczne, treść listu pocztowego).

- **Dane niedotyczące treści/metadane** – informacje związane z komunikacją przesyłaną drogą elektroniczną, np. czas połączenia, miejsce połączenia, dane odbiorcy, ale nieobejmujące treści komunikatu przesyłanego drogą elektroniczną/na odległość.

- **Dane abonenckie/dane o abonencie** – dane pozwalające zidentyfikować użytkownika usług łączności, np. imię, nazwisko, numer PESEL, nr dowodu osobistego/paszportu.

- **Dane transmisyjne/dane o ruchu (traffic data)** – dane, jakie są przetwarzane i gromadzone w związku z przesłaniem komunikatu elektronicznego umożliwiające m.in. ustalenie nadawcy i odbiorcy komunikatu, daty i czasu trwania połączenia, rodzaju połączenia/rodzaju komunikacji, a także parametrów technicznych transmisji.

- **Dane o lokalizacji** – dane, które wskazują położenie geograficzne użytkownika urządzenia końcowego (np. telefonu komórkowego łączącego się z nadajnikiem BTS) przetwarzane w związku ze świadczeniem usługi łączności.

- **Dane z billingów** – dane o połączeniach (numer telefonu adresata i odbiorcy połączenia, godzina połączenia, czas trwania połączenia i rodzaj połączenia) zwykle przedstawiane w formie wykazu/zestawienia.

- **Adres IP** – unikalny numer identyfikacyjny urządzenia, które łączy się z siecią.

- **Dynamiczne IP** - adres IP, który nie jest przypisany na stałe do łącza/urządzenia, tylko jest przydzielany tymczasowo przez dostawcę Internetu i może się zmieniać z każdym połączeniem z Internetem.

- **Stałe IP** – adres przypisany do użytkownika/urządzenia, który nie zmienia się wraz z kolejnymi połączeniami z Internetem.

- **Retencja danych** - ustawowy obowiązek przechowywania przez dostawców usług łączności (operatorów sieci komórkowych, dostawców Internetu itp.) określonych kategorii danych niedotyczących treści przez wskazany w przepisach prawa okres.

- **Uogólniona i niezróżnicowana retencja danych** – zatrzymywanie danych niedotyczących treści obejmujące wszystkich użytkowników usług łączności i szerokie kategorie danych (tj. dane abonenckie, dane o lokalizacji, dane o ruchu), bez ograniczeń geograficznych, czasowych, podmiotowych i przedmiotowych.

- **Retencja ukierunkowana** – zatrzymywanie danych, które jest ograniczone obiektywnymi i niedyskryminacyjnymi kryteriami (np. zatrzymywanie danych ze względów geograficznych, w określonych miejscach, kategorią użytkowników, czy z uwagi na zwiększone zagrożenia dla bezpieczeństwa powszechnego w określonym czasie), stosowana w celu minimalizacji ingerencji w prawo do prywatności.

- **Zabezpieczenie danych (mechanizm *quick freeze*)** – niezwłoczne zabezpieczenie danych w związku z realizacją konkretnych celów, np. ochrony bezpieczeństwa narodowego, zwalczania poważnej przestępczości, by uchronić dane przed usunięciem.

- **Dostęp do danych retencyjnych** - możliwość pozyskania danych podlegających retencji przez organ uprawniony. Konieczne jest posiadanie odpowiedniej podstawy prawnej – normy kompetencyjnej – pozwalającej na bezpośredni dostęp do danych przechowywanych przez operatorów usług łączności albo na zwrócenie się do operatorów ze stosownym wnioskiem/żądaniem.

- **Dostęp bezpośredni/zautomatyzowany/mechanizm „stałego łącza”** – model, w którym uprawnione podmioty mogą mieć dostęp do danych niedotyczących treści bez zaangażowania pracowników dostawców usług łączności. Dostęp do danych jest udzielany na podstawie porozumień zawieranych pomiędzy dostawcami usług łączności a odpowiednią służbą/odpowiednim organem za pośrednictwem systemu teleinformatycznego.

- **Tryb procesowy dostępu do danych retencyjnych** – możliwość zwrócenia się przez prokuratora w postępowaniu przygotowawczym lub sąd do dostawców usług

łączności o przekazanie danych retencyjnych w trybie art. 218 k.p.k. w toku prowadzonego postępowania karnego.

- **Tryb pozaprocesowy dostępu do danych retencyjnych** – możliwość uzyskania dostępu do danych retencyjnych przez uprawnione podmioty (Policję, Agencję Bezpieczeństwa Wewnętrznego, Centralne Biuro Antykorupcyjne, Służbę Kontrwywiadu Wojskowego, Żandarmerię Wojskową, Krajową Administrację Skarbową, Służbę Ochrony Państwa, Straż Graniczną oraz Generalnego Inspektora Informacji Finansowej) od dostawców usług łączności albo przy zaangażowaniu pracowników dostawców usług łączności albo przy wykorzystaniu mechanizmu stałego łącza.

- **Kontrola uprzednia (kontrola *ex ante*)** – kontrola/weryfikacja legalności, konieczności (celowości) i proporcjonalności dostępu do danych retencyjnych dokonywana przed udostępnieniem danych. Kontrolę *ex ante* powinien sprawować niezależny organ (niekoniecznie sąd).

- **Kontrola następcza (kontrola *ex post*) -** kontrola/weryfikacja legalności, konieczności (celowości) i proporcjonalności dostępu do danych retencyjnych dokonywana po udostępnieniu danych.

- **Notyfikacja** – następcze poinformowanie osoby o pozyskaniu jej danych abonenckich, danych o lokalizacji, danych o ruchu. Notyfikacja może być odłożona w czasie dla zapewnienia prawidłowego toku postępowania lub z uwagi na przeważający interes publiczny.

- **Rozliczalność –** obowiązek stworzenia takiego systemu zabezpieczeń, który umożliwi odtworzenie i przypisanie określonego działania (operacji obejmującej dostęp do danych niedotyczących treści) określonej osobie i umiejscowienie tego zdarzenia w czasie.

I. Wprowadzenie

Dane niedotyczące treści komunikatów przesyłanych drogą elektroniczną są często postrzegane jako *stricte* techniczne i neutralne z punktu widzenia ochrony prywatności. Tymczasem ich gromadzenie i analiza pozwalają na daleko idącą rekonstrukcję aktywności danej osoby, jej relacji społecznych oraz wzorców zachowań, co nadaje im istotny „potencjał ingerencyjny" w sferę prywatności.

Retencja danych telekomunikacyjnych często jest zagadnieniem poruszanym „na uboczu" zagadnień związanych z niejawną inwigilacją. Dostęp, pozyskiwanie i przechowywanie danych niedotyczących treści, tj. nieobejmujących komunikatów przesyłanych drogą elektroniczną przez organy ścigania i służby policyjne (bezpieczeństwa) może wydawać się mniej dolegliwą ingerencją w prawo do prywatności jednostki. Ostatecznie przecież organy państwa nie dysponują treścią komunikatów przesyłanych drogą elektroniczną, a „jedynie" danymi o lokalizacji (gdzie znajdował się użytkownik sieci telekomunikacyjnej), danymi o połączeniach wychodzących i przychodzących (dane z billingów), itp. Informacje o subskrypcjach (np. gazet, podcastów) czy o danych używanych do logowania również nie wydają się czynnością nadmiernie ingerującą w przestrzeń prywatności jednostki. Tymczasem zakres informacji analizowany łącznie dostarcza organom państwa precyzyjnych informacji o życiu danej osoby – o tym, gdzie i jak długo przebywa, z kim się kontaktuje, jakie ma zainteresowania, itp. Informacje te mogą być przechowywane, a następnie – w dogodnym momencie – użyte przeciwko jednostce. Podsłuch – pozyskanie danych dotyczących treści obejmujących treść komunikatów, rozmów, smsów, maili, itp. – jest swoistą „opcją atomową" i najbardziej agresywnym wkroczeniem w sferę prywatności jednostki. Dane o lokalizacji, dane transmisyjne (dane o ruchu), dane IP czy dane abonenckie, to swego rodzaju „*soft inwigilacja*". Patrząc całościowo owa „soft inwigilacja" może być równie dolegliwa dla jednostki, co „klasyczna" niejawna inwigilacja – czyli obejmująca dostęp do komunikatów, rozmów, itp.

Celem opracowania jest ocena obowiązującego modelu retencji danych oraz dostępu do danych niedotyczących treści przekazu przez organy państwa – służby policyjne, służby specjalne, prokuraturę i sądy – z perspektywy zgodności przepisów ustawowych z normami prawnymi wyższego rzędu – normami konstytucyjnymi, konwencyjnymi i prawem unijnym. **Wiąże się to z koniecznością pełnego wykonania wyroku ETPC w**

sprawie Pietrzak i Bychawska-Siniarska i inni przeciwko Polsce[1]. Obecnie, prowadzone są prace legislacyjne nad wdrożeniem tego orzeczenia[2]. Wątek odnoszący się do danych niedotyczących treści przekazu nie został dotychczas poruszony - projekt UD278 odnosi się bowiem do problematyki kontroli operacyjnej[3]. Kwestie dotyczące danych retencyjnych – zatrzymywania i dostępu do nich – mają znaczenie także z uwagi na fakt, że w dniu 16 sierpnia 2026 r. wejdzie w życie rozporządzenie 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[4]. Krajowe rozwiązania dotyczące tej problematyki nie powinny być mniej gwarancyjne dla jednostki i tworzyć swoistej „luki" w unijnym systemie, pozwalając na dalej idące ograniczenia prawa do prywatności.

Stwierdzenie systemowych wadliwości krajowego mechanizmu pozyskiwania danych niedotyczących treści (retencji danych) w wyroku ETPC w sprawie Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce, nie wydaje się być zaskoczeniem. Wcześniej bowiem Najwyższa Izba Kontroli[5], Trybunał Konstytucyjny[6], Rzecznik Praw Obywatelskich[7], a także organizacje społeczne[8] zwracali uwagę na szereg problemów, jakie wiążą się z retencją danych i dostępem do danych internetowych, danych o lokalizacji,

[1] Wyrok ETPC z 28 maja 2024 r. w sprawie *Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce,* skargi nr 72038/17 i 25237/18.

[2] Tak wynika z pisma Ministra Sprawiedliwości z dnia 28 października 2025 r., DPK-I.053.15.2025. Pismo dostępne na stronie: https://bip.brpo.gov.pl/sites/default/files/2025-10/Odpowiedz_MS_kontrola_operacyjna_zasady_28_10_2025.pdf.

[3] Projekt ustawy o zmianie niektórych ustaw w celu wzmocnienia nadzoru sądowego nad kontrolą operacyjną dostępny na stronach Rządowego Centrum Legislacji: https://legislacja.rcl.gov.pl/projekt/12404202.

[4] Dz. U. UE. L. z 2023 r. Nr 191, str. 118.

[5] Zob. raport i informacje prezentowane na konferencji prasowej Najwyższej Izby Kontroli: https://www.nik.gov.pl/najnowsze-informacje-o-wynikach-kontroli/nik-o-billingach.html.

[6] Zob. wyrok TK z dnia 30 lipca 2014 r., K 23/11, OTK-A 2014, nr 7, poz. 80.

[7] Por. m.in. wystąpienie RPO z dnia 13 września 2017 r., VII.520.11.2017.AG, https://bip.brpo.gov.pl/sites/default/files/Wystąpienie%20do%20Ministra%20Spraw%20Zagranicznych%20w%20sprawie%20konieczności%20dostosowania%20prawa%20polskiego%20do%20wymogów%20prawa%20Unii%20Europejskiej%20w%20zakresie%20tzw.%20retencji%20danych%20telekomunikacyjnych.pdf; wystąpienie RPO z dnia 1 lutego 2017 r., VII.501.178.2015.AG, https://bip.brpo.gov.pl/sites/default/files/Wystąpienie%20do%20Ministra%20Spraw%20Wewnętrznych%20i%20Administracji%20w%20sprawie%20ustawy%20inwigilacyjnej%20w%20związku%20z%20wyrokiem%20TSUE%20dotyczącym%20retencji%20danych.pdf. Zob. także stanowisko RPO w sprawie K 23/11 dostępne na stronie: https://ipo.trybunal.gov.pl/ipo/Sprawa?cid=2&sprawa=7533.

[8] Por. m.in. prace Fundacji Panoptykon: https://panoptykon.org/wiadomosc/jak-dziala-ustawa-inwigilacyjna, raport „Rok z ustawą inwigilacyjną": https://panoptykon.org/inwigilacyjna.

połączeniach, itp. Zmiany – w pożądanym kierunku – nie zostały jednak wprowadzone. Tymczasem analiza danych statystycznych w zakresie szeroko rozumianego pozyskiwania danych z bilingów jest alarmująca. Zgodnie z informacją przedstawianą przez Ministra Sprawiedliwości[9], w 2024 r. uprawnione organy[10] w trybie pozaprocesowym[11] sięgały po dane telekomunikacyjne, pocztowe i internetowe 2.143.377. Przeważającą część stanowiły dane telekomunikacyjne – 2.069.901, dane pocztowe – 52.975, a dane internetowe - 20.501. Liczba ta była najwyższa, od kiedy wprowadzono obowiązek publicznego informowania o pozyskiwaniu danych niedotyczących treści. Porównując dane rok do roku (między 2023 r. a 2024 r.), można zauważyć, że ogółem liczba zapytań o dane telekomunikacyjne wzrosła o 13,7%, a między rokiem 2016 a 2024 wzrosła o 82,87%. W tym samym okresie mniej więcej na tym samym poziomie pozostawała liczba prowadzonych przez prokuraturę postępowań karnych[12].

Tabela 1.
– dane niedotyczące treści w latach 2016-2024 pozyskane przez uprawnione organy policyjne i służby specjalne

Rok	Dane telekomunikacyjne	Dane pocztowe	Dane internetowe	Łącznie
2016	1.147.092	1.806	23.150	1.172.048
2017	1.227.314	13.630	23.913	1.264.857
2018	1.325.241	8.601	22.933	1.356.775
2019	1.345.207	8.595	19.526	1.373.328

[9] Druk sejmowy nr 1464; https://sejm.gov.pl/Sejm10.nsf/druk.xsp?nr=1464.
[10] Uprawnione podmioty, które uzyskiwały dane telekomunikacyjne, pocztowe i internetowe w roku 2024 to: Komenda Główna Policji, Komenda Stołeczna Policji, Krajowa Administracja Skarbowa, Komenda Główna Straży Granicznej, Nadwiślański Oddział Straży Granicznej, Agencja Bezpieczeństwa Wewnętrznego, Centralne Biuro Antykorupcyjne, Centralne Biuro Śledcze Policji, Biuro Spraw Wewnętrznych Policji, Biuro Spraw Wewnętrznych Straży Granicznej, Służba Ochrony Państwa, inspektor Nadzoru Wewnętrznego MSWiA, Generalny Inspektor Informacji Finansowej MF, Mazowiecki Urząd Celno-Skarbowy w Warszawie, Służba Kontrwywiadu Wojskowego, Żandarmeria Wojskowa, Inspektorat Wewnętrzny Służby Więziennej oraz Centralne Biuro Zwalczania Cyberprzestępczości.
[11] Tryb procesowy, tj. na podstawie art. 218 k.p.k.
[12] Por. dane statystyczne prezentowane przez Prokuraturę Krajową: https://www.gov.pl/web/prokuratura-krajowa/sprawozdania-i-statystyki. W 2024 r. wpływ spraw wynosił 1.129.566. W 2023 r. – 1.113.206. W 2022 r. - 1.093.318.

2020	1.546.326	13.309	24.959	1.584.594
2021	1.820.630	16.764	20.107	1.857.501
2022	1.787.885	22.283	20.360	1.830.528
2023	1.825.683	38.218	21.062	1.884.963
2024	2.069.901	52.975	20.501	2.143.377

Wzrost liczb bezwzględnych pozyskiwania danych telekomunikacyjnych, pocztowych i internetowych nie jest skorelowany ze wzrostem kontroli sądowych przeprowadzanych w trybie art. 20ca ustawy o Policji[13]. W 2024 r. kontroli było 200 i w żadnej nie stwierdzono nieprawidłowości w pozyskiwaniu danych niedotyczących treści. Rok wcześniej przeprowadzono 254 kontrole – również one wszystkie były pozytywne.

Tabela 2.
– wyniki przeprowadzonych kontroli sądowych w latach 2016-2024

Rok	Ogółem	Pozytywne	Negatywne
2016	121[14]	102	3
2017	71	67	4
2018	82	80	2
2019	107	106	1
2020	163	162	1
2021	136	134	2
2022	241	241	0
2023	254	254	0
2024	200	200	0

[13] Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2025 r. poz. 636 z późn. zm.).
[14] Takie dane przedstawiono w druku nr 1464, nie wskazano, co z pozostałymi 16 kontrolami, które umknęły w wykazie kontroli.

Dodatkowo, obok służb policyjnych i służb specjalnych, dane niedotyczące treści komunikatów przesyłanych drogą elektroniczną mogą być pozyskiwane przez sąd lub prokuratora w trybie art. 218 k.p.k. Zgodnie z informacjami przekazanymi przez Prokuraturę Krajową[15], informacje o liczbie przypadków, kiedy prokurator w trybie procesowym zwraca się o dostęp do danych telekomunikacyjnych, pocztowych lub internetowych, nie są gromadzone. W piśmie w tym wyjaśniono, że „Z uwagi na to, że dane telekomunikacyjne pocztowe i internetowe udostępniane są tylko do konkretnego postępowania, prokuratura nie gromadzi danych odnoszących się do liczby skierowanych zapytań telekomunikacyjnych, pocztowych i internetowych, gdyż są one pozyskiwane jedynie w celu wykrywania i zwalczania przestępstw objętych prowadzonym postępowaniem. Z tego też względu to prokurator referent danego postępowania samodzielnie podejmuje decyzję o zakresie żądanych danych w zależności od procesowych potrzeb. Jak wynika z praktyki prokuratorskiej dane telekomunikacyjne najczęściej obejmują dane abonentów, wykazy rozmów wychodzących i przychodzących, rzadziej dane lokalizacyjne. Dane internetowe dotyczą najczęściej danych abonenta usług internetowych, adresy poczty internetowej czy numerów IP”[16].

W odpowiedzi na pismo Rzecznika Praw Obywatelskich z dnia 8 sierpnia 2025 r.[17], Ministerstwo Sprawiedliwości[18] przekazało informację na temat pozyskiwania przez sądy danych niedotyczących treści w latach 2016-2024.

Tabela 3.
– liczba przypadków, kiedy sądy rejonowe zwracały się o dostęp do danych telekomunikacyjnych, pocztowych lub internetowych w trybie art. 218 k.p.k.

Rok	Łącznie	Dane z billingów	Dane o lokalizacji	Dane identyfikujące użytkowników	Pozostałe sprawdzenia (np. IMEI, przekierowanie połączeń)

[15] Pismo Prokuratury Krajowej z dnia 18 sierpnia 2025 r., 1001-1.071.153.2025.1, w odpowiedzi na zapytanie dotyczące liczby spraw, w których dane telekomunikacyjne zostały pozyskane w trybie z art. 218 k.p.k.
[16] Tak: pismo Prokuratury Krajowej z dnia 18 sierpnia 2025 r., 1001-1.071.153.2025.1, w odpowiedzi na zapytanie dotyczące liczby spraw, w których dane telekomunikacyjne zostały pozyskane w trybie z art. 218 k.p.k. Zob. jednak wywiad z prof. Agnieszką Gryszczyńską, Departamentu ds. Cyberprzestępczości i Informatyzacji Prokuratury Krajowej: https://www.pb.pl/przepisy-o-tajemnicy-bankowej-trzeba-zmienic-1247573.
[17] Pismo z dnia 8 sierpnia 2025 r., II.519.1068.2022.DC.
[18] Pismo z dnia 21 sierpnia 2025 r.; DAiS-II.071.17.2025.

2016	835	216	52	469	98
2017	936	310	79	418	129
2018	971	258	90	496	127
2019	796	181	62	430	123
2020	525	117	48	295	65
2021	551	157	44	264	86
2022	608	141	65	310	92
2023	460	129	39	310	68
2024	468	114	27	251	76

Tabela 4.

– liczba przypadków, kiedy sądy okręgowe zwracały się o dostęp do danych telekomunikacyjnych, pocztowych lub internetowych w trybie art. 218 k.p.k.

Rok	Łącznie	Dane z billingów	Dane o lokalizacji	Dane identyfikujące użytkowników	Pozostałe sprawdzenia (np. IMEI, przekierowanie połączeń)
2016	50	13	5	11	21
2017	56	39	6	8	3
2018	55	11	11	17	16
2019	71	19	9	35	8
2020	29	9	7	8	5
2021	23	10	1	9	3
2022	36	9	6	19	2
2023	28	7	3	10	8
2024	24	5	3	10	6

W kontekście ustalenia skali pozyskiwania danych niedotyczących treści, dane prezentowane publicznie są niepełne i mogą nie oddawać rzeczywistego obrazu. Z jednej strony brakuje informacji dotyczących liczby przypadków, kiedy prokurator – bezpośrednio, na podstawie art. 218 k.p.k. pozyskuje dane internetowe, telekomunikacyjne lub pocztowe. Z drugiej strony, nie można wykluczyć, że dane telekomunikacyjne, internetowe i pocztowe dotyczące jednej osoby za ten sam okres zostały udostępnione kilku podmiotom, skoro dane są prezentowane zbiorczo. Z publicznie dostępnych danych nie wynika także, jaka jest metodologia sporządzania statystyk: czy podaje się informację o tym, ile razy uprawnione podmioty uzyskały dostęp do danych niedotyczących treści, jak jest agregowany wniosek obejmujący np. dane z bilingów kilku osób albo jednej osoby, która posiada więcej niż jeden numer telefonu. Dodatkowo brak jest informacji dotyczącej liczby osób, których dane pozyskano[19]. Stąd też liczby odnoszące się do skali pozyskiwania danych telekomunikacyjnych, internetowych i pocztowych, należy traktować z dużą ostrożnością, bardziej w celu zilustrowania określonych tendencji[20].

Przed przystąpieniem do bardziej szczegółowej analizy warto wyjaśnić, czym jest retencja danych. Retencję danych można zdefiniować jako **ustawowo uregulowany obowiązek przechowywania przez dostawców publicznie dostępnych usług telekomunikacyjnych (usług łączności) oraz operatorów sieci telekomunikacyjnych określonych kategorii danych dotyczących korzystania z tych usług, które nie obejmują treści komunikacji, są wytwarzane w związku z realizacją połączeń lub transmisji danych, dotyczą identyfikacji użytkowników, źródeł i adresatów komunikacji, czasu, miejsca oraz rodzaju połączenia, są przechowywane przez oznaczony w ustawie okres.** Obowiązek zatrzymywania określonych kategorii danych niedotyczących treści należy odróżnić od obowiązku udostępniania ich uprawnionym organom w związku z realizacją przez nie wskazanych w ustawie celów.

---

[19] Na problemy metodologiczne zwracał uwagę NIK w raporcie z 2013 r. Raport NIK, *Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180c i d ustawy Prawo telekomunikacyjne*, KPB-P/12/191, Warszawa 2013, dostępny jest na stronie: https://www.nik.gov.pl/aktualnosci/nik-na-temat-billingow.html.

[20] Na marginesie warto zauważyć, że na etapie opiniowania ustawy z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz. U. poz. 147) GIODO wskazało, że „jak wynika z informacji przygotowanej przez Urząd Komunikacji Elektronicznej, w 2014 r. służby, sądy i prokuratury złożyły łącznie 2 177 916 zapytań o dane telekomunikacyjne. Większa kontrola nad tym procesem pomogłaby zapobiec przypadkom sięgania po dane w sposób automatyczny i tym samym ograniczyć skalę zjawiska"; Opinia Generalnego Inspektora Danych Osobowych do poselskiego projektu ustawy projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk nr 154), s. 3; https://orka.sejm.gov.pl/Druki8ka.nsf/0/9E317D85E84BDE3DC1257F310041F2E8/%24File/154-002.pdf.

Obecnie to, jakie dane podlegają obowiązkowi retencji wynika z art. 47 ustawy - Prawo komunikacji elektronicznej[21] (dalej: p.k.e.). Dodatkowo na podstawie art. 18 ust. 1-5 ustawy o świadczeniu usług drogą elektroniczną[22] oraz art. 82 ust. 1 pkt 1 ustawy - Prawo pocztowe[23] obowiązkowi zatrzymywania podlegają także inne kategorie danych, w tym także dane osobowe, dane związane ze świadczoną usługa drogą elektroniczną[24], czy pocztową[25]. Nie jest to retencja danych w ścisłym tego słowa znaczeniu, chociaż informacja o skali pozyskiwania danych pocztowych i internetowych jest podawana

[21] Ustawa z dnia 12 lipca 2024 r. - Prawo komunikacji elektronicznej (Dz. U. poz. 1221 z późn. zm.).
[22] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2024 r. poz. 1513 z późn. zm.).
[23] Ustawa z dnia 23 listopada 2012 r. Prawo pocztowe (Dz. U. z 2025 r. poz. 366 z późn. zm.).

[24] Zgodnie z art. 18 ust. 1 tej ustawy, możliwe jest przechowywanie i przetwarzanie danych osobowych usługobiorcy niezbędnych do nawiązania, ukształtowania treści, zmiany lub rozwiązania stosunku prawnego między nimi: imienia (imion) i nazwiska usługobiorcy, numeru PESEL (albo numeru paszportu, dowodu osobistego lub numeru innego dokumentu potwierdzającego tożsamość), adresu zameldowania na pobyt stały, adresu do korespondencji, jeśli jest inny niż adres zameldowania, dane służące do weryfikacji podpisu elektronicznego, a także adresy elektroniczne usługobiorcy (adresy mailowe). Dostawca usług internetowych może gromadzić też inne dane (art. 18 ust. 2 ustawy o świadczeniu usług drogą elektroniczną) niezbędne do świadczenia usługi, np. numer konta bankowego, czy karty płatniczej (jeśli usługa elektroniczna wiąże się z płatną subskrypcją), numer telefonu do otrzymywania powiadomień, parametry zakupionego pakietu usługi, historię płatności. Za zgodą użytkownika mogą być przetwarzane także inne dane – zgodnie z art. 18 ust. 4 ustawy o świadczeniu usług drogą elektroniczną – które nie są niezbędne, ale mogą być przydane np. ze względów marketingowych, czy profilowania zachowań użytkownika (np. statystyki użytkowania). Najwięcej wątpliwości z perspektywy zakresu przetwarzania danych w związku ze świadczeniem usług internetowych może pojawić się w związku z art. 18 ust. 5 ustawy o świadczeniu usług drogą. Przepis ten pozwala na gromadzenie danych eksploatacyjnych, tj. dane charakteryzujące sposób korzystania przez usługobiorcę z usługi świadczonej drogą elektroniczną. Dane te umożliwiają ustalenie godziny logowania i wylogowania, czasu trwania sesji, liczby wysłanych e-maili, liczby przesłanych plików, czy też transferu danych. Dane eksploatacyjne nie obejmują natomiast treści przesyłanych drogą elektroniczną (treści wiadomości email), czy historii wyszukiwania. Tak samo jak tytuły – nagłówki – maili, czy adresy URL odwiedzanych stron internetowych zalicza się już do treści komunikacji elektronicznej. Dostęp do tego rodzaju danych powinien być możliwy na podstawie przepisów dotyczących kontroli operacyjnej. Zob. A. Adamski, *Problem retencji danych o ruchu na tle przepisów ustawy - Prawo telekomunikacyjne*, https://panoptykon.org/sites/default/files/FeedsEnclosure-adamski_13.pdf.

[25] Ze wszystkich kategorii danych podlegających retencji, najmniej inwazyjne wydają się dane pocztowe. Zakres danych podlegających zatrzymywaniu obejmuje „uzyskanie danych o operatorze pocztowym, świadczonych usługach pocztowych oraz informacji umożliwiających identyfikację korzystających z tych usług". Chodzi zatem o dane podmiotowe przedsiębiorcę takie jak nazwa operatora (np. Poczta Polska, InPost, DHL), forma prawna prowadzenia działalności pocztowej wraz z siedzibą, a także informację o zakresie działalności. Informacje odnoszące się do „świadczonych usług pocztowych" obejmują rodzaj przesyłki (czy była to przesyła listowa, czy paczka, czy przesyłka zwykła, polecona, czy kurierska), datę nadania i doręczenia przesyłki, numer przesyłki, a także sposób jej doręczenia (czy do rąk własnych, czy do paczkomatu, czy do skrytki pocztowej). Operator pocztowy gromadzi także informacje o nadawcy i odbiorcy przesyłki.

razem z pozyskiwaniem danych telekomunikacyjnych. Dane są gromadzone, co do zasady, na potrzeby świadczonej usługi pocztowej lub internetowej i mogą być udostępniane uprawnionym organom, a nie z uwagi na nałożony przez ustawodawcę obowiązek ich zatrzymywania i przechowywania. Odwrócona jest zatem reguła w przypadku danych telekomunikacyjnych (związanych z łącznością), a danych pocztowych i związanych ze świadczeniem usług internetowych. W przypadku danych telekomunikacyjnych, są one zatrzymywane z uwagi na ustawowy obowiązek, z uwagi na potrzeby państwa/bezpieczeństwa publicznego. Dane pocztowe i związane ze świadczeniem usług drogą elektroniczną, są niezbędne do wykonania usługi i dopiero – jeśli będzie taka potrzeba – mogą zostać udostępnione uprawnionym podmiotom. Z tego powodu, odmiennych celów gromadzenia i zatrzymywania danych[26], przepisy prawa pocztowego i ustawy o świadczeniu usług drogą elektroniczną nie będą analizowane w dalszej części opracowania.

II. Wyrok Trybunału Konstytucyjnego z dnia 30 lipca 2014 r. w sprawie o sygn. K 23/11[27] i jego wykonanie ustawą z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw[28]

II.1. Wyrok Trybunału Konstytucyjnego z dnia 30 lipca 2014 r. w sprawie o sygn. K 23/11

Wyrok Trybunału Konstytucyjnego w sprawie o sygn. K 23/11 jest najczęściej analizowany z perspektywy oceny zgodności z Konstytucją kontroli operacyjnej, a także ogólnych standardów niejawnej inwigilacji[29]. Warto jednak pamiętać, że orzeczenie to

[26] Upraszczając – dane pocztowe i interentowe gromadzi się dlatego, że takie są potrzeby wykonania usługi.
[27] Wyrok TK z dnia 30 lipca 2014 r., K 23/11, OTK-A 2014, nr 7, poz. 80.
[28] Ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz. U. poz. 147).
[29] Zob. szerzej: raport RPO w sprawie wykonania wyroku Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce: www.bip.brpo.gov.pl/sites/default/files/2025-08/Załącznik%20Wykonanie%20wyroku%20Europejskiego%20Trybunału%20Praw%20Człowieka%20w%20sprawie%20Pietrzak%20i%20Bychawska-Siniarska%20i%20inni%20przeciwko%20Polsce.pdf. A także wystąpienie generalne RPO dotyczące tej problematyki dostępne na stronie: https://bip.brpo.gov.pl/pl/content/rpo-kontrola-operacyjna-przepisy-ms-mswia-koordynator-sluzb-odpowiedzi.

dotyczyło także dostępu do danych telekomunikacyjnych[30]. Trybunał Konstytucyjny stwierdził niezgodność m.in. art. 20c ustawy o Policji[31] z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji w zakresie, w jakim nie przewidują niezależnej kontroli udostępniania danych telekomunikacyjnych z art. 180c i 180d[32] ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne[33].

We wniosku inicjującym postępowanie w sprawie o sygn. K 23/11 Rzecznik Praw Obywatelskich[34] - w odniesieniu do uzyskiwania dostępu do danych telekomunikacyjnych – zwrócił uwagę na trzy grupy problemów. Po pierwsze, umożliwienie pozyskiwania danych dla bardzo szeroko określonych celów (w tym dla zapobiegania i wykrywania przestępstw bez względu na ich wagę, a w części regulacji także dla realizacji ogólnie ujętych zadań służb[35]). Po drugie, brak odniesienia się do subsydiarności pozyskania danych telekomunikacyjnych. Przepisy nie uzależniają dostępu od uprzedniego wykorzystania mniej ingerujących metod pozyskania danych/informacji o jednostce. Po trzecie, obowiązujące przepisy nie wprowadzały obowiązku uzyskania zgody sądu albo innego niezależnego organu ani równoważnego mechanizmu zewnętrznej kontroli. Uzupełniając tę argumentację, Prokurator Generalny w swoim stanowisku zwrócił uwagę m.in. na to, że dostęp do danych bywa nieprzydatny dla części wskazanych czynów. W wielu wypadkach dobra chronione penalizacją „drobnych" naruszeń nie uzasadniają tak daleko idącej ingerencji w prywatność i tajemnicę komunikowania się, co świadczy o niewłaściwym wyważeniu kolidujących wartości[36].

---

[30] Poza zakresem kontroli znajdowała się sama retencja. Przedmiotem oceny było jedynie udostępnianie zatrzymanych danych służbom w ramach czynności operacyjno-rozpoznawczych.

[31] A także art. 10b ust. 1 ustawy o Straży Granicznej, art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej, art. 30 ust. 1 ustawy o Żandarmerii Wojskowej; art. 28 ust. 1 pkt 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu; art. 32 ust. 1 pkt 1 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego; art. 18 ust. 1 pkt 1 ustawy o Centralnym Biurze Antykorupcyjnym; art. 75d ust. 1 ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej.

[32] Odpowiednikiem tych przepisów w aktualnie obowiązujących są art. 45 i 49 ustawy Prawo komunikacji elektronicznej.

[33] Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz. U. z 2024 r. poz. 34 z późn. zm.) została zastąpiona ustawą z dnia 12 lipca 2024 r. - Prawo komunikacji elektronicznej (Dz. U. poz. 1221 z późn. zm.).

[34] Stanowisko RPO dostępne na stronie: https://ipo.trybunal.gov.pl/ipo/Sprawa?&pokaz=dokumenty&sygnatura=K%2023/11.

[35] Zob. szerzej uwagi w pkt VII.2.

[36] Stanowisko Prokuratora Generalnego dostępne na stronie: https://ipo.trybunal.gov.pl/ipo/Sprawa?&pokaz=dokumenty&sygnatura=K%2023/11.

W uzasadnieniu wyroku o sygn. K 23/11 Trybunał Konstytucyjny częściowo odniósł się do tych zagadnień, podzielając zastrzeżenia zarówno Rzecznika Praw Obywatelskich jak i Prokuratora Generalnego. Zwracał uwagę m.in. na lakoniczność uregulowań pozwalających uzyskać dostęp do danych zatrzymywanych przez dostawców usług telekomunikacyjnych, brak jasnych przepisów odnoszących się do wykorzystywania danych telekomunikacyjnych jako dowodu w postępowaniu karnym. Problematyczny był także – zdaniem Trybunału Konstytucyjnego – brak subsydiarności w pozyskiwaniu takich danych (tj. służby mogą skorzystać z tej formy działania zawsze, gdy one widzą taką potrzebę) oraz brak odpowiedniej ochrony tajemnic zawodowych. Wskazał jednak, że relatywnie ogólne wskazanie zadań organu władzy publicznej samo w sobie nie jest niezgodne z Konstytucją, ale problem powstaje, gdy w ramach takich zadań organy władzy publicznej mogą podejmować działania ingerujące w wolności i prawa jednostek polegające na niejawnym pozyskiwaniu informacji. Dostrzegając złożoność problemu konstytucyjnego, który sprowadza się do wyważenia ochrony praw jednostki z „dobrem wspólnym", tj. ochroną bezpieczeństwa powszechnego, efektywnym zwalczaniem przestępczości oraz ochroną bezpieczeństwa narodowego, Trybunał podkreślił, że nie da się abstrakcyjnie określić, jaka wartość powinna mieć pierwszeństwo – w takiej sytuacji „punkt ciężkości przesuwa się więc na zapewnienie stosownych gwarancji proceduralnych, eliminujących nieuprawnione pozyskanie przez służby policyjne oraz służby ochrony państwa informacji, które - z uwagi na ich treść i okoliczności przekazania - powinny podlegać ochronie prawnej"[37].

Ostatecznie jednak orzeczenie Trybunału Konstytucyjnego miało węższy zakres i odnosiło się wyłącznie do braku niezależnej kontroli uzyskania/dostępu do danych telekomunikacyjnych[38]. W wyroku Trybunał nie przesądził, jak ma wyglądać procedura dostępu do danych telekomunikacyjnych. Podkreślił jednak, że można rozważyć, w odniesieniu do udostępniania danych telekomunikacyjnych w toku czynności operacyjno-rozpoznawczych - wprowadzenie jako zasady kontroli następczej. „**Regulując ten mechanizm, ustawodawca powinien uwzględnić m.in. specyfikę działania i ustawowy zakres zadań poszczególnych rodzajów służb, sytuacje niecierpiące zwłoki, w których szybkie pozyskanie danych telekomunikacyjnych może być niezbędne dla zapobieżenia popełnieniu przestępstwa lub jego wykrycia.** Zgodnie z konstytucyjną zasadą sprawności działania instytucji publicznych

[37] Wyrok TK z dnia 30 lipca 2014 r., K 23/11, OTK-A 2014, nr 7, poz. 80, pkt 11.7.

[38] W zdaniu odrębnym sędzia Wojciech Hermeliński zwrócił uwagę, że nie wszystkie zarzuty RPO zostały rozpoznane. Zob. pkt 3.1. zdania odrębnego do wyroku TK z 30.07.2014 r., K 23/11, OTK-A 2014, nr 7, poz. 80.

(wstęp do Konstytucji) należy wykreować mechanizm, który umożliwi służbom odpowiedzialnym za bezpieczeństwo państwa i porządek publiczny efektywną walkę z zagrożeniami. **Trybunał dostrzega jednak argumenty za wprowadzeniem kontroli uprzedniej w pewnych wypadkach.** W szczególności chodzić może o dostęp do danych telekomunikacyjnych osób wykonujących zawody zaufania publicznego lub jeśli nie ma konieczności pilnego działania służb. Kwestie te musi jednak odpowiednio wyważyć ustawodawca"[39]. Wyraźnie podkreślił, że kontrola udostępniania danych telekomunikacyjnych nie musi być koniecznie sprawowana przez sądy. Zwracał jedynie uwagę na konieczność, by był to **organ niezależny od rządu i niepozostający z funkcjonariuszami pozyskującymi dane w bezpośredniej lub pośredniej relacji zwierzchności**.

Ustawodawca w uzasadnieniu do projektu ustawy z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw wskazywał, że uchwalone przepisy są implementacją wyroku w sprawie o sygn. K 23/11[40]. Kluczową zmianą było wprowadzenie sądowej kontroli następczej sprawowanej przez, co do zasady, właściwy miejscowo sąd okręgowy[41]. Jednocześnie jednak zmieniono przepisy tak, że Policja i inne służby otrzymały możliwość szerokiego pozyskania danych telekomunikacyjnych na zasadzie „stałego łącza" – tj. bez konieczności zaangażowania dostawców usług telekomunikacyjnych (usług łączności). Najistotniejszą zmianą wprowadzoną równolegle było jednak dodanie przepisów m.in. art. 20cb ustawy o Policji, które umożliwiały uzyskanie dostępu do danych telekomunikacyjnych bez jakiejkolwiek kontroli sądowej. Wprowadzając mechanizm sądowego nadzoru *ex post* ustawodawca jednocześnie skonstruował go w taki sposób, by nie mógł być w pełni efektywny[42].

---

[39] Wyrok TK z dnia 30 lipca 2014 r., K 23/11, OTK-A 2014, nr 7, poz. 80, pkt 10.4.4.

[40] W uzasadnieniu projektu ustawy wskazano, że „realizując pkt 5 wyroku Trybunału Konstytucyjnego w sprawie K 23/11, stwierdzający niezgodność z Konstytucją RP obecnych uregulowań nieprzewidujących niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i 180d ustawy – Prawo telekomunikacyjne, w projekcie ustawy zaproponowano, aby podmiotem uprawnionym do kontroli uzyskiwania danych telekomunikacyjnych został: sąd okręgowy właściwy dla siedziby podmiotu uprawnionego do złożenia wniosku – w odniesieniu do Policji, Straży Granicznej i Służby Celnej, wojskowy sąd okręgowy właściwy dla siedziby organu Żandarmerii Wojskowej, Sąd Okręgowy w Warszawie – w odniesieniu do organu kontroli skarbowej, Agencji Bezpieczeństwa Wewnętrznego i Centralnego Biura Antykorupcyjnego oraz Wojskowy Sąd Okręgowy w Warszawie – w odniesieniu do Służby Kontrwywiadu Wojskowego". Uzasadnienie projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw, druk sejmowy Sejmu VIII kadencji nr 154, s. 13. Uzasadnienie dostępne na stronie: https://www.sejm.gov.pl/Sejm8.nsf/druk.xsp?nr=154.

[41] Zob. art. 20ca ustawy o Policji.

[42] Zob. uwagi w pkt VII.2.

II.2. Opinia Komisji Weneckiej[43] do ustawy z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw

Przepisy wprowadzone ustawą z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw były analizowane przez Komisję Wenecką. W opinii z dnia 13 czerwca 2016 r. zwrócono uwagę na szereg zagrożeń dla prawa do prywatności i nieprawidłowe wyważenie kolidujących interesów, tj. bezpieczeństwa powszechnego i prawa do prywatności.

Po pierwsze, wskazano, że art. 20c ustawy o Policji przyznaje bardzo szeroką swobodę w pozyskiwaniu danych telekomunikacyjnych. Użyta w ustawie o Policji formuła „w celu zapobiegania lub wykrywania przestępstw" oraz cel ratunkowy nie zawęża w dostatecznym stopniu stosowania tego środka do spraw najpoważniejszych. **Zdaniem Komisji Weneckiej, przepis art. 20c ustawy o Policji budzi wątpliwości z perspektywy spełnienia wymogu przewidywalności prawa dla jednostki**[44].

Po drugie, **Komisja Wenecka zaznaczyła, że art. 20c ustawy o Policji nie wprowadza wprost wymogu zastosowania klauzuli subsydiarności oraz „testu prawdopodobieństwa".** Jeśli chodzi o klauzulę subsydiarności, to przepisy nie wprowadzają zastrzeżenia, że dostęp do danych niedotyczących treści jest możliwy wtedy, gdy inne metody były wcześniej wykorzystane lub aby wykazano, że byłyby bezskuteczne. Zwiększa to ryzyko nadużywania sięgania po te dane, a także – zwiększa potrzebę wprowadzenia dodatkowych zabezpieczeń proceduralnych. W odniesieniu do „testu prawdopodobieństwa" problematyczne jest niedookreślenie przesłanek sięgania po dane niedotyczące treści. Nie jest bowiem konieczne ustalenie, że istnieje prawdopodobieństwo popełnienia przestępstwa (albo że przestępstwo trwa albo jest przygotowywane) ani czy pozyskanie danych wniesie istotne informacje do sprawy[45].

Po trzecie, **Komisja Wenecka krytycznie oceniła to, że katalog danych, jakie podlegają retencji, i do jakich mogą mieć następnie dostęp Policja oraz inne służby, prokurator i sąd, jest dopracowywany w rozporządzeniu właściwego ministra**. Stwarza to ryzyko niekontrolowanej ekspansji zakresu danych

[43] Opinia Komisji Weneckiej z dnia 13 czerwca 2016 r. w sprawie ustawy z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw; https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2016)012-e; dalej: opinia Komisji Weneckiej.

[44] Por. pkt 33 Komisji Weneckiej w kwestii rozumienia wymogu przewidywalności prawa oraz pkt 54 Komisji Weneckiej dotyczący niespełnienia tego wymogu przez art. 20c ustawy o Policji.

[45] Por. pkt 49-59 opinii Komisji Weneckiej.

niedotyczących treści przekazu, jakie mogą być pozyskane w trybie art. 20c ustawy o Policji, z zastosowaniem regulacji podustawowej[46].

Po czwarte, „**raportowanie" w okresach 6 miesięcznych do sądu okręgowego nie zapewnia rozliczalności korzystania z dostępu do danych niedotyczących treści.** Raport przekazywany do sądu zawiera informacje zagregowane (rodzaj przestępstwa, liczba spraw, w których zwrócono się o dostęp do danych niedotyczących treści) **i nie daje realnego wglądu w podstawy i proporcjonalność w konkretnych sprawach.** Co prawda sąd może zażądać materiałów uzasadniających pozyskanie danych, ale Komisja wskazała, że mechanizm nie jest skonstruowany tak, by motywował do realnej „indywidualizacji" kontroli[47]. Co więcej, szersza kontrola sądowa jest fakultatywna. Sąd bowiem „może" zażądać materiałów, ale równie dobrze może podjąć decyzję pokontrolną w oparciu o zagregowane informacje.

Po piąte, **mechanizm „stałego łącza", tj. bezpośredniego dostępu do danych niedotyczących treści bez zaangażowania dostawców usług łączności, jest szczególnie podatny na nadużycia**. W ocenie Komisji Weneckiej, model taki nie jest automatycznie zakazany, ale w takiej sytuacji przepisy prawa powinny wprowadzać szczególnie silne zabezpieczenia. Minimalne gwarancje, jakie powinny zostać wprowadzone to: ograniczenie dostępu w formie „stałego łącza" dla wąsko wyznaczonej grupy funkcjonariuszy, pełna identyfikowalność osoby uzyskującej dostęp do danych niedotyczących treści oraz rejestrowanie logowań[48].

W podsumowaniu opinii Komisja Wenecka zaznaczyła, że wiele państw stoi przed problemem odpowiedniego wyważenia interesu jednostki z interesem publicznym. Bardzo realne są zagrożenia ze strony przestępczości zorganizowanej oraz terrorystycznej. Polski ustawodawca nie jest jedynym, który spotkał się z krytyką tego, w jaki sposób wyważony został interes publiczny z interesem prywatnym. W zaleceniach, jakie zostały sformułowane w opinii Komisji Weneckiej, zwrócono uwagę na:

- konieczność wzmocnienia zasady proporcjonalności w pozyskiwaniu danych na podstawie art. 20c ustawy o Policji;

- zobowiązanie Policji do prowadzenia rzetelnej dokumentacji (ewidencji), umożliwiającej skuteczną kontrolę następczą (*ex post*) operacji polegających na

[46] Por. pkt 62 opinii Komisji Weneckiej.
[47] Por. pkt 112-119 opinii Komisji Weneckiej.
[48] Por. pkt 120-125 opinii Komisji Weneckiej.

dostępie do danych niedotyczących treści, w szczególności realizowanych poprzez „stałe łącze";

- zagwarantowanie skutecznego mechanizmu nadzoru nad konkretnymi operacjami pozyskania danych niedotyczących treści, sprawowanego przez niezależny organ; organ ten powinien dysponować niezbędnymi uprawnieniami śledczymi i wiedzą ekspercką oraz mieć możliwość korzystania z adekwatnych środków prawnych[49].

Oceniając prawidłowość wdrożenia wyroku Trybunału Konstytucyjnego w sprawie o sygn. K 23/11[50] można zasadnie twierdzić, że orzeczenie to nie zostało wykonane. Zmiany, które w teorii miały dostosować przepisy ustawowe do wymagań, jakie wynikają z przepisów konstytucyjnych – nawet w wąskim zakresie, w jakim Trybunał rozpoznawał sprawę – nie były zaprojektowane tak, by były one efektywne. Mechanizm kontroli sądowej, będący kluczowym wątkiem w sprawie o sygn. K 23/11, został zaprojektowany tak, by w praktyce sąd nie miał możliwości sprawowania efektywnego nadzoru. Pozostałe rozwiązania wprowadzone ustawą z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw pogłębiły wadliwość pozyskiwania danych o lokalizacji, danych o ruchu i danych abonenckich. Nie tylko nie zmieniły przepisów w pożądanym kierunku, np. wprowadzając klauzulę subsydiarności, czy ograniczając zakres przedmiotowy spraw, w których można pozyskać dane niedotyczące treści, ale zwiększyły wadliwość krajowego systemu – wyłączając część spraw/zapytań spod jakiejkolwiek kontroli sądowej oraz rozbudowując mechanizm bezpośredniego dostępu do danych (mechanizm stałego łącza).

II.3. Konstytucyjny model retencji i dostępu do danych niedotyczących treści – minimalne wymogi regulacji ustawowej

Trybunał Konstytucyjny koncentrował się na kwestii dostępu do danych podlegających retencji i nie oceniał obowiązku zatrzymywania danych jako takiego. W wyroku w sprawie o sygn. K 23/11 podkreślił, że nie jest możliwe abstrakcyjne rozstrzygnięcie, która z wartości – prawa jednostki, czy też cele związane z ochroną bezpieczeństwa powszechnego - powinna mieć pierwszeństwo. W konsekwencji „punkt ciężkości" przesuwa się na zapewnienie takich gwarancji proceduralnych, które będą minimalizowały ryzyko nieuprawnionej ingerencji w sferę prywatności jednostki.

[49] Por. pkt 131 opinii Komisji Weneckiej.

[50] Zob. także: B. Grabowska-Moroz, *Ochrona gromadzonych danych telekomunikacyjnych i zasady ich udostępniania na tle Konstytucji RP i prawa Unii Europejskiej. Glosa do wyroku TS z dnia 8 kwietnia 2014 r., C-293/12 i C-594/12 oraz do wyroku TK z dnia 30 lipca 2014 r., K 23/11*, EPS 2016, nr 1, s. 31-36.

Najważniejszym elementem chroniącym przed nadużyciami, jest istnienie zewnętrznej, niezależnej kontroli udostępniania danych telekomunikacyjnych. Nie musi być sprawowana wyłącznie przez sądy, ale organ kontrolujący musi mieć odpowiednie gwarancje niezależności – tj. być niezależny od władzy wykonawczej i apolityczny oraz nie pozostawać z funkcjonariuszami pozyskującymi dane w relacji zwierzchności (np. organem kontrolnym nie może być Komendant Główny Policji, itp.).

Chociaż nie znalazło to odzwierciedlenia w sentencji wyroku Trybunału Konstytucyjnego, to z analizy uzasadnienia orzeczenia w sprawie o sygn. K 23/11, jak i z opinii Komisji Weneckiej wynika, że niezbędne jest ograniczenie dowolności w sięganiu po dane telekomunikacyjne przez dostatecznie precyzyjne określenie celów sięgania po te dane, jak i przesłanek. Komisja Wenecka także zwróciła uwagę, że bardzo szerokie formuły celu (np. odnoszące się ogólnie do „zapobiegania lub wykrywania przestępstw") mogą nie spełniać wymogu przewidywalności dla jednostki, jeżeli nie zawężają stosowania środka do spraw najpoważniejszych albo nie wprowadzają dodatkowych wymogów/przesłanek uprawniających do uzyskania dostępu do danych niedotyczących treści (np. zwalczanie przestępczości internetowej/przestępstw popełnianych przy wykorzystaniu środków komunikowania się na odległość).

Regulacje ustawowe powinny uwzględniać zasadę subsydiarności i uzewnętrzniać ją w konkretnych regulacjach. Sięgnięcie po dane niedotyczące treści, w szczególności po dane o lokalizacji i dane transmisyjne (dane o ruchu) powinno następować wówczas, gdy inne, mniej ingerujące środki, okazały się niewystarczające lub byłyby bezskuteczne. Komisja Wenecka zwróciła również uwagę na potrzebę doprecyzowania przesłanek dostępu poprzez wprowadzenie „testu prawdopodobieństwa" (w rozumieniu konieczności określenia czy istnieją dostateczne podstawy wskazujące na związek z przestępstwem oraz czy pozyskanie danych może wnieść istotne informacje do sprawy), tak aby dostęp do danych nie był środkiem rutynowym.

Komisja Wenecka zwracała również uwagę na konieczność uregulowania w ustawie – a nie w akcie podustawowym (rozporządzeniu) – katalogu danych, do których organy mogą uzyskać dostęp, Ustawodawca powinien określić wprost, jakie kategorie danych niedotyczących treści mogą być objęte obowiązkami zatrzymywania i udostępniania oraz jakie są granice ich pozyskiwania, aby uniknąć niekontrolowanej ekspansji zakresu ingerencji poprzez regulację wykonawczą.

W odniesieniu do mechanizmów kontrolnych, zwłaszcza kontroli następczej, Komisja Wenecka podkreśliła, że muszą one umożliwiać realną weryfikację legalności,

zasadności i celowości pozyskania danych, a nie ograniczać się do informacji zagregowanych. W tym kontekście Trybunał Konstytucyjny zwrócił uwagę na problem braku odpowiedniej ochrony tajemnic zawodowych oraz zaakcentował, że mogą istnieć kategorie sytuacji, w których argumenty przemawiają za kontrolą uprzednią – w szczególności w odniesieniu do dostępu do danych osób wykonujących zawody zaufania publicznego. Przedstawienie wyłącznie zagregowanych danych, uniemożliwia zweryfikowanie, czy np. dane lokalizacyjne nie zostały powiązane z danymi abonenckimi, by ujawnić dziennikarskie źródła informacji, czy tożsamość sygnalistów.

Komisja Wenecka wskazała również, że rozwiązania oparte na stałym i bezpośrednim dostępie do danych bez udziału dostawcy usług łączności są szczególnie podatne na nadużycia i – jeżeli prawo krajowe taki mechanizm przewiduje – wymagają wzmocnionych zabezpieczeń. Jak to zostało wcześniej wskazane, w modelowym ujęciu minimalne gwarancje obejmują: ograniczenie dostępu do wąsko określonej grupy funkcjonariuszy, pełną identyfikowalność osoby uzyskującej dostęp oraz obowiązek rejestrowania logowań i operacji, tak aby możliwy był skuteczny audyt/realna rozliczalność.

III. Prawo unijne – retencja danych oraz możliwość udostępnienia danych w związku z podejrzeniem popełnienia przestępstwa

III.1. Zasada poufności komunikacji w dyrektywie 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej

Przepis art. 5 dyrektywy 2002/58[51] wprowadza zasadę poufności komunikacji[52]. Odstępstwa od tej zasady są możliwe dla zapewnienia bezpieczeństwa narodowego, bezpieczeństwa państwa, obronności, bezpieczeństwa publicznego oraz w celu wykrywania, dochodzenia i karania przestępstw kryminalnych (art. 15 dyrektywy 2002/58[53]). Klauzula ograniczająca poufność m.in. danych o lokalizacji, danych o ruchu ma charakter wyczerpujący i nie podlega rozszerzającej interpretacji. Dopuszczalne jest zatrzymywanie danych o ruchu, danych o lokalizacji, danych abonenckich, ale pod

[51] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz. U. UE. L. z 2002 r. Nr 201, str. 37 z późn. zm.); dalej: dyrektywa 2002/58.

[52] Przepis ten brzmi: Państwa Członkowskie zapewniają, poprzez ustawodawstwo krajowe, poufność komunikacji i związanych z nią danych o ruchu za pośrednictwem publicznie dostępnej sieci łączności i publicznie dostępnych usług łączności elektronicznej. W szczególności zakazują słuchania, nagrywania, przechowywania lub innych rodzajów przejęcia lub nadzoru komunikatu i związanych z nim danych o ruchu przez osoby inne niż użytkownicy, bez zgody zainteresowanych użytkowników, z wyjątkiem upoważnienia zgodnego z art. 15 ust. 1. Niniejszy ustęp nie zabrania technicznego przechowywania, które jest niezbędne do przekazania komunikatu bez uszczerbku dla zasady poufności.

[53] Przepis art. 15 ust. 1 dyrektywy 2002/58 brzmi: Państwa Członkowskie mogą uchwalić środki ustawodawcze w celu ograniczenia zakresu praw i obowiązków przewidzianych w art. 5, 6, art. 8 ust. 1-4, i art. 9 tej dyrektywy, gdy takie ograniczenia stanowią środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego/bezpieczeństwa państwa, obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej, jak określono w art. 13 ust. 1 dyrektywy 95/46/WE. W tym celu, Państwa Członkowskie mogą, między innymi, uchwalić środki ustawodawcze przewidujące przechowywanie danych przez określony czas uzasadnione na podstawie zasad ustanowionych w niniejszym ustępie. Wszystkie środki określone w niniejszym ustępie są zgodne z ogólnymi zasadami prawa wspólnotowego, w tym zasadami określonymi w art. 6 ust. 1 i 2 Traktatu o Unii Europejskiej.

warunkiem, że celem tego działania jest walka z przestępczością[54]. Dane te mogą być przekazane (udostępniane) organom państwa (np. Policji, prokuraturze) na zasadach – i przy zachowaniu gwarancji praw jednostki – określonych w dyrektywie 2016/680[55]. **Udostępnianie (dostęp) jest dopuszczalny w celach wskazanych w art. 15 ust. 1 dyrektywy 2002/58, przede wszystkim w celu ochrony bezpieczeństwa narodowego czy zwalczania poważnej przestępczości, przy spełnieniu wymogów konieczności i proporcjonalności**. **Co do zasady, na wniosek danej osoby należy udzielić informacji, czy jej dane osobowe były przetwarzane przez służby policyjne [56], a także może ona żądać usunięcia swoich danych, jeśli są nieprzydatne dla realizacji celów, o których mowa w dyrektywie lub są nieaktualne albo pozyskano je niezgodnie z prawem[57].** Kontrolę nad prawidłowością przetwarzania danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości powinien sprawować niezależny organ, a jednostka – jeśli jej dane nie zostały usunięte mimo żądania lub uznaje, że są przetwarzane niezgodnie z prawem – może skierować sprawę na drogę sądową[58].

Regulacje unijne nie określają jednak, w jakich sprawach można pozyskiwać dane o ruchu, dane lokalizacyjne, dane abonenckie i inne dane niedotyczące treści przekazu ani nie wskazują (wprowadzając konkretne terminy przechowywania danych), jak długo te dane mogą być przechowywane[59]. Przepis art. 15 dyrektywy 2002/58 umożliwia państwom członkowskim wprowadzenie w prawie krajowym

---

[54] Opinia Rzecznika Generalnego z dnia 15 stycznia 2020 r., C-520/18. Opinia dostępna na stronie: https://infocuria.curia.europa.eu/tabs/jurisprudence?sort=DOC_DATE-DESC&searchTerm=%22C-520%2F18%22.

[55] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. U. UE. L. z 2016 r. Nr 119, str. 89 z późn. zm.).

[56] Zob. art. 13 i 14 dyrektywy 2016/680. Ograniczenia tego prawa – zob. art. 15 dyrektywy 2016/680. Z urzędu informuje się osobę, jeśli naruszenie danych osobowych niesie za sobą zagrożenie dla życia, zdrowia lub bezpieczeństwa tej osoby. Zob. art. 31 dyrektywy 2016/680.

[57] Zob. art. 16 dyrektywy 2016/680.

[58] Zob. art. 17 ust. 3 dyrektywy 2016/680.

[59] Tzw. dyrektywa retencyjna wprowadzała możliwość przechowywania danych do lat 2 (zob. art. 6 dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE; Dz. U. UE. L. z 2006 r. Nr 105, str. 54). Wyrokiem TSUE z dnia 8 kwietnia 2012 r. w sprawie Digital Rights Irleand, C-293/12, stwierdził nieważność dyrektywy. Zob. także: A. Grzelak, *Granica między skuteczną walką z przestępczością a prawem do prywatności i do ochrony danych osobowych. Glosa do wyroku TS z dnia 8 kwietnia 2014 r., C-293/12 i C-594/12*, EPS 2014, nr 7, s. 45-52.

środków ograniczających poufność, w tym rozwiązania odnoszące się do retencji danych, a także dostępu przez organy ścigania do tych danych, w celu zwalczania poważnej przestępczości. Jeśli dane zostały przekazane organom ścigania, art. 5 dyrektywy 2016/680 wymaga, by państwa Unii wprowadziły „odpowiednie terminy usuwania danych osobowych lub okresowego przeglądu konieczności przechowywania danych osobowych". **Prawodawca unijny pozostawił państwom członkowskim margines swobody w uregulowaniu tego zagadnienia, tj. tego w jakich sprawach i w jakim celu będą gromadzone dane, a także przez jaki okres będą one przechowywane.** Swoboda implementacyjna państw członkowskich jest jednak kontrolowana przez Trybunał Sprawiedliwości UE.

III.2. Orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej – wyjątki od zasady poufności komunikacji elektronicznej w związku z zapobieganiem i zwalczaniem przestępstw oraz ochroną bezpieczeństwa narodowego

III.2.1. Wyrok TSUE z dnia 21 grudnia 2016 r., C-203/15 i C-698/15, Tele2 i Watson

W wyroku w sprawie Tele2 i Watson[60], TSUE oceniał przepisy obowiązujące w Szwecji oraz Zjednoczonym Królestwie. Prawo ówcześnie obowiązujące w Szwecji obligowało dostawcę usług łączności elektronicznej do przekazania – na żądanie prokuratury, policji lub innego organu odpowiedzialnemu za zwalczanie przestępczości – danych abonenta, jeśli odnosiły się one do domniemanego naruszenia prawa, przy czym przedmiotem postępowania karnego nie musiało być „poważne przestępstwo"[61]. Rozwiązania przyjęte w Zjednoczonym Królestwie nie precyzowały zakresu przedmiotowego dostępu do danych o lokalizacji[62]. Organ powołany do zapobiegania i zwalczania przestępstw miał prawo zwrócić się do operatora sieci komórkowej z żądaniem udostępnienia danych ze względu na: bezpieczeństwo narodowe, interes gospodarczy państwa, ochronę zdrowia publicznego, konieczność zapobiegania lub wykrywania przestępstw lub zapobiegania naruszeniom porządku publicznego,

[60] Wyrok TSUE z dnia 21 grudnia 2016 r., C-203/15 i C-698/15. Sądy skierowały pytania prejudycjalne po tym jak TSUE w wyroku Digital Rights Ireland stwierdził nieważność tzw. dyrektywy retencyjnej, a regulacje obowiązujące w Szwecji i Zjednoczonym Królestwie w związku z którymi skierowano pytanie prejudycjalne, było implementacją powyższej dyrektywy. Zob. także: A. Grzelak, *Trybunał Sprawiedliwości ponownie o relacji między koniecznością zwalczania przestępczości a prawem do prywatności. Glosa do wyroku TS z dnia 21 grudnia 2016 r., C-203/15 oraz C-698/15*, EPS 2017, nr 3, s. 31-36.

[61] Zob. pkt. 25 wyroku TSUE z dnia 21 grudnia 2016 r., Tele2 i Watson, C-203/15 i C-698/15. Treść pytania sądu szwedzkiego zob. pkt 51 wyroku TSUE z dnia 21 grudnia 2016 r., C-203/15 i C-698/15.

[62] Zob. wyrok TSUE z dnia 21 grudnia 2016 r., Tele2 i Watson, C-203/15 i C-698/15, pkt 33. Pytania prejudycjalne sądu Zjednoczonego Królestwa: zob. pkt. 59.

określenia wymiaru lub poboru podatków, danin, opłat lub innych zobowiązań, składek lub obciążeń należnych jednostce administracji państwowej, a także w nagłych przypadkach, w celu zapobieżenia obrażeniom lub szkodzie na zdrowiu fizycznym lub psychicznym człowieka albo zmniejszeniu rozmiaru szkody na zdrowiu fizycznym lub psychicznym człowieka. Ponadto minister spraw wewnętrznych mógł zarządzeniem określić inne sytuacje, w których organy państwa mogły uzyskać dostęp do danych o lokalizacji.

W wyroku Tele2 i Watson Trybunał Sprawiedliwości UE przypomniał, że wynikająca z art. 5 dyrektywy 2002/58 **ochrona poufności łączności elektronicznej ma na celu uniemożliwienie każdego niezgodnego z prawem dostępu do danych, w tym danych związanych z komunikatem[63], niezależnie od tego, czy dostęp ten mogłyby uzyskać podmioty publiczne (państwowe) czy prywatne.** Przepisy nakładające na dostawców usług telekomunikacyjnych obowiązek przekazania danych mieszczą się w zakresie art. 5 dyrektywy 2002/58. W analizowanym orzeczeniu Trybunał luksemburski sformułował ogólne zasady retencji danych, w tym także danych o lokalizacji, a następnie przekazania ich organom procesowym. Po pierwsze**, w prawie krajowym powinny zostać wprowadzone jasne i precyzyjne reguły dotyczące zakresu i sposobu stosowania środka związanego z przechowywaniem danych**. Ocena, czy istnieje np. realne zagrożenie dla bezpieczeństwa narodowego, należy do państw członkowskich UE. Trybunał ocenia jednak, czy obowiązujące w danych państwie prawo nie pozwala na nieuprawnioną i nieproporcjonalną ingerencję w prawo do prywatności jednostki[64]. Po drugie, **retencja danych musi być prowadzona w oparciu o obiektywne kryteria, wskazujące na związek między danymi, które zostały zatrzymane, a uprawnionym celem, któremu to zatrzymanie ma służyć**. Po trzecie, te **kryteria muszą umożliwić identyfikację i namierzenie osób, które mają – choćby pośredni – związek z poważną przestępczością**. Niezgodne z prawem unijnym są regulacje krajowe, które zapewniają powszechny dostęp do zatrzymywanych danych, niezależnie od istnienia jakiegokolwiek związku z jednym z celów wskazanych w art. 15 dyrektywy 2002/58. **Uogólniony i niezróżnicowany obowiązek zatrzymywania wszystkich danych dotyczących ruchu i lokalizacji wszystkich abonentów i użytkowników w nieproporcjonalny sposób narusza prawa podstawowe z art. 7, 8 i 11 Karty Praw Podstawowych UE**[65]. Użytkownicy sieci telekomunikacyjnych nie mogą być pod stałym nadzorem państwa i nie powinni się

[63] Wyrok TSUE z dnia 21 grudnia 2016 r., Tele2 i Watson, C-203/15 i C-698/15, pkt 77.
[64] Wyrok TSUE z dnia 21 grudnia 2016 r., Tele2 i Watson, C-203/15 i C-698/15, pkt 94-96.
[65] Por. również: Opinia Rzecznika Generalnego z dnia 15 stycznia 2020 r., C-520/18; pkt. 72.

obawiać, że każdy ich ruch jest śledzony, rejestrowany i może być w przyszłości wykorzystany przeciwko nim. Ponadto, konieczne jest wprowadzenie terminu przechowywania danych o lokalizacji – niedopuszczalne jest przechowywanie informacji o jednostce dłużej niż jest to niezbędne dla zapewnienia bezpieczeństwa publicznego[66].

W odpowiedzi na pytania prejudycjalne Trybunał Sprawiedliwości UE zakwestionował rozwiązania obowiązujące w Szwecji i Zjednoczonym Królestwie i orzekł, że artykuł 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8, 11 i art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej, należy interpretować w ten sposób, że stoi on na przeszkodzie uregulowaniu krajowemu:

- przewidującemu do celów zwalczania przestępczości uogólnione i niezróżnicowane zatrzymywanie wszystkich danych o ruchu oraz danych dotyczących lokalizacji wszystkich abonentów i zarejestrowanych użytkowników wszystkich środków łączności elektronicznej; oraz

- dotyczącego ochrony i bezpieczeństwa danych o ruchu i danych o lokalizacji, a w szczególności dostępu właściwych organów władz krajowych do przechowywanych danych, które to przepisy, w ramach zwalczania przestępczości, nie ograniczającego tego dostępu jedynie do celów walki z poważną przestępczością, nie uzależniającego przyznania tego dostępy od uprzedniej kontroli sprawowanej przez sąd lub niezależny organ administracyjny i nie ustanawiają wymogu, aby dane te były przechowywane na obszarze Unii.

III.2.2. Wyrok TSUE z dnia 6 października 2020 r. w sprawie Privacy International, C-623/17

Zagadnienie pozyskiwania dostępu do danych o ruchu (danych o lokalizacji, danych z bilingów) było rozstrzygane także w sprawie Privacy International[67]. Podstawą do wystąpienia przez sąd brytyjski z pytaniem prejudycjalnym[68] była wątpliwość, czy przepisy pozwalające masowo pozyskiwać dane telekomunikacyjne dotyczące ruchu i lokalizacji od operatorów sieci telekomunikacyjnych[69] na podstawie poleceń wydawanych przez sekretarza stanu, aby wykorzystać tak zgromadzone informacje w

[66] Zob. wyrok TSUE z dnia 6 października 2020 r., Privacy International, C-623/17, pkt. 108-111
[67] Wyrok TSUE z dnia 6 października 2020 r., Privacy International, C-623/17.
[68] Treść pytania prejudycjalnego: zob. wyrok TSUE z dnia 6 października 2020 r., Privacy International, C-623/17, pkt 29.
[69] Dane gromadziły brytyjskie służby specjalne, m.in. MI5 i MI6. Zob. wyrok TSUE z dnia 6 października 2020 r., Privacy International, C-623/17, pkt 20.

celu zapewnienia bezpieczeństwa państwowego[70] są zgodne z prawem unijnym[71]. Przepisy brytyjskie pozwalały na niezróżnicowany i uogólniony dostęp do danych o lokalizacji i danych o ruchu/danych transmisyjnych. Aby informacje zostały przekazane organom służb bezpieczeństwa nie było konieczności wykazania, że dana osoba miała związek z działalnością, która mogła stanowić zagrożenie dla bezpieczeństwa narodowego.

TSUE przypomniał, że każda ingerencja w prywatność jednostki musi spełniać warunek proporcjonalności[72]. **Ograniczenie prywatności może następować w ściśle określonych granicach oraz tylko wtedy, gdy jest to konieczne dla realizacji uprawnionego celu (np. zapewnienia bezpieczeństwa publicznego, zwalczania przestępczości)[73]. Do realizacji tych celów nie można dążyć za wszelką cenę, tj. bez uwzględnienia i poszanowania praw jednostki[74].** Regulacje prawne, pozwalające na wkroczenie w prywatność jednostki muszą spełniać warunki określoności, tj. wskazywać podstawy i zakres ograniczenia (tj. jakie dane będą przetwarzane) oraz przewidywać gwarancje proceduralne, które zmniejszą ryzyko nadużyć. Chodzi o stworzenie efektywnych mechanizmów, które zapewnią, że dane będą przetwarzane tylko w zakresie, w jakim to jest niezbędne[75]. Warto jednak podkreślić, że **TSUE wskazał, iż cel w postaci zapewnienia bezpieczeństwa narodowego (publicznego) pozwala na dalej idące ograniczenia praw podstawowych niż zwalczanie przestępczości, w tym także poważnych przestępstw. Organy państwa muszą dysponować**

[70] Por. wyrok TSUE z dnia 6 października 2020 r., Privacy International, C-623/17, pkt. 16-18. Rządy: brytyjski, węgierski, polski i czeski zgłosiły zastrzeżenia, wskazując, że bezpieczeństwo narodowe jest wyłączną sprawą państw członkowskich i nie mieści się w zakresie dyrektywy 2002/58, zatem TSUE nie ma w tym zakresie kompetencji do orzekania. Por. także: wyrok z dnia 6 października 2020, La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, pkt 87-103.

[71] Tj. dyrektywą 2002/58.

[72] Kwestię proporcjonalności ingerencji w prawo do prywatności – w odniesieniu do danych użytkownika telefonu/abonenta – TSUE analizował w wyroku w sprawie Ministero Fiscal. Zob. wyrok TSUE z dnia 2 października 2018 r., Ministerio Fiscal, C - 207 / 16, pkt 55. Ingerencja w prawa jednostki może zostać uznana za proporcjonalną, jeśli ze względu na wagę przestępstwa, okoliczności sprawy, bardziej korzystne – z perspektywy ogółu społeczeństwa – jest ograniczenie praw jednostki.

[73] Wyrok TSUE z dnia 6 października 2020 r., Privacy International, C-623/17, pkt 77.

[74] Należy odpowiednio wyważyć interes prywatny i interes ogółu społeczeństwa. Nie można z góry zakładać, że zapewnienie porządku publicznego i bezpieczeństwa powszechnego w każdym przypadku przewyższa prawa i wolności jednostki. Zob. wyrok TSUE z dnia 6 października 2020 r., Privacy International, C-623/17, pkt 67, a także z dnia 8 kwietnia 2014 r., Digital Rights Ireland i in., C-293/12 i C-594/12, pkt 52.

[75] Wyrok TSUE z dnia 6 października 2020 r., Privacy International, C-623/17, pkt 68 i wskazane tam orzecznictwo. Zob. także: wyrok TS UE z dnia 6 października 2020 r., Privacy International, C-623/17, pkt 74 oraz wyrok z dnia 6 października 2020, La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, pkt 132.

adekwatnymi i skutecznymi metodami pozyskiwania informacji o ewentualnych zagrożeniach, mogących zdestabilizować działalność państwa – struktury konstytucyjne, polityczne lub społeczne w kraju – oraz bezpośrednio zagrozić społeczeństwu i ludności[76]. **Dążenie do zapewnienia bezpieczeństwa narodowego nie pozwala jednak na ogólne, powszechne i niezróżnicowane gromadzenie i przetwarzanie danych o lokalizacji**. W odpowiedzi na pytanie sądu brytyjskiego Trybunał luksemburski stwierdził niezgodność przepisów obowiązujących w Zjednoczonym Królestwie z prawem unijnym. Wskazał bowiem, że art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 4 ust. 2 TUE, a także art. 7, 8 i 11 oraz 52 ust. 1 Karty praw podstawowych Unii Europejskiej „należy interpretować w ten sposób, że stoi on na przeszkodzie uregulowaniu krajowemu umożliwiającemu organowi państwa nałożenie na dostawców usług łączności elektronicznej obowiązku uogólnionego i niezróżnicowanego transmitowania służbom wywiadu i bezpieczeństwa danych o ruchu i danych o lokalizacji do celów ochrony bezpieczeństwa narodowego".

III.2.3. Wyrok TSUE z dnia 6 października 2020 r., w sprawie La Quadrature du Net i inni, C-511/18, C-512/18, C-520/18

Problem masowego pozyskiwania danych o ruchu i lokalizacji był także analizowany w wyroku La Quadrature du Net i inni[77]. W tym postępowaniu Trybunał luksemburski badał przepisy francuskie i belgijskie, które dopuszczały możliwość prewencyjnego zatrzymywania danych o ruchu i lokalizacji w celu zapewnienia bezpieczeństwa powszechnego i zapobieżenia poważnym przestępstwom[78]. Jednak nawet jeśli dane o lokalizacji są prewencyjnie zatrzymywane w celu zapewnienia bezpieczeństwa narodowego, takie działania organów państwa muszą być ograniczone do tego, co jest absolutnie koniecznie. Niezbędne jest wprowadzenie ograniczeń (np. przez ustalenie zakresu podmiotowego i temporalnego) i zabezpieczeń, które umożliwią skuteczną ochronę danych osób, wobec których dane zostały udostępnione organom państwa,

[76] Chodzi m.in. o działalność terrorystyczną. Zob.: wyrok TSUE z dnia 6 października 2020 r., Privacy International, C-623/17, pkt 74 oraz wyrok z dnia 6 października 2020, La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, pkt 135.

[77] Wyrok TSUE z dnia 6 października 2020 r., C-511/18, C-512/18, C-520/18, La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net (dalej: La Quadrature du Net i inni).

[78] Jednym z pozytywnych obowiązków państwa wynikających z art. 8 EKPC oraz art. 7 KPP jest bowiem wprowadzenie odpowiednich przepisów materialnych i proceduralnych pozwalających skutecznie zwalczać poważną przestępczość i zapewnić bezpieczeństwo powszechne.

przed ryzykiem nadużyć[79]. Niedopuszczalne jest systematyczne, ciągłe i nieograniczone żadnym terminem zatrzymywanie danych o lokalizacji. Ponadto, **decyzje zobowiązujące dostawców usług łączności elektronicznej do zatrzymania danych o lokalizacji i danych o ruchu, a następnie przekazania ich organom państwa, powinny podlegać skutecznej kontroli sądu lub niezależnego organu administracyjnego, którego będzie miał możliwość oceny legalności działań podjętych przez organy procesowe**[80]. W odniesieniu do realizacji celu w postaci zapewnienia bezpieczeństwa powszechnego TSUE dopuścił – pod wskazanymi wyżej warunkami - prewencyjne zatrzymywanie i gromadzenie danych o lokalizacji. **Natomiast masowe, prewencyjne zatrzymywanie danych o lokalizacji i danych o ruchu w celu zapobiegania przestępstwom, prowadzenia dochodzeń, wykrywania i ścigania przestępstw jest niedopuszczalne. Trybunał stwierdził, że ustawodawstwo krajowe, które przewiduje ogólne i niezróżnicowane zatrzymywanie tych danych, wykracza poza to, co jest konieczne w celu zwalczania poważnej przestępczości i nie może być uzasadnione w społeczeństwie demokratycznym**[81]. Przepisy francuskie i belgijskie pozwalały na zatrzymywanie danych o lokalizacji wszystkich osób korzystających z usług łączności elektronicznej, nawet jeśli nie znajdowały się – choćby pośrednio – w sytuacji, która mogłaby skutkować wszczęciem przeciwko nim postępowania karnego. Regulacje te obejmowały swoim zakresem także osoby, których zachowania nie powodowały żadnego zagrożenia dla bezpieczeństwa publicznego[82]. Nie ma znaczenia, czy zatrzymane dane zostały wykorzystane w późniejszym postępowaniu karnym. Ważne jest to, że organy procesowe wkroczyły w sferę prywatności jednostki, naruszając poufność komunikowania się, wyrażoną w art. 5 dyrektywy 2002/58[83]. **Sama możliwość dostępu do danych osobowych jest ingerencją w prawo do prywatności**.

---

[79] Wyrok TSUE z dnia 6 października 2020 r., C-511/18, C-512/18, C-520/18, La Quadrature du Net, pkt 138.

[80] Wyrok TSUE z dnia 6 października 2020 r., C-511/18, C-512/18, C-520/18, La Quadrature du Net, pkt 139. Zob. także: A. Grzelak, K. S. Zielińska, *Między prawem do prywatności i ochrony danych osobowych a zapewnieniem bezpieczeństwa publicznego i walką z przestępczością. Problemu retencji danych ciąg dalszy. Glosa do wyroku TS z dnia 6 października 2020 r., C-623/17, C-511/18, C-512/18 oraz C-520/18*, EPS 2021, nr 8, s. 28-36.

[81] Wyrok TSUE z dnia 6 października 2020 r., C-511/18, C-512/18, C-520/18, La Quadrature du Net, pkt 141.

[82] Wyrok TSUE z dnia 6 października 2020 r., C-511/18, C-512/18, C-520/18, La Quadrature du Net, pkt 143.

[83] Wyrok TSUE z dnia 6 października 2020 r., C-511/18, C-512/18, C-520/18, La Quadrature du Net, pkt 116.

III.2.4.Wyrok TSUE z dnia 2 marca 2021 r., H.K. przeciwko Prokuratuur, C-746/18[84]

Kolejny raz problematyką retencji danych przez dostawców usług łączności i udostępniania ich organom państwa TSUE zajmował się w sprawie C-746/18, Prokuratuur[85]. Pytanie prejudycjalne zadał sąd estoński, który miał wątpliwość odnośnie do dowodowego wykorzystania w postępowaniu protokołów sporządzonych na podstawie danych niedotyczących treści pozyskanych od dostawców usług łączności. Przepisy estońskie nakładały na dostawców tych usług obowiązek zatrzymywania szerokiego zakresu danych niedotyczących treści[86] niezależnie od tego, czy istniało wobec danej osoby podejrzenie popełnienia przestępstwa[87]. Organy procesowy mogły pozyskać dane niedotyczące treści na potrzeby postępowania karnego w celu zwalczania i zapobiegania przestępstw, niezależnie od wagi czynu zabronionego[88]. Dodatkowo sąd estoński zwrócił się do TSUE o rozstrzygnięcie, czy prokuratura może zostać uznana za „niezależny organ administracyjny" dokonujący kontroli uprzedniej zasadności zwrócenia się do dostawców usług łączności o dane o ruchu, dane o lokalizacji, itp.

W odniesieniu do kwestii obowiązku zatrzymywania danych przez dostawców usług łączności, Trybunał luksemburski w zasadzie powtórzył (przypomniał) to, co wynika z wcześniej analizowanych orzeczeń. Odwołując się przede wszystkim do wyroków w sprawach *Privacy International* i *La Quadrature du Net* wskazał, że art. 15 ust. 1 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 KPP UE[89] „**stoi na przeszkodzie środkom ustawodawczym przewidującym w tych celach prewencyjne uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych o lokalizacji**"[90]. Analizując możliwość uzyskania dostępu przez organy procesowe do danych zatrzymywanych przez operatorów usług łączności, Trybunał Sprawiedliwości UE przypomniał, że taki dostęp może być wyłącznie uzasadniony względami zapobiegania,

[84] Zob. także wystąpienie generalne dotyczące tego wyroku z dnia 31 marca 2021 r., II.519.109.2015.MM. Wystąpienie generalne dostępne na stronie: https://bip.brpo.gov.pl/pl/content/rpo-zmienic-zasady-pobierania-bilingow-tsue-premier-odpowiedz.

[85] Wyrok TSUE z dnia 2 marca 2021 r., C-746/18; H.K. przeciwko Prokuratuur.

[86] Zob.: wyrok TSUE z dnia 2 marca 2021 r., C-746/18; H.K. przeciwko Prokuratuur, pkt 9.

[87] Sąd estoński miał wątpliwość, czy przepisy, które zezwalają organom publicznym na dostęp do danych o ruchu lub danych lokalizacyjnych mogących ujawniać szczegółowe informacje o życiu prywatnym jednostki, w celu zapobiegania i ścigania przestępstw, bez ograniczenia tego dostępu wyłącznie do zwalczania poważnej przestępczości, niezależnie od okresu, zakresu i rodzaju udostępnianych danych, są zgodne z art. 15 dyrektywy 2002/58 oraz art. 7, 8, 11 i 52 Karty Praw Podstawowych UE.

[88] Wyrok TSUE z dnia 2 marca 2021 r., C-746/18; H.K. przeciwko Prokuratuur, pkt 11

[89] Karta praw podstawowych Unii Europejskiej (t.j. Dz. U. UE. C. z 2016 r. Nr 202, str. 389); dalej: KPP UE.

[90] Zob. wyrok TSUE z dnia 2 marca 2021 r., C-746/18; H.K. przeciwko Prokuratuur, pkt 30.

dochodzenia, wykrywania i ściganiu przestępstw. Jedynie walka z poważną przestępczością i zapobieganie poważnym zagrożeniom bezpieczeństwa publicznego może uzasadniać poważne ingerencje w prawa podstawowe ustanowione w art. 7 i 8 KPP UE[91]. Nawet dostęp do ograniczonej ilości danych o ruchu lub danych o lokalizacji lub dostęp do danych na krótki okres, dostarcza dokładnych informacji na temat określonej osoby. **Co dodatkowo istotne, nie jest możliwa uprzednia ocena skali ingerencji w prawo do prywatności. Dopiero bowiem po tym, jak organy uzyskają dostęp danych, jest możliwe zweryfikowanie stopnia ingerencji.**

W odniesieniu do możliwości dowodowego wykorzystania w procesie karnym danych niedotyczących treści, pozyskanych od dostawców usług łączności, TSUE stwierdził, że z **zasady skuteczności prawa unijnego wynika – co do zasady – obowiązek nieuwzględnienia informacji i dowodów uzyskanych w drodze uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji niezgodnego z prawem UE**[92]**.** Jeśli krajowy system zatrzymywania danych niedotyczących treści jest wadliwy, to sąd orzekający w sprawie karnej powinien nie dopuścić, by tak pozyskane materiały zostały wykorzystane jako podstawa orzeczenia. TSUE nie przesądził jednak, jak powinien zachować się sąd krajowy – prawo dowodowe, w tym zasady dopuszczalności dowodów są bowiem domeną prawa krajowego.

W wyroku w sprawie *Prokuratuur* TSUE analizował także to, czy prokurator jest „niezależnym organem", który może sprawować efektywny nadzór uprzedni nad pozyskaniem danych niedotyczących treści od dostawców usług łączności[93]. Ponownie, odwołują się do wcześniejszego orzecznictwa, przypomniał o konieczności wprowadzenia obiektywnych kryteriów umożliwiających określenie okoliczności i warunków przyznania dostępu do danych o ruchu oraz lokalizacji uprawnionym organom[94]. **Taki dostęp jest możliwy wyłącznie w odniesieniu do danych osób podejrzewanych o planowanie, popełnianie czy popełnienie poważnego przestępstwa oraz innych osób zaangażowanych w to przestępstwo. Dla zagwarantowania proporcjonalności ingerencji w prawo do prywatności, prawo krajowe powinno przewidywać uprzednią kontrolę sądową lub innego niezależnego organu administracyjnego**. W pilnych sprawach, możliwe jest działanie przez organy ścigania bez wyrażenia uprzedniej zgody przez sąd/inny niezależny organ,

[91] Wyrok TSUE z dnia 2 marca 2021 r., C-746/18; H.K. przeciwko Prokuratuur; pkt 33.
[92] Wyrok TSUE z dnia 2 marca 2021 r., C-746/18; H.K. przeciwko Prokuratuur; pkt 44. Zwłaszcza jeśli strona postępowania nie mogła skutecznie się do nich odnieść i ich kwestionować.
[93] Wyrok TSUE z dnia 2 marca 2021 r., C-746/18; H.K. przeciwko Prokuratuur; pkt 49 i nast.
[94] Wyrok TSUE z dnia 2 marca 2021 r., C-746/18; H.K. przeciwko Prokuratuur; pkt 51.

ale wówczas zgoda następcza powinna być wydana w krótkim czasie[95]. Jeśli kontrola jest sprawowana przez organ inny niż sąd (niezależny organ administracyjny), organ ten musi posiadać status pozwalający na wykonywanie swoich obowiązków w sposób obiektywny i bezstronny, pozostając poza jakimkolwiek wpływem z zewnątrz[96]. Organ ten powinien być także niezaangażowany w prowadzenie postępowania karnego, a także zajmować neutralną pozycję względem stron postępowania[97].

Takim organem nie może być prokurator (prokuratura), która prowadzi dochodzenie/śledztwo, a następnie występuje w postępowaniu w charakterze oskarżyciela publicznego. Zadaniem prokuratur nie jest rozstrzyganie sporu przy zachowaniu całkowitej niezależności, ale skierowanie sporu do właściwego sądu[98]. Okoliczność, że prokuratura jest zobowiązana do weryfikacji okoliczności obciążających i odciążających (korzystnych) dla podejrzanego, jest niewystarczający dla przyznania jej statusu organu niezależnego – „strony trzeciej" – w stosunku do spornych interesów[99]. W konsekwencji **prokurator (prokuratura) nie może zostać uznany za niezależny organ administracyjny, który mógłby przeprowadzić uprzednią kontrolę zasadności uzyskania dostępu do danych niedotyczących treści, gromadzonych (zatrzymywanych) przez dostawców usług łączności**[100]**.** Brak uprzedniej kontroli nie może być uzupełniony na późniejszym etapie postępowania. Jeśli nawet – np. rozpoznając sprawę karną w postępowaniu sądowym – analizuje prawidłowość, proporcjonalność i celowość pozyskania na etapie przedsądowym danych niedotyczących treści od dostawców usług łączności, to kontrola *ex post* nie konwaliduje braku kontroli uprzedniej. **W takiej sytuacji (kontroli następczej) nie jest bowiem możliwa realizacja celu „polegającego na nieumożliwianiu udzielaniu zezwoleń na dostęp do danych", jeśli wykraczałoby poza granice tego, co jest ściśle niezbędne[101].**

[95] Wyrok TSUE z dnia 2 marca 2021 r., C-746/18; H.K. przeciwko Prokuratuur; pkt 51 i wskazane tam orzecznictwo.
[96] Wyrok TSUE z dnia 2 marca 2021 r., C-746/18; H.K. przeciwko Prokuratuur; pkt 53.
[97] Por. wyrok TSUE z dnia 2 marca 2021 r., C-746/18; H.K. przeciwko Prokuratuur; pkt 54.
[98] Por. wyrok TSUE z dnia 2 marca 2021 r., C-746/18; H.K. przeciwko Prokuratuur; pkt 55.
[99] Tak: wyrok TSUE z dnia 2 marca 2021 r., C-746/18; H.K. przeciwko Prokuratuur; pkt 56.
[100] Tak: wyrok TSUE z dnia 2 marca 2021 r., C-746/18; H.K. przeciwko Prokuratuur; pkt 57.
[101] Tak: wyrok TSUE z dnia 2 marca 2021 r., C-746/18; H.K. przeciwko Prokuratuur; pkt 58.

III.2.5. Wyrok TSUE z dnia 5 kwietnia 2022 r. w sprawie G.D. przeciwko Commissioner of An Garda Siochána, C-140/20[102]

W sprawie zainicjowanej pytaniami prejudycjalnymi sądu irlandzkiego TSUE ponownie analizował kwestie zgodności z art. 15 ust. 1 dyrektywy 2002/58 krajowych przepisów odnoszących się do problematyki retencji danych niedotyczących treści i udostępniania tych danych organom ścigania[103]. Przepisy irlandzkie nakładały na dostawców usług łączności elektronicznej niezróżnicowany i ogólny obowiązek zatrzymywania danych o lokalizacji i danych o ruchu przez okres 1 roku[104]. Dostęp do danych mógł uzyskać funkcjonariusz Policji o stopniu co najmniej nadinspektora, o ile zwrócił się do dostawcy usług łączności ze wskazaniem, że dane niedotyczące treści są konieczne do celów zapobiegania poważnym przestępstwom, ich wykrywania, dochodzenia lub ścigania, ochrony bezpieczeństwa państwa oraz ochrony życia ludzkiego. Przepisy przewidywały również procedurę zażaleniową na decyzję o udostępnieniu danych, a także postępowanie przed wyznaczonym sędzią, jako jedną z gwarancji zabezpieczających przed nieuprawnionym dostępem.

Ponownie analizując problematykę zgodności z prawem unijnym uogólnionego i niezróżnicowanego zatrzymywania danych niedotyczących treści przez dostawców usług łączności, TSUE przypomniał, że już samo zatrzymywanie danych o ruchu i lokalizacji dla celów policyjnych może naruszać prawo do prywatności (art. 7 KPP UE) i wywoływać „efekt mrożący" wobec korzystania z wolności wypowiedzi (art. 11 KPP UE). Powyższe dotyczy zwłaszcza przypadków, gdy retencja obejmuje bardzo szeroki zakres danych. Ponadto, ponieważ dane mogą być gromadzone ciągle w ramach uogólnionej i niezróżnicowanej retencji, a informacje z nich należą do szczególnie wrażliwych, już samo ich przechowywanie przez operatorów stwarza podwyższone ryzyko nieuprawnionego dostępu[105]. Niemniej, w kontekście skutecznej walki z przestępczością, zwłaszcza, gdy pokrzywdzonymi są osoby małoletnie (i inne osoby podatne na zagrożenia), ingerencja w sferę prywatności jednostki może być

[102] Zob. także wystąpienia generalne RPO dotyczące tego wyroku wraz z odpowiedziami Kancelarii Prezesa Rady Ministrów oraz Ministra Spraw Wewnętrznych i Administracji dostępne na stronie: https://bip.brpo.gov.pl/pl/content/rpo-inwigilacja-standardy-ponaglenie-premier-mswia-odpowiedz.

[103] Zob. także: K. S. Zielińska, *Powracający problem retencji danych telekomunikacyjnych. Potrzeba zapewnienia bezpieczeństwa narodowego czy może chęć utrzymania niekontrolowanej inwigilacji? - glosa do wyroku Trybunału Sprawiedliwości z 5.04.2022 r., C-140/20, G.D. przeciwko The Commissioner of the Garda Síochána i in*, EPS 2022, nr 11, s. 41-49.

[104] Zob. szerzej wyrok TSUE z dnia 5 kwietnia 2022 r.; C-140/20, G.D. przeciwko Commissioner of An Garda Siochána; pkt 12.

[105] Por. wyrok TSUE z dnia 5 kwietnia 2022 r.; C-140/20, G.D. przeciwko Commissioner of An Garda Siochána; pkt 46.

uzasadniona[106]. Odwołując się do orzecznictwa ETPC, Trybunał luksemburski wskazał, że konieczne jest przyjęcie takich rozwiązań normatywnych, które umożliwią skuteczne zwalczanie przestępstw[107].

Z brzmienia art. 15 ust. 1 zd. 1 dyrektywy 2002/58 wynika, że odstępstwo od zasady poufności komunikacji jest dopuszczalne tylko, gdy jest „niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego", a motyw 11 do dyrektywy 2002/58 wymaga, by było „ściśle" proporcjonalne do zamierzonego celu[108]. **TSUE wskazał również na istnienie „hierarchii celów": ochrona bezpieczeństwa narodowego**[109] **przewyższa cele zwalczania przestępczości w ogólności (choćby poważnej) oraz ochrony bezpieczeństwa publicznego, dlatego – z zastrzeżeniem art. 52 ust. 1 Karty – może uzasadniać dalej idące ingerencje**[110]. Ochrony bezpieczeństwa narodowego nie należy jednak utożsamiać z przestępczością, nawet szczególnie poważną: bezpieczeństwo narodowe dotyczy zapobiegania i ścigania działalności mogącej poważnie zdestabilizować podstawowe struktury państwa lub bezpośrednio zagrozić społeczeństwu, a zagrożenie to musi być rzeczywiste i aktualne lub przynajmniej przewidywalne[111].

Trybunał luksemburski przypomniał, że **uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i lokalizacji do celów zwalczania poważnej przestępczości wykracza poza to, co absolutnie niezbędne i nie może być uzasadnione w społeczeństwie demokratycznym; retencja powinna być**

[106] Por. wyrok TSUE z dnia 5 kwietnia 2022 r.; C-140/20, G.D. przeciwko Commissioner of An Garda Siochána; pkt 49.
[107] Por. wyrok TSUE z dnia 5 kwietnia 2022 r.; C-140/20, G.D. przeciwko Commissioner of An Garda Siochána; pkt 50.
[108] Por. wyrok TSUE z dnia 5 kwietnia 2022 r.; C-140/20, G.D. przeciwko Commissioner of An Garda Siochána; pkt 51-53.
[109] Z tego względu art. 15 ust. 1 dyrektywy 2002/58 nie stoi na przeszkodzie nakazowi uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i lokalizacji dla ochrony bezpieczeństwa narodowego, gdy państwo członkowskie napotyka poważne zagrożenie dla bezpieczeństwa narodowego „rzeczywiste i aktualne lub możliwe do przewidzenia", a decyzja podlega skutecznej kontroli sądu lub niezależnego organu o wiążącej decyzji, nakaz jest wydany na określony czas ograniczony do tego, co ściśle niezbędne, z możliwością przedłużenia w razie utrzymywania się zagrożenia. Por. wyrok TSUE z dnia 5 kwietnia 2022 r.; C-140/20, G.D. przeciwko Commissioner of An Garda Siochána; pkt. pkt 58.
[110] Por. wyrok TSUE z dnia 5 kwietnia 2022 r.; C-140/20, G.D. przeciwko Commissioner of An Garda Siochána; pkt 56-57.
[111] Por. wyrok TSUE z dnia 5 kwietnia 2022 r.; C-140/20, G.D. przeciwko Commissioner of An Garda Siochána; pkt 61-64.

wyjątkiem, a nie regułą, i nie może być systemowa i stała[112]. Warto jednak zauważyć, że w odniesieniu do danych abonenckich (danych o użytkowniku), TSUE wskazał, że ani dyrektywa 2002/58, ani inne akty prawa UE nie stoją na przeszkodzie rozwiązaniu polegającemu na uzależnieniu nabycia karty SIM pre-paid od weryfikacji tożsamości i rejestracji danych nabywcy, z dostępem organów do tych informacji[113]. Zgodne z prawem UE jest także uogólnione i niezróżnicowane zatrzymywanie adresów IP przydzielonych źródłu połączenia. Dodatkowo, w analizowanym orzeczeniu Trybunał wskazał na dopuszczalność niezróżnicowanego, ukierunkowanego zatrzymywania danych. Kryteria te mogą wynikać z obszaru geograficznego – „obszarami tymi mogą być w szczególności miejsca charakteryzujące się dużą liczbą poważnych przestępstw, miejsca szczególnie narażone na popełnianie poważnych przestępstw, takie jak miejsca lub infrastruktura, w których regularnie przebywa bardzo wiele osób, lub też miejsca strategiczne, takie jak porty lotnicze, dworce, porty morskie lub strefy poboru opłat za przejazd”[114]. Ukierunkowane zatrzymywanie danych może odnosić się także do konkretnej osoby lub grupy osób, które są podejrzewane o udział w popełnianiu przestępstw. Dodatkowo, TSUE przypomniał, że w celu zwalczania poważnych przestępstw, możliwe jest nakazanie dostawcom usług łączności elektronicznej, w drodze decyzji właściwego organu (poddanej skutecznej, następczej kontroli sądowej), szybkiego zatrzymywania (mechanizm *quick freeze*) przez określony czas danych o ruchu i danych o lokalizacji, którymi ci dysponują[115].

[112] Por. wyrok TSUE z dnia 5 kwietnia 2022 r.; C-140/20, G.D. przeciwko Commissioner of An Garda Siochána; pkt 65.
[113] Por. wyrok TSUE z dnia 5 kwietnia 2022 r.; C-140/20, G.D. przeciwko Commissioner of An Garda Siochána; pkt 72.
[114] Por. wyrok TSUE z dnia 5 kwietnia 2022 r.; C-140/20, G.D. przeciwko Commissioner of An Garda Siochána; pkt 79.
[115] Por. wyrok TSUE z dnia 5 kwietnia 2022 r.; C-140/20, G.D. przeciwko Commissioner of An Garda Siochána; pkt 86.

III.2.6. Wyrok TSUE z dnia 20 września 2022 r. w sprawie SpaceNET AG i inni, C-793/19

Problematyka możliwości uogólnionego i niezróżnicowanego[116] dostępu do danych niedotyczących treści została rozwinięta w wyroku TSUE w sprawie SpaceNET AG i inni. Pytania prejudycjalne zadał sąd niemiecki[117], a sprowadzały się one do oceny, czy zgodne z prawem UE, w szczególności z art. 15 dyrektywy 2002/58, są przepisy nakładające – co do zasady - na dostawców usług łączności obowiązek uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu oraz lokalizacji użytkowników końcowych, na okres kilku tygodni w celu ścigania poważnych przestępstw lub zapobieganiu konkretnemu zagrożeniu dla bezpieczeństwa narodowego[118].

Przytaczając zasady ogólne, wynikające z dotychczasowego orzecznictwa TSUE, Trybunał luksemburski wskazał, że art. 15 ust. 1 dyrektywy 2002/58, interpretowany łącznie z art. 7, 8 i 11 oraz art. 52 ust. 1 Karty Praw Podstawowych UE, nie wyklucza wprowadzania rozwiązań ustawowych przewidujących zatrzymywanie danych w celu zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego, o ile są to środki odpowiednio zawężone i obwarowane gwarancjami. **Dopuszczalne mogą być w szczególności**:

- **ukierunkowana retencja danych o ruchu i lokalizacji** – ograniczona na podstawie obiektywnych i niedyskryminacyjnych kryteriów, np. ze względu na określone kategorie osób lub obszar geograficzny; stosowana przez czas ściśle niezbędny, ale z możliwością przedłużenia;

---

[116] Obowiązek zatrzymywania danych zgodnie z wówczas obowiązującym prawem obejmował w szczególności dane niezbędne do ustalenia źródła oraz odbiorcy połączenia, datę i godzinę jego rozpoczęcia i zakończenia lub - w przypadku komunikacji za pomocą SMS, wiadomości multimedialnej lub podobnej - moment wysłania i otrzymania wiadomości, „a także datę i godzinę rozpoczęcia i zakończenia połączenia, lub - w przypadku komunikacji za pomocą telefonii mobilnej - oznaczenie komórek, które zostały wykorzystane przez numer wywołujący i wywołany na początku połączenia. W ramach świadczenia usług dostępu do Internetu obowiązek zatrzymywania obejmuje między innymi przypisany abonentowi adres IP, datę i godzinę rozpoczęcia i zakończenia korzystania z Internetu z przypisanego adresu IP oraz, w przypadku korzystania z Internetu mobilnego, oznaczenie komórki wykorzystanej na początku połączenia internetowego. Zatrzymywane są również dane wskazujące na położenie geograficzne i kierunki wiązki głównej anten radiowych obsługujących daną komórkę". Tak: Wyrok TSUE z dnia 20 września 2022 r., C-793/19, SpaceNET AG i inni, pkt 77.

[117] Treść pytania prejudycjalnego została przytoczona w pkt 39 wyroku TSUE z dnia 20 września 2022 r., C-793/19, SpaceNET AG i inni.

[118] Wyrok TSUE z dnia 20 września 2022 r., C-793/19, SpaceNET AG i inni; pkt 47.

- **uogólniona retencja adresów IP przypisanych do źródła połączenia, ale wyłącznie przez okres ściśle niezbędny**;

- **uogólniona retencja danych identyfikacyjnych** (dotyczących tożsamości użytkowników usług łączności);

- **zastosowanie mechanizmu „quick freeze"**, tj. nakazu szybkiego zabezpieczenia danych o ruchu i lokalizacji, którymi dysponują dostawcy usług – wydawanego na określony czas decyzją właściwego organu, poddaną skutecznej kontroli sądowej.

Warunkiem dopuszczalności tych rozwiązań jest to, aby ustawodawstwo zawierało jasne i precyzyjne przepisy, które uzależniają retencję od spełnienia przesłanek materialnych (związanych z prawdopodobieństwem popełnienia czynu) i proceduralnych przesłanek (tryb dostępu do danych, uwzględniający uprzednią kontrolę niezależnego organu administracyjnego albo kontrolę sądową), oraz zapewniają osobom, których dane dotyczą, skuteczne gwarancje chroniące przed nadużyciami[119].

Analizując ustawodawstwo niemieckie, TSUE zwrócił uwagę, że obowiązek zatrzymywania danych, nałożony na dostawców usług łączności, obejmuje niemal całą populację nawet wtedy, gdy nie ma wobec nich żadnych podstaw, choćby pośrednich, do wszczęcia postępowania karnego. Zakres zatrzymywanych danych jest niemal tożsamy, jak w sytuacji, gdy podejrzewa się określoną osobę o popełnienie poważnego przestępstwa lub przestępstwa zagrażającego bezpieczeństwu narodowemu. Także okres zatrzymywania danych jest tożsamy. Co więcej, przepisy niemieckie nie różnicują podmiotowo obowiązku retencji danych, co umożliwia dostęp do danych osób objętych tajemnicą zawodową takich jak adwokaci, lekarze i dziennikarze[120]. TSUE odnotował, że dane były zatrzymywane na stosunkowo krótki okres – na 4 lub 10 tygodni[121]. Podkreślił jednak, że „całościowy zbiór danych o ruchu lub danych dotyczących lokalizacji, zatrzymywanych, odpowiednio, na dziesięć tygodni i na cztery tygodnie, może dostarczyć bardzo precyzyjnych wskazówek dotyczących życia prywatnego osób, których dane są zatrzymywane, takich jak ich codzienne nawyki, miejsca stałego lub czasowego pobytu, codziennie lub okazyjnie pokonywane trasy, podejmowane czynności, relacje społeczne i środowiska społeczne, w których osoby te się obracają i,

[119] Por. przytoczenie orzecznictwa w pkt 49-75, a zwłaszcza pkt 75 wyroku TSUE z dnia 20 września 2022 r., C-793/19, SpaceNET AG i inni.
[120] Por. wyrok TSUE z dnia 20 września 2022 r., C-793/19, SpaceNET AG i inni; pkt 82-84.
[121] Por. wyrok TSUE z dnia 20 września 2022 r., C-793/19, SpaceNET AG i inni; pkt 86

w szczególności, pozwolić na sporządzenie na ich podstawie profilu tych osób”[122]. W konsekwencji **retencja danych o ruchu, danych lokalizacyjnych, czy adresu IP ma zawsze poważny charakter, niezależnie od długości/czasu jej trwania.** Trybunał luksemburski przypomniał ponadto, że zatrzymywanie danych przez dostawców usług łączności i dostęp do danych podlegających retencji w związku z zapobieganiem i zwalczaniem przestępczości, to dwa odrębne rodzaje ingerencji w sferę prywatności jednostki. **Przepisy krajowe, zapewniające pełne poszanowanie praw jednostki na poziomie (etapie) dostępu do zatrzymanych danych, nie mogą jako takie „ani ograniczyć, ani zaradzić poważnej ingerencji, która wynikałaby z uogólnionego zatrzymywania tych danych przewidzianego w tych przepisach krajowych”[123]**. Odnosząc się do kwestii hierarchii celów, które umożliwiają uzyskanie dostępu do danych niedotyczących treści, TSUE odróżnił – ponownie – cel w postaci ochrony bezpieczeństwa narodowego od celu w postaci zwalczania poważnej przestępczości. Przez bezpieczeństwo narodowe – które uzasadnia zatrzymywanie danych w najszerszym zakresie – należy rozumieć ochronę podstawowych funkcji państwa i podstawowych interesów społeczeństwa, przez „zapobieganie i ściganie działalności mogącej poważnie zdestabilizować podstawowe struktury konstytucyjne, polityczne lub społeczne kraju, w szczególności bezpośrednio zagrozić społeczeństwu, ludności lub państwu jako takiemu”[124]. **Zagrożenie dla bezpieczeństwa narodowego musi być jednak realne, rzeczywiste i aktualne albo przynajmniej przewidywalne i dopiero przy spełnieniu takich warunków, dopuszczalne jest wprowadzenie (zastosowanie) środka w postaci uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji przez określony czas.** Z ochroną bezpieczeństwa narodowego nie można utożsamiać celu w postaci zwalczania poważnej przestępczości. Inny jestem bowiem charakter zagrożeń, zakres osób potencjalnie narażonych na pokrzywdzenie. **Dla realizacji celu w postaci zwalczania poważnej przestępczości dopuszczalne jest ukierunkowane zatrzymywanie danych o ruchu i danych dotyczących lokalizacji, którego granice zostają wyznaczone na podstawie obiektywnych i niedyskryminacyjnych przesłanek w zależności od kręgu osób, których dane dotyczą, lub kryterium geograficznego,**

[122] Tak: wyrok TSUE z dnia 20 września 2022 r., C-793/19, SpaceNET AG i inni; pkt 90. Zagrożenia związane z możliwością profilowania TSUE analizował także w kontekście dostępu do IP i wniosków, jakie można wywieść pozyskując adres IP. Por. pkt 79 analizowanego wyroku.
[123] Tak: wyrok TSUE z dnia 20 września 2022 r., C-793/19, SpaceNET AG i inni; pkt 91.
[124] Tak: wyrok TSUE z dnia 20 września 2022 r., C-793/19, SpaceNET AG i inni; pkt 92.

na okres ograniczony do tego, co ściśle niezbędne, ale z możliwością odnowienia tego okresu[125].

W analizowanym orzeczeniu TSUE rozwinął także kwestię zatrzymywania i dostępu do adresu (adresów) IP określonej osoby. Zatrzymywanie adresów IP nie pozwala na odtworzenie informacji o przeglądanych stronach internetowych, itp., ale i tak pozyskane adresy IP mogą posłużyć do „wyczerpującego" prześledzenia aktywności internauty w sieci i zbudowania jego profilu, co jest poważną ingerencją w prawa z art. 7 i 8 KPP UE[126]. Uogólnione zatrzymywanie adresów IP co do zasady nie jest sprzeczne z art. 15 ust. 1 dyrektywy 2002/58 (w zw. z art. 7, 8, 11 i art. 52 ust. 1 Karty Praw Podstawowych UE), ale pod warunkiem spełnienia warunków materialnych i proceduralnych dotyczących wykorzystywania tych danych[127]. Celem uogólnionego zatrzymywania adresów IP źródła połączenia może być walka z poważną przestępczością i zapobieganie poważnym zagrożeniom dla bezpieczeństwa publicznego, a także ochrona bezpieczeństwa narodowego. Okres zatrzymywania musi być jednak ograniczony do „ściśle niezbędnego" i należy wprowadzić ścisłe warunki i gwarancje wykorzystywania tych danych, zwłaszcza gdy mają służyć do śledzenia aktywności online[128]. TSUE nie sprecyzował jednak, jakie gwarancje i warunki wykorzystania danych powinny być wprowadzone w ustawodawstwie krajowym.

TSUE odniósł się także do problematyki szybkiego zatrzymywania danych o ruchu i danych dotyczących lokalizacji, przetwarzanych i przechowywanych przez dostawców usług łączności elektronicznej[129]. Co do zasady, po upływie ustawowych terminów, dane te powinny zostać usunięte lub zanonimizowane. TSUE zwrócił jednak uwagę, że w praktyce mogą pojawić się sytuacje, w których konieczne będzie zabezpieczenie danych o ruchu i danych o lokalizacji po upływie terminów ich usunięcia (anonimizacji). Może być to uzasadnione potrzebą prowadzenia postępowania w sprawach o poważne przestępstwa albo w sprawach dotyczących bezpieczeństwa narodowego - zarówno wtedy, gdy takie czyny zostały już wykryte, jak i wtedy, gdy po obiektywnym zbadaniu wszystkich istotnych okoliczności można racjonalnie podejrzewać, że miały miejsce[130]. W takich przypadkach państwa członkowskie mogą przewidzieć w prawie możliwość wydania operatorom – decyzją właściwego organu poddaną skutecznej kontroli

[125] Tak: sentencja wyroku TSUE z dnia 20 września 2022 r., C-793/19, SpaceNET AG i inni.
[126] Tak: wyrok TSUE z dnia 20 września 2022 r., C-793/19, SpaceNET AG i inni; pkt 79.
[127] Por. wyrok TSUE z dnia 20 września 2022 r., C-793/19, SpaceNET AG i inni; pkt 100-101.
[128] Tak: wyrok TSUE z dnia 20 września 2022 r., C-793/19, SpaceNET AG i inni; pkt 102.
[129] Na podstawie art. 5, 6 i 9 dyrektywy 2002/58 albo na podstawie środków przyjętych w trybie art. 15 ust. 1 dyrektywy 2002/58.
[130] Tak: wyrok TSUE z dnia 20 września 2022 r., C-793/19, SpaceNET AG i inni; pkt 114-115.

sądowej – nakazu „szybkiego zatrzymania" (*quick freeze*) danych o ruchu i lokalizacji, którymi operator dysponuje, na określony czas[131]. Z uwagi na fakt, że szybkie zatrzymywanie (*quick freeze*) dotyczy danych zebranych (zatrzymanych) pierwotnie w innym celu, ustawodawca krajowy musi jasno wskazać cel, dla którego taki nakaz może być stosowany. Z uwagi na wagę (dolegliwość) ingerencji w prywatność jednostki, może być ona usprawiedliwiona wyłącznie zwalczaniem poważnej przestępczości, a tym bardziej – ochroną bezpieczeństwa narodowego[132]. Trybunał luksemburski doprecyzował też, że szybkie zatrzymywanie danych nie musi dotyczyć wyłącznie osób podejrzewanych o popełnienie przestępstwa. Może – pod warunkiem zachowania granic „ściśle niezbędnych" oraz opierania się na obiektywnych i niedyskryminacyjnych kryteriach – obejmować także inne osoby, jeżeli mogą one realnie pomóc w wyjaśnieniu poważnego przestępstwa lub naruszenia bezpieczeństwa narodowego (np. dane o lokalizacji, dane o ruchu pokrzywdzonego i osób z otoczenia tej osoby)[133]. W konsekwencji, środek ten może obejmować m.in. dane osób, z którymi pokrzywdzony był w kontakcie przed zdarzeniem, może zostać rozszerzony na określone strefy geograficzne (np. miejsce popełnienia/przygotowania czynu albo miejsce zaginięcia potencjalnej ofiary)[134], a także może zostać zarządzony już na pierwszym etapie dochodzenia dotyczącego poważnego zagrożenia dla bezpieczeństwa narodowego lub ewentualnie – innego poważnego przestępstwa[135].

Ostatnią analizowaną kwestią w wyroku SpaceNET AG i inni była problematyka dostępu do danych niedotyczących treści przekazu, które zostały zatrzymane w wyniku uogólnionego i niezróżnicowanego obowiązku retencji. Na rozprawie przed TSUE m.in. rząd duński argumentował, że organy krajowe – dla celów walki z poważną przestępczością – powinny móc uzyskiwać dostęp do danych o ruchu i danych lokalizacyjnych, które zostały zatrzymane w sposób uogólniony i niezróżnicowany, jeżeli retencja ta została wprowadzona w reakcji na poważne zagrożenie dla bezpieczeństwa narodowego[136]. Trybunał luksemburski zakwestionował dopuszczalność takiego działania. Po pierwsze wskazał, że dopuszczenie dostępu w związku z realizacją celu w postaci zwalczania poważnej przestępczości do danych zatrzymanych ze względu na ochronę bezpieczeństwa narodowego prowadziłoby do tego, że możliwość korzystania z tak daleko idącej ingerencji byłaby uzależniona od okoliczności niezwiązanych z celem

[131] Tak: wyrok TSUE z dnia 20 września 2022 r., C-793/19, SpaceNET AG i inni; pkt 115.
[132] Tak: wyrok TSUE z dnia 20 września 2022 r., C-793/19, SpaceNET AG i inni; pkt 116.
[133] Tak: wyrok TSUE z dnia 20 września 2022 r., C-793/19, SpaceNET AG i inni; pkt 117-118.
[134] Tak: wyrok TSUE z dnia 20 września 2022 r., C-793/19, SpaceNET AG i inni; pkt 119.
[135] Tak: wyrok TSUE z dnia 20 września 2022 r., C-793/19, SpaceNET AG i inni; pkt 120.
[136] Wyrok TSUE z dnia 20 września 2022 r., C-793/19, SpaceNET AG i inni; pkt 126.

walki z poważną przestępczością, tj. od tego, czy w danym państwie występuje akurat poważne zagrożenie dla bezpieczeństwa narodowego[137]. **Po drugie TSUE przypomniał zasadę, że dostęp do danych zatrzymywanych na podstawie art. 15 ust. 1 dyrektywy 2002/58 może być co do zasady uzasadniony tylko tym celem interesu ogólnego, dla którego dostawcy zostali zobowiązani do ich zatrzymywania**[138]. Po trzecie Trybunał podkreślił, przyjęcie dopuszczalności dostępu w celu zwalczania poważnej przestępczości do zatrzymanych danych w celu ochrony bezpieczeństwa narodowego byłoby sprzeczne z hierarchią celów[139]. Cel w postaci ochrony bezpieczeństwa narodowego ma nadrzędne znaczenie i nie można tego pojęcia rozumieć w sposób rozszerzający. Po czwarte zaś, Trybunał podkreślił, że dane o ruchu i dane lokalizacyjne nie mogą być przedmiotem uogólnionej i niezróżnicowanej retencji dla celów walki z poważną przestępczością, a zatem również dostęp do takich danych nie może być uzasadniany tym celem. Jeżeli natomiast dane zostały wyjątkowo zatrzymane w sposób uogólniony i niezróżnicowany dla ochrony bezpieczeństwa narodowego (w warunkach dopuszczalności takiej retencji), to organy prowadzące postępowanie karne nie mogą uzyskać do nich dostępu w ramach ścigania karnego, bo prowadziłoby to do pozbawienia skuteczności (*effet utile*) zakazu generalnej retencji dla zwalczania poważnej przestępczości[140].

III.2.7. Wyrok TSUE z dnia 30 kwietnia 2024 r., w sprawie Procura della Repubblica presso il Tribunale di Bolzano, C-178/22

W sprawie C-178/22, Procura della Repubblica presso il Tribunale di Bolzano TSUE ponownie zajmował się problematyką zarówno nałożenia na dostawców usług internetowych uogólnionego i niezróżnicowanego obowiązku zatrzymywania danych niedotyczących treści. Kluczowym zagadnieniem, nieporuszanym we wcześniejszym orzecznictwie TSUE odnoszącym się do tej problematyki, był zakres kompetencji sądu

[137] Oznacza to, że w państwie, w którym występuje realne zagrożenie dla bezpieczeństwa narodowego, dane zatrzymywane w sposób uogólniony, mogłyby zostać wykorzystane np. w sprawie o „poważne przestępstwo", np. zagrożone karą pozbawienia wolności przekraczającą trzy lata. W państwach, w których brak jest takiego zagrożenia dla bezpieczeństwa narodowego, dane niedotyczące treści nie mogłyby być w ogóle zatrzymywane w sposób niezróżnicowany i uogólniony. W zależności od istniejących zagrożeń – co do zasady zewnętrznych – odmienne byłyby możliwości śledcze w klasycznej przestępczości. W ocenie Trybunału – skoro celem dostępu miałaby być walka z poważną przestępczością – nic nie uzasadnia różnicowania sytuacji między państwami członkowskimi w zależności od występowania takiego zagrożenia (tak: wyrok TSUE z dnia 20 września 2022 r., C-793/19, SpaceNET AG i inni; pkt 127).

[138] Wyrok TSUE z dnia 20 września 2022 r., C-793/19, SpaceNET AG i inni; pkt 128.

[139] Wyrok TSUE z dnia 20 września 2022 r., C-793/19, SpaceNet AG i inni; pkt 129.

[140] Wyrok TSUE z dnia 20 września 2022 r., C-793/19, SpaceNet AG i inni; pkt 130.

do badania zasadności żądania dostępu do danych niedotyczących treści przekazu, a także jak należy rozumieć pojęcie „poważnej przestępczości". Przepisy włoskie co do zasady nakazywały udzielić zgodę na dostęp do danych o ruchu i lokalizacji, gdy organ wnioskujący (prokurator) albo obrońca oskarżonego żądał tego dostępu dla potrzeb postępowania karnego prowadzonego w sprawie o przestępstwo zagrożone karą co najmniej 3 lat pozbawienia wolności i spełnione zostały przesłanki prawdopodobieństwa popełnienia czynu, jak i istotności danych dla potrzeb prowadzonego postępowania[141].

Następnie odnosząc się konkretnie do okoliczności sprawy, w której zadane zostało pytanie prejudycjalne, TSUE zwrócił uwagę, że prokuratura wnioskowała o szeroki zakres danych, w szczególności: dane „użytkowników i numerów IMEI urządzeń wywoływanych lub wywołujących, odwiedzanych lub odbieranych stron, czasu i długości wywołań/połączeń, wskazania odpowiednich stacji przekaźnikowych lub anten oraz użytkowników i numerów IMEI urządzeń będących nadawcami/odbiorcami wiadomości SMS lub MMS"[142]. Celem żądania było ustalenie domniemanych sprawców kradzieży telefonów komórkowych, a wnioski dotyczyły „jedynie krótkich okresów, poniżej dwóch miesięcy, od dnia domniemanych kradzieży telefonów komórkowych do dnia, w którym wnioski te sporządzono"[143].

W części dotyczącej zdefiniowania pojęcia „poważne przestępstwo" Trybunał podkreślił, że w braku harmonizacji Unii, to do państw członkowskich należy określenie, jak rozumieć ten termin[144]. **Ponieważ art. 15 ust. 1 dyrektywy 2002/58 jest wyjątkiem od zasady poufności komunikacji, musi być interpretowany ściśle: odstępstwo od zasady poufności komunikacji nie może stać się regułą[145]**. Środki krajowe muszą też respektować zasadę proporcjonalności i prawa z art. 7, 8 i 11 Karty Praw Podstawowych UE[146]. **Państwo nie może wypaczać pojęcia poważnej przestępczości przez obejmowanie nim czynów oczywiście drobnych tylko dlatego, że ustawodawca**

[141] Wyrok TSUE z dnia 30 kwietnia 2024 r., C-178/22, Procura della Repubblica presso il Tribunale di Bolzano; pkt 9-15, 24.
[142] Wyrok TSUE z dnia 30 kwietnia 2024 r., C-178/22, Procura della Repubblica presso il Tribunale di Bolzano; pkt 38.
[143] Wyrok TSUE z dnia 30 kwietnia 2024 r., C-178/22, Procura della Repubblica presso il Tribunale di Bolzano; pkt 40.
[144] Wyrok TSUE z dnia 30 kwietnia 2024 r., C-178/22, Procura della Repubblica presso il Tribunale di Bolzano; pkt 44-47.
[145] Wyrok TSUE z dnia 30 kwietnia 2024 r., C-178/22, Procura della Repubblica presso il Tribunale di Bolzano; pkt 48.
[146] Wyrok TSUE z dnia 30 kwietnia 2024 r., C-178/22, Procura della Repubblica presso il Tribunale di Bolzano; pkt 49.

przewidział dla nich maksimum 3 lat pozbawienia wolności[147]. W analizowanej sprawie próg „co najmniej 3 lata pozbawienia wolności" jest kryterium obiektywnym i nie wydaje się zbyt niski[148]. Nie można jednak wykluczyć, że w konkretnej sprawie – formalnie mieszczącej się w grupie przestępstw zagrożonych karą co najmniej 3 lat pozbawienia wolności – dostęp do danych o ruchu, danych o lokalizacji byłby nieproporcjonalną ingerencją[149].

Kluczowe jest to, by sąd (lub inny niezależny organ) na etapie uprzedniej kontroli oceny żądania dostępu do danych o ruchu i danych o lokalizacji mógł odmówić albo ograniczyć dostęp do tych danych, jeżeli ingerencja w prawo do prywatności byłaby nadmierna (nieproporcjonalna), a jest oczywiste, że czyn nie mieści się w poważnej przestępczości[150]. Obowiązkiem sądu jest zagwarantowanie właściwej równowagi między potrzebami postępowania karnego a prawami podstawowymi[151].

III.3. Unijny model retencji i dostępu do danych niedotyczących treści – minimalne wymogi regulacji ustawowej

Orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej, od czasu wyroku w sprawie Digital Rights Irleand, stale się rozwija. TSUE stopniowo uzupełnia i precyzuje zasady odnoszące się do obowiązku retencji danych niedotyczących treści. Obecnie można już – patrząc całościowo – wywieść z niego precyzyjne wskazania dla ustawodawcy krajowego dotyczące ukształtowania modelu retencji danych oraz dostępu do danych zatrzymywanych.

Nałożenie na dostawców usług łączności obowiązku zatrzymywania danych niedotyczących treści należy odróżnić od dostępu przez organy ścigania (organy procesowe) do tych danych.

Prawo krajowe może zobowiązywać dostawców usług łączności elektronicznej do zatrzymywania danych niedotyczących treści przez określony czas. TSUE nie wskazuje

[147] Wyrok TSUE z dnia 30 kwietnia 2024 r., C-178/22, Procura della Repubblica presso il Tribunale di Bolzano; pkt 50.
[148] Wyrok TSUE z dnia 30 kwietnia 2024 r., C-178/22, Procura della Repubblica presso il Tribunale di Bolzano; pkt 56.
[149] Wyrok TSUE z dnia 30 kwietnia 2024 r., C-178/22, Procura della Repubblica presso il Tribunale di Bolzano; pkt 57.
[150] Wyrok TSUE z dnia 30 kwietnia 2024 r., C-178/22, Procura della Repubblica presso il Tribunale di Bolzano; pkt 60-62.
[151] Wyrok TSUE z dnia 30 kwietnia 2024 r., C-178/22, Procura della Repubblica presso il Tribunale di Bolzano; pkt 61.

jednolitego „maksymalnego" okresu retencji w ujęciu liczbowym, wymaga jednak, aby retencja była ograniczona do tego, co ściśle niezbędne – zarówno co do kategorii danych, celu, jak i okresu przechowywania. Ocena dopuszczalności retencji jest zróżnicowana w zależności od rodzaju danych (danych abonenckich, danych o IP, danych o ruchu/transmisyjnych i danych o lokalizacji).

Z orzecznictwa TSUE wynikają odmienne reguły dla różnych kategorii danych niedotyczących treści:

- dane identyfikacyjne abonenta/użytkownika (*civil identity*) – co do zasady dopuszczalna jest retencja uogólniona i niezróżnicowana, przy zachowaniu wymogów konieczności i odpowiednich gwarancji;

– adresy IP przypisane do źródła połączenia internetowego – dopuszczalna jest możliwość retencji uogólnionej i niezróżnicowanej, konieczne jest jej ograniczenie w czasie do tego, co ściśle niezbędne oraz powiązania z celem o odpowiedniej wadze w „hierarchii celów";

– dane o ruchu i dane lokalizacyjne - są traktowane jako dane szczególnie wrażliwe, ponieważ pozwalają na wyciągnięcie precyzyjnych wniosków o życiu prywatnym jednostki; co do zasady niedopuszczalna jest ich uogólniona i niezróżnicowana retencja dla celów zwalczania przestępczości, z wyjątkiem ściśle określonych sytuacji.

TSUE różnicuje również dopuszczalny model retencji w zależności od celu zatrzymywania danych niedotyczących treści, wprowadzając swoistą „hierarchię celów".

Celem o najwyższej wadze jest ochrona bezpieczeństwa narodowego. Bezpieczeństwo narodowe jest rozumiane jako ochrona podstawowych funkcji państwa i fundamentalnych interesów społeczeństwa przed zagrożeniem o szczególnej (istotnej) wadze, które jest poważne, rzeczywiste i aktualne albo co najmniej możliwe do przewidzenia. W wyjątkowych warunkach ochrona bezpieczeństwa narodowego może uzasadniać np. uogólnione i niezróżnicowane zatrzymywanie danych niedotyczących treści, w tym danych o ruchu i danych o lokalizacji. Konieczne jest jednak wprowadzenie ograniczeń, które będą chroniły przed nadużyciami (np. ograniczenie czasowe, związane z istnieniem zagrożenia dla bezpieczeństwa narodowego).

Cel w postaci zapewnienia/ochrony bezpieczeństwa narodowego należy odróżnić od ochrony bezpieczeństwa powszechnego i zwalczania poważnej przestępczości. Dla realizacji tych celów:

- niedopuszczalna jest uogólniona i niezróżnicowana retencja danych o lokalizacji i danych o ruchu/transmisyjnych;

- możliwa jest uogólniona i niezróżnicowana retencja danych abonenckich;

- oraz adresów IP, przy czym w tym ostatnim przypadku, konieczne jest uwzględnienie zasady proporcjonalności i np. ograniczenie czasowe.

Jeśli chodzi o zatrzymywanie danych lokalizacyjnych i transmisyjnych/danych o ruchu, TSUE dopuszcza możliwość ukierunkowanej retencji danych, np. ze względów geograficznych (przykładowo na lotniskach, dworcach kolejowych, miejscach o zwiększonym zagrożeniu poważną przestępczością, miejsca o zwiększonym ryzyku) albo określonej kategorii osób. Ważne, by taka ukierunkowana retencja nie odbywała się na podstawie kryteriów dyskryminacyjnych, ale muszą być one zobiektywizowane, weryfikowalne i proporcjonalne.

W pozostałych sytuacjach, dotyczących w ogólności przestępczości (w tym drobnej przestępczości), TSUE dopuszcza retencję danych abonenckich, pozwalających na identyfikację użytkownika oraz danych o IP. Takie sprawy nie uzasadniają sięgania po środki dolegliwie ingerujące w sferę prywatności jednostki. W szczególności niedopuszczalne jest zatrzymywanie danych o ruchu/transmisyjnych i lokalizacji.

Dostęp do danych zatrzymywanych przez dostawców usług łączności elektronicznej jest odrębną ingerencją w prawo do prywatności jednostki. **Nawet jeżeli prawo krajowe dopuszcza zatrzymywanie określonych kategorii danych (np. danych abonenckich lub adresów IP), nie oznacza to automatycznie dopuszczalności dostępu do tych danych przez organy publiczne w dowolnym zakresie i dla dowolnych celów. TSUE konsekwentnie podkreśla, że dostęp do danych – zwłaszcza danych o ruchu i danych lokalizacyjnych – musi podlegać odrębnej ocenie proporcjonalności oraz być ograniczony do sytuacji, w których jest to ściśle niezbędne do realizacji celu o odpowiedniej wadze.**

Z orzecznictwa TSUE wynika, że warunki dostępu do danych niedotyczących treści powinny być zróżnicowane.

W odniesieniu do danych o ruchu i danych lokalizacyjnych, które pozwalają na rekonstrukcję aktywności jednostki, jej relacji społecznych oraz schematów życia, dostęp stanowi ingerencję o szczególnej intensywności, a zatem jest zasadniczo dopuszczalny jedynie w związku ze zwalczaniem poważnej przestępczości albo

zapobieganiem poważnym zagrożeniom dla bezpieczeństwa publicznego, a także – w związku z zapewnieniem bezpieczeństwa narodowego. Jeśli chodzi o rozumienie pojęcia poważnej przestępczości, to TSUE nie przesądza tej okoliczności, pozostawiając konkretne uregulowania państwom członkowskim UE. Co do zasady, przestępstwa zagrożone karą wyższą niż 3 lata pozbawienia wolności mogą zostać uznane za „poważne przestępstwa", ale w konkretnej sytuacji nie można wykluczyć, że czyn, zagrożony tak surową karą nie jest „poważnym przestępstwem", a przestępstwem o średniej lub nieznacznej społecznej szkodliwości. W tym zakresie konieczna jest zindywidualizowana ocena organu, który będzie decydował o dostępie do zatrzymanych danych.

Dostęp do danych identyfikacyjnych (abonentowych) może podlegać łagodniejszym warunkom, jednak również w tym zakresie prawo krajowe powinno przewidywać jasne podstawy prawne oraz wprowadzić mechanizmy zapobiegające dostępowi o charakterze blankietowym (pozyskiwaniu danych „na wszelki wypadek").

W każdym przypadku TSUE wymaga, aby prawo krajowe w sposób jasny i precyzyjny określało przesłanki dostępu, w tym powiązanie żądanych danych z konkretnym celem oraz ze sprawą, dla której dane mają zostać wykorzystane, a także aby dostęp był ograniczony w czasie i zakresie do tego, co ściśle niezbędne. Dostęp i wykorzystanie danych bowiem pozostawać w ścisłym związku z celem, który uzasadniał ich zatrzymywanie. Wykorzystanie danych w innym celu nie może prowadzić do obejścia gwarancji właściwych dla danej kategorii danych. Nie można zatem „skorzystać" w sprawie o drobne przestępstwo z danych lokalizacyjnych czy transmisyjnych zatrzymanych w celu zwalczania poważnej przestępczości.

Kluczowym elementem modelu zgodnego z orzecznictwem TSUE i prawem unijnym jest również ustanowienie uprzedniej kontroli – wykonywanej przez sąd lub niezależny organ – która następuje na podstawie wniosku organu żądającego danych i umożliwia realną weryfikację zasadności, legalności i proporcjonalności żądania. TSUE wskazuje, że kontrola ta nie może mieć charakteru wyłącznie formalnego (organ musi mieć możliwość odmowy uwzględnienia żądania albo modyfikacji – ograniczenia – zakresu żądania), a organ kontrolny powinien być niezależny względem organu prowadzącego czynności. W tym kontekście TSUE podkreśla, że prokurator kierujący postępowaniem nie spełnia wymogu niezależności właściwej dla organu uprzedniej kontroli. Jest bowiem organem, który pełni funkcję oskarżyciela publicznego na późniejszym (sądowym) etapie postępowania karnego, stąd też nie można go uznać za „stronę trzecią", obiektywnie oceniającą zasadność żądania dostępu do danych.

Jeśli chodzi o uprawnienia jednostki, która może podejrzewać, że jej dane osobowe były przetwarzane w związku z zapobieganiem i zwalczaniem przestępczości, to zastosowanie znajdują ogólne zasady wynikające z art. 13 – 17 dyrektywy 2016/680. Oznacza to, że osoba powinna mieć możliwość uzyskania informacji od administratora, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli takie dane są przetwarzane, prawo dostępu do danych osobowych. Przepis art. 14 dyrektywy 2016/680 wskazuje, że może ona się domagać wskazania m.in. celu przetwarzania danych w planowanego okresu ich przechowywania lub, gdy nie jest to możliwe, kryteria służące określeniu tego okresu. Prawo to może być ograniczone zgodnie z zasadami wynikającymi z art. 15 dyrektywy 2016/680[152]. Jeśli jednak prawo do bezpośredniego „wglądu" w przetwarzanie i przechowywanie danych osobowych zostało ograniczone, to prawo krajowe musi przewidywać mechanizm „pośredniego" wykonywania tego uprawnienia. Właściwy organ nadzorczy – zgodnie z art. 17 dyrektywy 2016/680 powinien mieć możliwość uzyskania informacji o celu przetwarzania danych, czasie przetwarzania, odbiorcach danych osobowych, rodzaju danych, jakie są przetwarzane (por. art. 14 dyrektywy 2016/680).

[152] Przepis ten brzmi: Państwa członkowskie mogą przyjąć akty prawne pozwalające ograniczyć w całości lub w części prawo dostępu osoby, której dane dotyczą, w takim stopniu i przez taki okres, w jakim takie częściowe lub całkowite ograniczenie jest działaniem niezbędnym i proporcjonalnym w społeczeństwie demokratycznym, z należytym uwzględnieniem praw podstawowych i uzasadnionych interesów danej osoby fizycznej, aby: a) uniemożliwić utrudnianie czynności postępowań urzędowych lub sądowych, postępowań przygotowawczych lub procedur; b) uniemożliwić zakłócanie zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar; c) chronić bezpieczeństwo publiczne; d) chronić bezpieczeństwo narodowe; e) chronić prawa i wolności innych osób.

IV. Retencja danych i dostęp do zatrzymywanych danych w orzecznictwie Europejskiego Trybunału Praw Człowieka

IV.1. Wyrok Europejskiego Trybunału Praw Człowieka w sprawie Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce (problem retencji danych)

W wyroku w sprawie Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce, ETPC stwierdził naruszenie art. 8 EKPC także w odniesieniu do przepisów o retencji danych[153]. W orzeczeniu tym Trybunał strasburski wskazał, że „**przepisy krajowe, zgodnie z którymi dostawcy usług łączności[154] są zobowiązani do przechowywania danych dotyczących komunikacji w sposób ogólny i niezróżnicowany do celów ewentualnego dostępu przez właściwe organy krajowe, są niewystarczające, aby ograniczyć ingerencję w korzystanie przez skarżących z ich prawa do poszanowania życia prywatnego do tego, co jest niezbędne w demokratycznym społeczeństwie**"[155].

Trybunał przypomniał, że obecne możliwości technologiczne, komunikowanie się za pośrednictwem telefonów, Internetu i innych usług łączności, może ujawniać dane osobowe jednostki, a także dostarczać precyzyjnych informacji na temat życia prywatnego określonej osoby. Monitorowanie aktywności danej osoby w sieciach społecznościowych, monitorowanie schematów przemieszczania się, nawyków komunikacyjnych pozwala na stworzenie jej intymnego portretu[156]. Problem ten jest zwielokrotniony, jeśli przepisy pozwalają na masowe przechwytywanie, przechowywanie i udostępnianie danych o abonentach usług telekomunikacyjnych,

---

[153] Zasadnicza część wyroku dotyczyła problematyki kontroli operacyjnej oraz problematyki ustawy o działaniach antyterrorystycznych. W przedmiocie tej części orzeczenia, opracowany został pierwszy raport w Biurze Rzecznika Praw Obywatelskich. Raport – wraz z wystąpieniem generalnym Rzecznika Praw Obywatelskich do Ministra Spraw Wewnętrznych i Administracji, Ministra Sprawiedliwości oraz Ministra Koordynatora ds. Służb Specjalnych oraz odpowiedziami ministerstw jest dostępny na stronie: https://bip.brpo.gov.pl/pl/content/rpo-kontrola-operacyjna-przepisy-ms-mswia-koordynator-sluzb-odpowiedzi.

[154] Usługi ICT to termin obejmujący wszystkie technologie służące do przetwarzania, przesyłania, przechowywania i odbierania informacji, w tym sprzęt (komputery, smartfony), oprogramowanie, sieci (internet, telekomunikacja) oraz usługi i aplikacje z nimi związane.

[155] Wyrok ETPC z dnia 28 maja 2024 r. w sprawie Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce, skargi nr 72038/17 i 25237/18; § 264.

[156] Wyrok ETPC z dnia 28 maja 2024 r. w sprawie Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce, skargi nr 72038/17 i 25237/18; § 249. Wyrok ETPC z dnia 25 maja 2021 r. w sprawie Centrum för rättvisa przeciwko Szwecji, skarga nr 35252/08; 256, wyrok ETPC z dnia 25 maja 2021 w sprawie Big Brother Watch i inni przeciwko Zjednoczonemu Królestwu, skargi nr 58170/13, 62322/14, 24960/15, § 432 oraz wyrok ETPC z dnia 11 stycznia 2022 r. w sprawie Ekimdzhiev i inni przeciwko Bułgarii, skarga nr 70078/12; § 394.

danych o ruchu/danych transmisyjnych oraz danych o lokalizacji. Ze względu na możliwość powiązania różnych kategorii danych oraz zakres możliwych do uzyskania informacji o jednostce „**pozyskiwanie powiązanych danych dotyczących komunikacji w kontekście masowego przechwytywania może być tak samo inwazyjne jak pozyskiwanie treści komunikatów, a zatem przechwytywanie i zatrzymywanie takich danych oraz przeprowadzane na nich wyszukiwania muszą być analizowane w świetle tych samych zabezpieczeń, które mają zastosowanie do treści komunikatów, bez konieczności, aby przepisy prawne regulujące przetwarzanie takich danych były identyczne pod każdym względem z przepisami regulującymi przetwarzanie treści komunikatów"**[157].

Trybunał strasburski nie zanegował możliwości wprowadzenia w konkretnym ustawodawstwie uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu/danych transmisyjnych i danych o lokalizacji. Dla realizacji celu w postaci ochrony bezpieczeństwa narodowego[158], czy w odniesieniu do przechwytywania komunikacji transgranicznej, danych od służb wywiadowczych, takie działanie może okazać się konieczne dla ochrony społeczeństwa demokratycznego (art. 8 ust. 2 EKPC)[159]. Jeśli rozwiązania krajowe przewidują uogólnione i niezróżnicowane zatrzymywanie danych przez dostawców usług komunikacyjnych, ich przetwarzaniu – w konkretnej sprawie – muszą towarzyszyć zabezpieczenia i gwarancje przed nadużyciami. Prawo powinno jasno określać podstawy, kiedy dozwolone jest masowe zatrzymywanie danych niedotyczących treści oraz procedurę udzielania zezwolenia na niejawny nadzór[160]. Tak jak w sprawach o „klasyczną" niejawną inwigilację (niejawną inwigilację polegającą na zapoznaniu się z treścią komunikatów przesyłanych drogą elektroniczną), ETPC bada:

1) dostępność prawa krajowego;

2) zakres i czas trwania środków niejawnego nadzoru;

3) procedury, których należy przestrzegać w celu przechowywania, sprawdzania, analizowania, wykorzystywania, przekazywania i niszczenia przechwyconych danych;

---

[157] Wyrok ETPC z dnia 28 maja 2024 r. w sprawie Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce, skargi nr 72038/17 i 25237/18; § 249.

[158] Wyrok ETPC z dnia 4 grudnia 2025 r. w sprawie Roman Zakharov przeciwko Rosji, skarga nr 47143/06; § 238.

[159] Zob. także: wyrok ETPC z dnia 25 maja 2021 r. w sprawie Centrum för rättvisa przeciwko Szwecji, skarga nr 35252/08; § 256; wyrok ETPC z dnia 25 maja 2021 w sprawie Big Brother Watch i inni przeciwko Zjednoczonemu Królestwu, skargi nr 58170/13, 62322/14, 24960/15.

[160] Wyrok ETPC z dnia 28 maja 2024 r. w sprawie Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce, skargi nr 72038/17 i 25237/18; § 251.

4) procedury udzielania zezwoleń na niejawną inwigilację;

5) ustalenia dotyczące kontroli stosowania środków niejawnego nadzoru;

6) istnienie mechanizmu powiadamiania/notyfikacji o niejawnej inwigilacji; oraz

7) istnienie środków odwoławczych w prawie krajowym pozwalających zweryfikować podstawy zastosowania oraz procedury zarządzenia niejawnego nadzoru[161].

Oceniając prawo krajowe – polskie rozwiązania dotyczące nałożonego na dostawców usług internetowych obowiązku retencji danych – ETPC wskazał, że „**obowiązujące przepisy ustanowiły system nadzoru, w ramach którego wszyscy użytkownicy usług telekomunikacyjnych i internetowych są objęci środkiem zatrzymywania danych związanych z ich komunikacją bez informowania ich o tym**”[162]. System dostępu do tych danych – „stałe łącze” pozwalające na bezpośredni dostęp funkcjonariuszy Policji i innych służb do danych niedotyczących treści bez zaangażowania dostawców usług łączności - nie gwarantuje odpowiednich zabezpieczeń przed nadużyciami. Cele zatrzymywania danych oraz dostępu do zatrzymanych danych są sformułowane na tyle ogólnie, że mogą one zostać wykorzystane niemal dowolnie – o ile mieści się w zakresie działania określonej służby. Mechanizm sądowej kontroli, w kształcie, jaki został wprowadzony w krajowym ustawodawstwie, jest niewystarczającym zabezpieczeniem przed nadużyciami[163]. Odwołując się do orzecznictwa TSUE, Trybunał strasburski skonstatował, „przepisy krajowe (...) **nie mogą, ze względu na swój charakter, być w stanie ograniczyć ani nawet zaradzić poważnej ingerencji w prawa osób, których dane dotyczą, która wynikałaby z ogólnego zatrzymywania przedmiotowych danych”**[164].

Podsumowując główne zastrzeżenia, jakie miał ETPC do krajowego systemu retencji danych, wydaje się, że można je uporządkować w następujący sposób. Po pierwsze, **ogólny i niezróżnicowany charakter retencji danych**. Gromadzone są dane wszystkich osób, bez należytego ich zróżnicowania i bez związku z jakimkolwiek zagrożeniem bezpieczeństwa lub porządku publicznego. Po drugie, **nieprecyzyjnie**

[161] Wyrok ETPC z dnia 28 maja 2024 r. w sprawie Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce, skargi nr 72038/17 i 25237/18; § 251 i 259.
[162] Wyrok ETPC z dnia 28 maja 2024 r. w sprawie Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce, skargi nr 72038/17 i 25237/18; § 256.
[163] Wyrok ETPC z dnia 28 maja 2024 r. w sprawie Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce, skargi nr 72038/17 i 25237/18; 262.
[164] Wyrok ETPC z dnia 28 maja 2024 r. w sprawie Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce, skargi nr 72038/17 i 25237/18; § 262.

określone cele zatrzymywania danych, co pozwala na dostęp do danych zawsze, gdy wiąże się to z realizowaniem zadań przez uprawnioną służbę (i niekoniecznie w związku z podejrzeniem popełnienia przestępstwa przez daną osobę). Po trzecie, **bezpośredni i stały dostęp do danych w związku z porozumieniami** (poufnymi porozumieniami) **zawartymi między dostawcami usług internetowych i telekomunikacyjnych, a organami (służbami) uprawnionymi do pozyskiwania danych.** Po czwarte, **nieefektywny system nadzoru sądowego nad dostępem do danych, jakie zostały zatrzymane przez dostawców usług łączności.**

Warto jednak zaznaczyć, że w wyroku Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce, w części odnoszącej się do retencji danych, ETPC nie odniósł się do kwestii obowiązku poinformowania jednostki o tym, że była poddawana niejawnej inwigilacji. W tym orzeczeniu, problem ten był analizowany w odniesieniu do kontroli operacyjnej. Nie oznacza to jednak, że chcąc wykonać wyżej wskazany wyrok, można pominąć to zagadnienie i utrzymać swoisty status *quo*, tj. brak notyfikacji. W tym aspekcie warto odnieść się do decyzji ETPC w sprawie Ringler oraz Tretter i inni przeciwko Austrii[165]. Trybunał odrzucił skargi, kwestionując posiadanie przez skarżących statusu ofiar, ale dokonał dość szczegółowej analizy mechanizmu notyfikacji, jaki wprowadzony został w Austrii. ETPC wskazał, że organy ścigania były zobowiązane do zawiadamiania niezależnego organu o wnioskach kierowanych do operatorów sieci komórkowych. Organ ten był zobligowany do poinformowania danej osoby – na jej wniosek – o środkach, jakie były stosowane wobec niej, a jeśli odmówiono udzielenia informacji – osoba ta mogła złożyć skargę do niezależnej komisji, której decyzje podlegały kontroli sądowej[166]. Mogła ona domagać się usunięcia, sprostowania lub ograniczenia przetwarzania danych osobowych, jeśli nie były już one potrzebne dla ochrony bezpieczeństwa publicznego. Oprócz nadzoru organu ochrony danych osobowych, komisji ochrony danych osobowych oraz sądowej kontroli decyzji wydawanych przez komisję, system środków ochrony praw jednostki uzupełniała instytucja Rzecznika, który miał prawo dostępu i kontroli prawidłowości stosowania przepisów o ochronie danych osobowych[167]. Choć niektóre mechanizmy (m.in. informowanie na wniosek jednostki o stosowaniu względem niej środków niejawnej inwigilacji) Trybunał uznał, za uciążliwe, a nawet pozbawione praktycznego znaczenia, to ze względu na istnienie niezależnego systemu nadzoru nad prawidłowością przetwarzania danych osobowych,

[165] Decyzja ETPC z dnia 12 maja 2020 r. w sprawie Ringler i Tretter przeciwko Austrii, skarga nr 2309/10.
[166] Decyzja ETPC z dnia 12 maja 2020 r. w sprawie Ringler i Tretter przeciwko Austrii, skarga nr 2309/10; § 55 i 44.
[167] Decyzja ETPC z dnia 12 maja 2020 r. w sprawie Ringler i Tretter przeciwko Austrii, skarga nr 2309/10; § 55 i 78.

ETPC uznał, że na środki ochrony praw i wolności jednostki dostępne na poziomie krajowym są wystarczające, a zatem interwencja strasburska nie jest konieczna.

IV.2. Orzecznictwo Europejskiego Trybunału Praw Człowieka – granice dopuszczalnej ingerencji w prawo do prywatności (art. 8 EKPC) w związku z zatrzymywaniem i dostępem do danych niedotyczących treści

IV.2.1. Dane o abonencie – wyrok ETPC z dnia 30 stycznia 2020 r. w sprawie Breyer przeciwko Niemcom

Problematyka zatrzymywania danych osobowych przez dostawców usług internetowych oraz udostępniania tych danych analizowana jest w orzecznictwie ETPC nie tylko w ujęciu systemowym, ale także w odniesieniu do konkretnych kategorii danych. W sprawie Breyer przeciwko Niemcom[168] ETPC badał, czy nałożenie obowiązku rejestracji kart pre-paidowych, a tym samym zatrzymywanie danych osobowych użytkowników (abonentów) telefonii komórkowej nie jest nieproporcjonalną ingerencją w prawo do prywatności jednostki.

Niemiecka ustawa telekomunikacyjna przewidywała, że podmiot świadczący usługi telekomunikacyjne, który przydziela numery/identyfikatory połączeń, ma przed aktywacją numery zebrać i przechowywać m.in.: imię i nazwisko oraz adres użytkownika, a w przypadku osób fizycznych datę urodzenia, a także datę wejścia w życie umowy; dodatkowo przechowywana miała być (jeśli była znana) data zakończenia umowy. Dane te miały zostać usunięte po upływie roku kalendarzowego następującego po roku, w którym zakończyła się umowa. Ustawa ustanawiała też zautomatyzowaną procedurę pozyskania danych o abonencie: operator usług łączności miał zapewnić, żeby dane te były udostępniane w sposób umożliwiający ich pozyskanie przez *Federal Network Agency* bez wiedzy dostawcy usług łączności, a także aby możliwe było wyszukiwanie przy użyciu niepełnych danych abonenckich lub funkcji podobieństwa. Katalog organów, którym dane mogły być udostępniane w tej procedurze, obejmował m.in. sądy i organy ścigania, organy bezpieczeństwa oraz inne wskazane ustawowo podmioty. Jednocześnie dostęp do danych miał funkcjonować w modelu „podwójnych drzwi": przepisy telekomunikacyjne umożliwiały „uwolnienie" danych przez

[168] Wyrok ETPC z dnia 30 stycznia 2020 r. w sprawie Breyer przeciwko Niemcom, skarga nr 50001/12.

agencję/operatora, ale konieczna była dodatkowa podstawa prawna po stronie organu, który żądał dostępu do danych abonenckich[169].

ETPC zgodził się ze skarżącym, że konieczność rejestracji kart pre-paid, przechowywanie tych danych oraz możliwość udostępnienia ich innym organom, stanowi ingerencję w prawo do prywatności (art. 8 ust. 1 EKPC). Konieczne jest jednak wyważenie interesów jednostki z interesem publicznym oraz ocena proporcjonalności zastosowanych środków w społeczeństwie demokratycznym[170]. Trybunał strasburski wskazał, że „wstępna rejestracja abonentów telefonii komórkowej w znacznym stopniu upraszcza i przyspiesza dochodzenia prowadzone przez organy ścigania i może tym samym przyczyniać się do skutecznego egzekwowania prawa oraz zapobiegania zakłóceniom porządku publicznego lub zwalczaniu przestępczości"[171], a obowiązek przechowywania informacji o abonencie był co do zasady odpowiednią odpowiedzią na zmiany w zachowaniach komunikacyjnych i w środkach telekomunikacji[172]. Chociaż ingerencji w prawo do prywatności w tej sprawie nie uznano za „błahą", to ETPC zwrócił uwagę na jej ograniczony zakres (ograniczoną naturę)[173]. Dane, jakie były przechowywane i udostępniane właściwym organom obejmowały wyłącznie dane o użytkowniku, a nie dane odnoszące się do lokalizacji, czy też dane o ruchu/transmisyjne. Nie pozwalały w żadnej mierze na ustalenie np. rodzaju i czasu połączeń, miejsca połączenia telefonicznego, czy połączenia z Internetem. ETPC badał także to, jakie zabezpieczenia przed nadużyciami wprowadzono w prawie niemieckim. Zaznaczył, że czas przechowywania danych (jeden rok od czasu rozwiązania umowy) „nie wydaje się nieodpowiedni" biorąc pod uwagę czas prowadzenia dochodzeń, a przechowywane dane są ograniczone do informacji niezbędnych do jednoznacznego zidentyfikowania użytkownika[174]. Głównym zabezpieczeniem przed nieuprawnionym dostępem – zdaniem ETPC – był mechanizm podwójnych drzwi. Organ, który chciał uzyskać dostęp do danych abonenckich musiał mieć dodatkową podstawę prawną, do złożenia stosownego wniosku[175]. Realnym ograniczeniem zakresu formułowanych żądań o te dane było wprowadzenie klauzul generalnych w postaci wymogu konieczności i

[169] § 27, 29, 98 i 100. Model double door został wyjaśniony w § 100 wyroku.
[170] Wyrok ETPC z dnia 30 stycznia 2020 r. w sprawie Breyer przeciwko Niemcom, skarga nr 50001/12; § 91.
[171] Wyrok ETPC z dnia 30 stycznia 2020 r. w sprawie Breyer przeciwko Niemcom, skarga nr 50001/12; §90.
[172] Wyrok ETPC z dnia 30 stycznia 2020 r. w sprawie Breyer przeciwko Niemcom, skarga nr 50001/12; § 90
[173] Wyrok ETPC z dnia 30 stycznia 2020 r. w sprawie Breyer przeciwko Niemcom, skarga nr 50001/12; § 95.
[174] Wyrok ETPC z dnia 30 stycznia 2020 r. w sprawie Breyer przeciwko Niemcom, skarga nr 50001/12; § 96.
[175] Wyrok ETPC z dnia 30 stycznia 2020 r. w sprawie Breyer przeciwko Niemcom, skarga nr 50001/12; § 100.

proporcjonalności[176]. Dane abonenckie miały zostać usunięte bez zbędnej zwłoki po stwierdzeniu ich nieprzydatności[177].

W odniesieniu do braku sądowej kontroli uzyskania dostępu do danych abonenckich, ETPC zwrócił uwagę na różny – w porównaniu np. z podsłuchem i niejawną inwigilacją obejmującą treść komunikatów przesyłanych drogą elektroniczną – stopień ingerencji w prywatność. Przy wyłącznie danych o użytkownikach, kontrola sądowa nie została uznana za konieczną, zwłaszcza w sytuacji, gdy każde pozyskanie danych oraz informacje o nim były rejestrowane dla celów nadzoru ochrony danych, nadzór ten sprawowały niezależne organy ochrony danych, a osoba przekonana o naruszeniu mogła wnieść skargę do tego organu[178]. W konsekwencji prawo krajowe przewiduje kontrolę „niezależnego organu". Brak notyfikacji „z urzędu" dostępu do danych o użytkowniku – przy uwzględnieniu możliwości wniesienia skargi do organu ochrony danych osobowych – nie tworzył odrębnego problemu konwencyjnego[179].

Biorąc pod uwagę zakres przechowywanych i udostępnianych danych (wyłącznie dane o użytkowniku, które nie obejmowały danych o ruchu/danych transmisyjnych i danych o lokalizacji), rodzaj zabezpieczeń przed nieuprawnionym dostępem (mechanizm tzw. podwójnych drzwi, wprowadzenie wymogu konieczności, rozliczalność pozyskania danych, nadzór niezależnego organu ochrony danych osobowych, a także możliwość złożenia skargi przez jednostkę), ETPC nie stwierdził naruszenia art. 8 EKPC. Ograniczenie prawa do prywatności jednostki uznał za proporcjonalne i konieczne w społeczeństwie demokratycznym z uwagi na przeważający interes publiczny[180].

IV.2.2. Dane o IP użytkownika – wyrok ETPC z dnia 24 kwietnia 2018 r. w sprawie Benedik przeciwko Słowenii

W sprawie Benedik przeciwko Słowenii[181] ETPC analizował m.in. problem dostępu do danych związanych z dynamicznym adresem IP oraz pozyskania informacji o

[176] Wyrok ETPC z dnia 30 stycznia 2020 r. w sprawie Breyer przeciwko Niemcom, skarga nr 50001/12; § 97-100.
[177] Wyrok ETPC z dnia 30 stycznia 2020 r. w sprawie Breyer przeciwko Niemcom, skarga nr 50001/12; § 100.
[178] Wyrok ETPC z dnia 30 stycznia 2020 r. w sprawie Breyer przeciwko Niemcom, skarga nr 50001/12; § 115
[179] Wyrok ETPC z dnia 30 stycznia 2020 r. w sprawie Breyer przeciwko Niemcom, skarga nr 50001/12; § 107.
[180] Wyrok ETPC z dnia 30 stycznia 2020 r. w sprawie Breyer przeciwko Niemcom, skarga nr 50001/12; § 110.
[181] Wyrok ETPC z dnia 24 kwietnia 2018 r. w sprawie Benedik przeciwko Słowenii, skarga nr 62357/14.

subskrypcjach w związku z podejrzeniem popełnienia przestępstw seksualnych na szkodę małoletnich. Przepisy obowiązujące wówczas w Słowenii nie regulowały w sposób dostatecznie jasny i szczegółowy możliwości przekazania – na potrzeby postępowania karnego – danych abonenta powiązanych z dynamicznym adresem IP. Mechanizm żądania od operatora usług łączności informacji o „użytkowniku środka komunikacji elektronicznej" nie zawierał szczegółowych reguł odnoszących się do powiązania dynamicznego IP z danymi abonenta. Pozyskując dane dotyczące adresu IP, w związku z prowadzonym śledztwem w sprawie o seksualne wykorzystanie małoletnich oraz rozpowszechnianie materiałów o charakterze pedofilskim, służby policyjne zidentyfikowały ojca skarżącego, a nie samego skarżącego. Dopiero w wyniku dalszych czynności policyjnych ustalono, że to skarżący posiadał i rozpowszechniał materiały o charakterze pedofilskim[182].

Ponieważ sprawa dotyczyła wykorzystania seksualnego dzieci – przestępstwa o wyjątkowej społecznej szkodliwości i wyniszczających skutkach dla ofiar[183] - ETPC przypomniał, że państwo musi dysponować narzędziami pozwalającymi na skuteczne zwalczanie tego typu czynów zabronionych[184]. Ochrona dzieci przed seksualnym wykorzystaniem obejmuje potrzebę identyfikacji sprawców i pociągnięcia ich do odpowiedzialności karnej[185], co może wiązać się z wprowadzeniem metod śledczych ingerujących w prywatność jednostki. Niemniej, każda ingerencja w prawo wynikające z art. 8 ust. 1 EKPC, musi mieć odpowiednią podstawę prawną oraz spełniać wymogi „jakości prawa". W analizowanej sprawie, spornym zagadnieniem było to, czy – z uwagi na treść przepisów krajowych – skarżący mógł racjonalnie (rozsądnie) oczekiwać respektowania prawa do prywatności korzystając z dynamicznego adresu IP[186].

ETPC wskazał, że skarżący wymieniając się plikami pornograficznymi z udziałem małoletnich za pośrednictwem sieci Razorback subiektywnie oczekiwał, że jego aktywność pozostanie prywatna, a tożsamość nie zostanie ujawniona. Fakt, że nie ukrył

[182] Policja uzyskała nakaz sądowy pozwalający na pozyskanie danych z IP, powiązała dane z IP z lokalizacją komputera i potencjalnie z osobą. Informacje o użytkowniku IP pozwoliły zidentyfikować dom, z którego łączono się z internetem. Wyrok ETPC z dnia 24 kwietnia 2018 r. w sprawie Benedik przeciwko Słowenii, skarga nr 62357/14; § 113.

[183] Wyrok ETPC z dnia 24 kwietnia 2018 r. w sprawie Benedik przeciwko Słowenii, skarga nr 62357/14; § 99

[184] Zob. także: decyzja ETPC z dnia 2 grudnia 2008 r. w sprawie K.U. przeciwko Finlandii, skarga nr 2872/02; § 46.

[185] Tak: wyrok ETPC z dnia 24 kwietnia 2018 r. w sprawie Benedik przeciwko Słowenii, skarga nr 62357/14; § 99; decyzja ETPC z dnia 2 grudnia 2008 r. w sprawie K.U. przeciwko Finlandii, skarga nr 2872/0246; § 46.

[186] Wyrok ETPC z dnia 24 kwietnia 2018 r. w sprawie Benedik przeciwko Słowenii, skarga nr 62357/14; § 101 i 115.

on adresu dynamicznego IP, nie mógł być rozstrzygający przy ocenie oczekiwania prywatności z obiektywnego punktu widzenia. Problem nie leżał bowiem w tym, czy skarżący oczekiwał utrzymania w tajemnicy dynamicznego IP, ale czy rozsądnie mógł oczekiwać poszanowania prywatności w odniesieniu do swojej tożsamości[187]. Trybunał przypomniał, że anonimowość jest ważnym elementem aktywności internetowej[188]. Skarżący nigdy nie ujawnił swojej tożsamości, nie był identyfikowalny przez administratora konkretnej strony oraz podane dane kontaktowe[189]. Jego aktywność online obejmowała więc wysoki stopień anonimowości, „co potwierdza fakt, że przypisany dynamiczny adres IP – nawet jeśli widoczny dla innych użytkowników sieci – nie mógł zostać powiązany z konkretnym komputerem bez weryfikacji danych przez ISP po żądaniu policji”[190]. Z perspektywy obowiązującego wówczas prawa, oczekiwanie skarżącego co do prywatności jego aktywności online nie mogło zostać uznane za bezzasadne lub nierozsądne. Trybunał stwierdził, że uzyskanie danych abonenta powiązanych z dynamicznym adresem IP cechował się brakiem jasności, a przepisy krajowe nie zapewniały wystarczających zabezpieczeń przed arbitralną ingerencją w prawa z art. 8 EKPC[191]. W czasie, kiedy pozyskano dane o dynamicznym IP, a następnie powiązano je ze skarżącym, nie istniały przepisy[192] „określające warunki retencji danych uzyskanych na podstawie art. 149b ust. 3 KPK ani zabezpieczenia przed nadużyciami ze strony funkcjonariuszy państwowych w procedurze dostępu do takich danych i ich przekazywania. Co do tych ostatnich, policja – dysponując informacjami o konkretnej aktywności online – mogła zidentyfikować autora, po prostu prosząc ISP o sprawdzenie tych danych. (...) nie wykazano, by w relewantnym czasie istniał niezależny nadzór nad korzystaniem z tych uprawnień policyjnych, mimo że – zgodnie z wykładnią sądów krajowych – uprawnienia te zmuszały dostawców usług łączności do odszukania przechowywanych danych połączeń i umożliwiały policji powiązanie znacznej ilości informacji o aktywności online z konkretną osobą bez jej zgody”[193]. Mimo znacznej społecznej szkodliwości czynów zarzuconych skarżącemu oraz obowiązku zwalczania

[187] Wyrok ETPC z dnia 24 kwietnia 2018 r. w sprawie Benedik przeciwko Słowenii, skarga nr 62357/14; § 115 i 116.

[188] Tak: wyrok ETPC z dnia 16 czerwca 2015 r. w sprawie Delfi AS przeciwko Estonii, skarga nr 64569/09.

[189] Wyrok ETPC z dnia 24 kwietnia 2018 r. w sprawie Benedik przeciwko Słowenii, skarga nr 62357/14; § 117 i 33.

[190] Wyrok ETPC z dnia 24 kwietnia 2018 r. w sprawie Benedik przeciwko Słowenii, skarga nr 62357/14; § 117.

[191] Wyrok ETPC z dnia 24 kwietnia 2018 r. w sprawie Benedik przeciwko Słowenii, skarga nr 62357/14; § 132.

[192] Warto podkreślić, że po przepisy w Słowenii zostały zmienione już po skazaniu skarżącego i wprowadzono odpowiednią podstawę prawną do pozyskania danych o IP.

[193] Wyrok ETPC z dnia 24 kwietnia 2018 r. w sprawie Benedik przeciwko Słowenii, skarga nr 62357/14; § 130.

przestępczości seksualnej wobec małoletnich, ETPC uznał, że ingerencja w prawo do prywatności – tj. przełamanie anonimowości i identyfikacja tożsamości skarżącego – nie miały odpowiedniej podstawy prawnej. Regulacja słoweńska i praktyka organów ścigania były niejasne i brak było wystarczających zabezpieczeń przed arbitralnością (w tym także niezależnego nadzoru oraz reguł dotyczących retencji i dostępu do takich danych).

IV.2.3. Dane o lokalizacji – wyrok ETPC z dnia 8 lutego 2018 r. w sprawie Ben Faiza przeciwko Francji

Jeśli chodzi o dane lokalizacyjne, to ETPC rozróżnia dwie sytuacje – pozyskiwanie danych lokalizacyjnych w czasie rzeczywistym w wyniku zainstalowania nadajników GPS w samochodzie[194] oraz danych historycznych od operatorów dostawców usług łączności. W sprawie Ben Faiza przeciwko Francji[195], Trybunał analizował obie metody gromadzenia danych niedotyczących treści. Skarżący został skazany m.in. za przemyt narkotyków, pranie pieniędzy i udział w zorganizowanej grupie przestępczej. Prowadzone postępowanie przygotowawcze wymagało od organów ścigania zastosowania metod inwigilacyjnych i m.in. zainstalowany został nadajnik GPS w samochodzie skarżącego, który pozwalał na śledzenie lokalizacji w czasie rzeczywistym[196] oraz pozyskano od dostawców usług łączności historyczne dane o lokalizacji[197].

W odniesieniu do zainstalowania nadajnika GPS Trybunał wskazał, że prawo francuskie nie przewidywało – w tamtym okresie – takiej metody śledczej. Przepisy k.p.k. posługiwały się ogólnym sformułowaniem czynności wskazanych do ustalenia prawdy[198]. Nie były to przepisy wystarczająco precyzyjne i przewidywalne dla jednostki, i ETPC uznał, że doszło do naruszenia art. 8 ust. 1 EKPC z uwagi na brak odpowiedniej postawy prawnej do ingerencji w prywatność jednostki. W odniesieniu do wezwania skierowanego do operatora sieci komórkowej[199] do udostępnienia m.in. danych lokalizacyjnych, ETPC wskazał, że przepisy francuskie upoważniały prokuratora (lub inne organy śledcze, ale za zgodą prokuratora) do żądania wydania dokumentów

[194] Zob. także wyrok ETPC z dnia 2 września 2010 r. w sprawie Uzun przeciwko Niemcom, skarga nr 35623/05.
[195] Wyrok ETPC z dnia 8 lutego 2018 r. w sprawie Ben Faiza przeciwko Francji, skarga nr 31446/12.
[196] Wyrok ETPC z dnia 8 lutego 2018 r. w sprawie Ben Faiza przeciwko Francji, skarga nr 31446/12; § 14.
[197] Wyrok ETPC z dnia 8 lutego 2018 r. w sprawie Ben Faiza przeciwko Francji, skarga nr 31446/12; § 7.
[198] Wyrok ETPC z dnia 8 lutego 2018 r. w sprawie Ben Faiza przeciwko Francji, skarga nr 31446/12; § 58.
[199] Dotyczyło ono nie tylko danych lokalizacyjnych, ale też danych z bilingów. Wyrok ETPC z dnia 8 lutego 2018 r. w sprawie Ben Faiza przeciwko Francji, skarga nr 31446/12; § 66

niezbędnych dla prowadzonego postępowania karnego[200]. W analizowanej sprawie chodziło o pozyskanie danych już zapisanych w systemie operatora (połączenia przychodzące i wychodzące oraz stacje bazowe), co miało adekwatną podstawę prawną w prawie krajowym[201]. ETPC przypomniał także, że nie można wymagać od ustawodawcy stworzenia zamkniętego katalogu dokumentów możliwych do żądania na etapie postępowania przygotowawczego. Odnotował także, że przepisy zostały skonkretyzowane w orzecznictwie krajowym w zakresie żądania dostępu do danych niedotyczących treści[202].

W zakresie zabezpieczeń przed arbitralnością pozyskania danych o lokalizacji, ETPC zwrócił uwagę na dwa elementy. Po pierwsze, obowiązek uprzedniej zgody prokuratury na wezwania dokonywane przez funkcjonariusza policji, którego pominięcie skutkowałoby nieważnością czynności. Po drugie możliwość kontroli sądowej legalności środka w toku postępowania karnego, łącznie z uprawnieniem sądu do wyeliminowania dowodów uzyskanych z naruszeniem prawa[203]. Jednocześnie Trybunał wyraźnie odróżnił metody pozwalające lokalizować osobę „historycznie" (lokalizacja a posteriori) od metod umożliwiających lokalizowanie w czasie rzeczywistym. Te drugie, co do zasady, mogą w większym stopniu ingerować w prywatność. Przekazanie listy stacji bazowych uruchomionych przez numer telefonu pozwala na poznanie wcześniejszych pozycji geograficznych użytkownika, ale nadal chodzi o przekazanie danych już istniejących i przechowywanych, a nie o proaktywne śledzenie trasy w danym momencie[204].

ETPC nie stwierdził naruszenia EKPC w tym aspekcie (tj. w aspekcie sięgania po dane historyczne w formie zwrócenia się do dostawców usług łączności o przekazanie danych lokalizacyjnych). Wskazał, że zwrócenie się do dostawców usług łączności o przekazanie m.in. danych lokalizacyjnych służyło istotnym celom, tj. zapobieganiu i zwalczaniu poważnej przestępczości[205]. Trybunał wziął także pod uwagę realną kontrolę legalności i proporcjonalności uzyskania dostępu do danych lokalizacyjnych[206].

[200] Wyrok ETPC z dnia 8 lutego 2018 r. w sprawie Ben Faiza przeciwko Francji, skarga nr 31446/12; § 70.
[201] Wyrok ETPC z dnia 8 lutego 2018 r. w sprawie Ben Faiza przeciwko Francji, skarga nr 31446/12; § 71.
[202] Wyrok ETPC z dnia 8 lutego 2018 r. w sprawie Ben Faiza przeciwko Francji, skarga nr 31446/12; § 72.
[203] Wyrok ETPC z dnia 8 lutego 2018 r. w sprawie Ben Faiza przeciwko Francji, skarga nr 31446/12; § 73.
[204] Wyrok ETPC z dnia 8 lutego 2018 r. w sprawie Ben Faiza przeciwko Francji, skarga nr 31446/12; § 74.
[205] Wyrok ETPC z dnia 8 lutego 2018 r. w sprawie Ben Faiza przeciwko Francji, skarga nr 31446/12; § 77.
[206] Wyrok ETPC z dnia 8 lutego 2018 r. w sprawie Ben Faiza przeciwko Francji, skarga nr 31446/12; § 78-80.

W kontekście pozyskiwania od dostawców usług łączności danych o lokalizacji, warto także odnotować wyrok ETPC w sprawie Sedletska przeciwko Ukrainie[207]. W tej sprawie ETPC analizował kwestię pozyskania danych o lokalizacji od dostawców usług łączności w kontekście ochrony dziennikarskich źródeł informacji[208]. Wzorcem kontroli, zastosowanym przez ETPC był zatem art. 10 EKPC. Sąd krajowy[209], pozwalając na dostęp do danych o lokalizacji dziennikarki, nie wykazał istnienia przeważającego interesu publicznego w przełamaniu tajemnicy dziennikarskiej[210]. ETPC zwrócił uwagę na: 1) okres[211], za jaki pozyskano dane, tj. 16 miesięcy wstecz, co zwiększało ryzyko dostępu do danych niezwiązanych w żaden sposób ze sprawą, 2) ogólne uzasadnienie sprowadzające się do wymogów „efektywności śledztwa" oraz 3) brak analizy subsydiarności i proporcjonalności ingerencji, tj. czy środki mniej ingerujące w prywatność jednostki byłyby równie efektywne[212]. Trybunał uznał, że doszło do naruszenia art. 10 EKPC, ponieważ dostęp do danych lokalizacyjnych w okolicznościach analizowanej sprawy nie był konieczny w społeczeństwie demokratycznym i nie można uznać go za uzasadniony z uwagi na przeważający interes publiczny[213].

IV.2.4. Dane o ruchu (dane transmisyjne) – wyrok ETPC z dnia 15 lutego 2024 r. w sprawie Skorbene przeciwko Słowenii

W sprawie Skorbene przeciwko Słowenii[214] ETPC analizował m.in. kwestię zatrzymywania i dostępu do danych telekomunikacyjnych (danych z billingów) skarżącego, będącego sędzią, który był podejrzewany o popełnienie przestępstw

[207] Wyrok ETPC z dnia 1 kwietnia 2021 r. w sprawie Sedletska przeciwko Ukrainie, skarga nr 42634/18.
[208] O znaczeniu ochrony dziennikarskich źródeł informacji zob. szerzej: wyrok ETPC z dnia 1 kwietnia 2021 r. w sprawie Sedletska przeciwko Ukrainie, skarga nr 42634/18, § 54 i 55 i cytowane tam orzecznictwo.
[209] Konkretnie sędzia śledczy działając na wniosek prokuratora. Zob.: wyrok ETPC z dnia 1 kwietnia 2021 r. w sprawie Sedletska przeciwko Ukrainie, skarga nr 42634/18; § 16 i następne.
[210] Wyrok ETPC z dnia 1 kwietnia 2021 r. w sprawie Sedletska przeciwko Ukrainie, skarga nr 42634/18; § 70.
[211] Zob. szerzej: wyrok ETPC z dnia 1 kwietnia 2021 r. w sprawie Sedletska przeciwko Ukrainie, skarga nr 42634/18§ 61 i następne.
[212] Wyrok ETPC z dnia 1 kwietnia 2021 r. w sprawie Sedletska przeciwko Ukrainie, skarga nr 42634/18; § 71.
[213] Wyrok ETPC z dnia 1 kwietnia 2021 r. w sprawie Sedletska przeciwko Ukrainie, skarga nr 42634/18; § 72.
[214] Wyrok ETPC z dnia 15 lutego 2024 r. w sprawie Skorbene przeciwko Słowenii, skarga nr 19920/20.

korupcyjnych[215]. Dane z billingów zostały następnie wykorzystane w procesie karnym jako jeden z dowodów obciążających[216].

Trybunał w omawianym wyroku dokonał analizy słoweńskich przepisów – ówcześnie obowiązujących – dotyczących retencji danych. Nakładały one na dostawców usług łączności obowiązek zatrzymywania przez okres 14 miesięcy m.in. danych z billingów dla realizacji bardzo ogólnie określonych celów, tj. dla celów postępowania karnego oraz zapewnienia bezpieczeństwa narodowego, porządku konstytucyjnego, bezpieczeństwa oraz politycznych i gospodarczych interesów państwa, jak również obrony narodowej[217]. Trybunał uznał, że słoweńskie przepisy o retencji danych i dostępie do tych danych nie spełniały wymogu „jakości prawa" i nie były zdolne do ograniczenia ingerencji w prawa skarżącego z art. 8 EKPC do tego, co jest konieczne w społeczeństwie demokratycznym. W konsekwencji zaś, zarówno sam obowiązek retencji danych, jak i ich wykorzystanie i przetwarzanie naruszyły art. 8 EKPC.

W uzasadnieniu ETPC odwołał się do wyroku Breyer przeciwko Niemcom. O ile jednak w tamtej sprawie, zakres zatrzymywanych i udostępnianych danych był wąski (odnosił się do danych abonenckich), o tyle sprawa Skorbene przeciwko Słowenii odnosiła się do danych telekomunikacyjnych. Trybunał przypomniał, że dane te po powiązaniu z abonentem lub użytkownikiem – mogą ujawniać intymny obraz jego życia poprzez mapowanie sieci społecznych, śledzenie lokalizacji, mapowanie wzorców komunikacji oraz wgląd w to, z kim dana osoba wchodziła w interakcje[218]. Zdaniem ETPC **„systemowa inwigilacja wynikająca z obowiązkowej retencji danych telekomunikacyjnych stanowi przeszkodę w korzystaniu z praw do prywatności przez wszystkich użytkowników usług telekomunikacyjnych. Istnienie dużych zbiorów danych telekomunikacyjnych i ciągła retencja takich danych mogą w zrozumiały sposób rodzić poczucie podatności i narażenia oraz mogą negatywnie wpływać na możliwość korzystania z prywatności i poufności korespondencji, rozwijania relacji z innymi oraz wykonywania innych praw podstawowych[219].**

[215] Wyrok ETPC z dnia 15 lutego 2024 r. w sprawie Skorbene przeciwko Słowenii, skarga nr 19920/20; § 10.
[216] Zob. jednak: wyrok ETPC z dnia 15 lutego 2024 r. w sprawie Skorbene przeciwko Słowenii, skarga nr 19920/20§ 146.
[217] Wyrok ETPC z dnia 15 lutego 2024 r. w sprawie Skorbene przeciwko Słowenii, skarga nr 19920/20; § 64 i 126.
[218] Wyrok ETPC z dnia 15 lutego 2024 r. w sprawie Skorbene przeciwko Słowenii, skarga nr 19920/20; § 133.
[219] Wyrok ETPC z dnia 15 lutego 2024 r. w sprawie Skorbene przeciwko Słowenii, skarga nr 19920/20; § 133.

ETPC przyjął, że ingerencja w prawo do prywatności w związku z szeroko zakreślonym obowiązkiem retencji danych, miała poważny charakter. Z perspektywy zgodności z art. 8 ust. 2 EKPC nie jest wystarczające to, że określone działania polegające na niejawnej inwigilacji będą skuteczne w zwalczaniu poważnej przestępczości. Kluczowe jest bowiem zachowanie uczciwej równowagi pomiędzy konkurującymi ze sobą wartościami – interesem publicznym i prawami jednostki. Nawet w przypadku ochrony bezpieczeństwa narodowego i zwalczania poważnej przestępczości, kiedy państwa dysponują szerszym marginesem swobody w zakresie limitowania praw i wolności jednostki, margines ten podlega kontroli Trybunału[220].

Trybunał zauważył, że dla celów interesu publicznego przepisy słoweńskie wymagały zatrzymywania wszystkich danych niedotyczących treści generowanych lub przetwarzanych w toku świadczenia usług łączności. Każda osoba lub podmiot korzystający z usług dostawców telekomunikacyjnych w Słowenii mógł przewidywać, że jego dane telekomunikacyjne są zatrzymywane. Jednoznaczność ustawy, ustanawiającej jako zasadę ogólną i niezróżnicowaną retencję danych telekomunikacyjnych, nie mogła sama w sobie stanowić wystarczającej gwarancji zgodności z zasadami praworządności i proporcjonalności. Przepisy w żaden sposób, poza wprowadzeniem 14-miesięcznego okresu zatrzymywania danych, nie ograniczały zakresu zastosowania obowiązku retencji danych. Retencja danych miała charakter systemowy, uogólniony i niezróżnicowany. ETPC uznał, że brak przepisów lub mechanizmów mających zapewnić, że środek był faktycznie ograniczony do tego, co „konieczne w społeczeństwie demokratycznym" dla realizacji celów w postaci ochrony bezpieczeństwa narodowego, zwalczania przestępczości itp. czynił taki reżim nie do pogodzenia z obowiązkami państwa na gruncie art. 8 EKPC[221].

Trybunał ocenił także zagadnienie wykorzystania danych retencyjnych w procesie karnym. Na etapie procesu karnego, kiedy skarżący wskazywał, że dane telekomunikacyjne były zatrzymywane z naruszeniem prawa do prywatności, a ocena sądu orzekającego w sprawie była ograniczona wyłącznie do zbadania przesłanek formalnych – tj. czy dane zostały zatrzymane w związku z realizacją odpowiedniego celu, a także, czy zgodę na dostęp wyraził właściwy sąd. ETPC wskazał, że „jeżeli retencja danych telekomunikacyjnych zostaje uznana za naruszającą art. 8 EKPC z powodu niespełnienia wymogu „jakości prawa" i/lub zasady proporcjonalności, to dostęp do

[220] Wyrok ETPC z dnia 15 lutego 2024 r. w sprawie Skorbene przeciwko Słowenii, skarga nr 19920/20; § 136.
[221] Wyrok ETPC z dnia 15 lutego 2024 r. w sprawie Skorbene przeciwko Słowenii, skarga nr 19920/20; § 139.

tych danych – oraz ich późniejsze przetwarzanie i przechowywanie przez władze – z tego samego powodu nie może być zgodny z art. 8 EKPC”[222].

IV.3. Strasburski model retencji i dostępu do danych niedotyczących treści – minimalne wymogi regulacji ustawowej

W orzecznictwie ETPC retencja danych niedotyczących treści oraz dostęp do tych danych są traktowane jako odrębne ingerencje w prawo do poszanowania życia prywatnego (art. 8 EKPC). Współczesne możliwości technologiczne powodują, iż metadane komunikacyjne – w szczególności dane o abonencie, dane o ruchu/transmisyjne oraz dane o lokalizacji – mogą dostarczać precyzyjnych informacji o życiu jednostki, a w warunkach masowego przechwytywania i łączenia kategorii danych mogą prowadzić do ustalenia „intymnego portretu” danej osoby. W konsekwencji pozyskiwanie powiązanych danych dotyczących komunikacji, a następnie ich wykorzystanie w sprawie karnej, może być tak samo inwazyjne jak pozyskiwanie treści komunikatów. Zatrzymywanie danych niedotyczących treści, a także możliwość przeszukiwania tych danych, powiązywania określonych informacji itp. powinny być zatem analizowane w świetle zabezpieczeń właściwych dla niejawnej inwigilacji. Nie jest jednak niezbędne, by regulacje dotyczące metadanych były identyczne pod każdym względem z regulacjami dotyczącymi „klasycznej” niejawnej inwigilacji, obejmującej dostęp do komunikatów przesyłanych np. drogą elektroniczną za pośrednictwem dostawców usług łączności[223].

Jak to już zostało wcześniej wskazane, nałożenie na dostawców usług łączności obowiązku zatrzymywania danych niedotyczących treści należy odróżnić od dostępu organów publicznych do danych zatrzymywanych. Oba etapy stanowią odrębne ingerencje w prawo do prywatności i każdy z nich musi spełniać wymóg legalności oraz konieczności w społeczeństwie demokratycznym (art. 8 EKPC). **Jednocześnie Trybunał strasburski podkreśla, że jeśli system retencji danych niedotyczących treści nie spełnia wymogów art. 8 EKPC (w szczególności ze względu na brak „jakości prawa” lub brak proporcjonalności ingerencji), to późniejszy dostęp do takich danych oraz ich dalsze przetwarzanie np. w związku z wykorzystaniem jako dowód w procesie karnym również nie może zostać uznane za zgodne z art. 8 EKPC.**

[222] Wyrok ETPC z dnia 15 lutego 2024 r. w sprawie Skorbene przeciwko Słowenii, skarga nr 19920/20; § 144

[223] Por.: wyrok ETPC z dnia 11 stycznia 2022 r. w sprawie Ekimdzhiev i inni przeciwko Bułgarii, skarga nr 70078/12; § 395.

Próbując zrekonstruować model retencji danych i dostępu do danych retencyjnych w orzecznictwie ETPC można wskazać na następujące elementy.

Po pierwsze, ingerencja musi odbywać się na podstawie przepisów prawa krajowego, które są dostatecznie jasne i przewidywalne dla jednostki. Chodzi bowiem oto, by jednostka mogła racjonalnie ocenić, w jakich sytuacjach i na jakich zasadach jej dane mogą zostać zatrzymane (retencja danych) oraz udostępnione innym organom władzy publicznej. Regulacje krajowe powinny jednocześnie ograniczać uznaniowość organów, tj. zawierać kryteria i procedury, które zmniejszają ryzyko arbitralnego sięgania po dane. Prawo powinno co najmniej określać:

1. cele retencji danych oraz cele dostępu do danych retencyjnych;
2. kategorie danych objętych obowiązkiem zatrzymywania oraz to, jakie dane – i w jakich sytuacjach – mogą zostać udostępnione;
3. okres przechowywania danych oraz zasady ich usuwania;
4. warunki i tryb dostępu do danych retencyjnych przez inne organy (np. policję, prokuraturę lub sądy);
5. mechanizmy nadzoru i kontroli zewnętrznej sprawowanych przez niezależne organy.

Po drugie, prawo krajowe powinno regulować retencję i dostęp do danych niedotyczących treści w sposób ograniczający ingerencję do tego, co jest konieczne w społeczeństwie demokratycznym (art. 8 ust. 2 EKPC). Analizując orzeczenia ETPC można wskazać na trzy grupy ograniczeń:

- zakresowe (jakie dane są zatrzymywane i udostępniane; tj. czy są to dane o abonencie, czy dane o lokalizacji, czy dane o IP, czy dane o ruchu/transmisyjne itp.);

- czasowe (jaki jest okres retencji danych, a także jaki okres obejmuje żądanie dostępu do danych niedotyczących treści);

- celowe/kierunkowe (dla realizacji jakich celów dane są zatrzymywane i udostępnianie).

Warto jednak wskazać, że sama jednoznaczność ustawy ustanawiającej powszechny, uogólniony i niezróżnicowany obowiązek retencji wszystkich rodzajów danych niedotyczących treści nie stanowi wystarczającej gwarancji zgodności z art. 8 EKPC,

jeżeli regulacja – poza wskazaniem okresu przechowywania – nie zawiera rozwiązań zdolnych w praktyce ograniczyć zakres ingerencji i ryzyko nadużyć.

Po trzecie, uogólniona i niezróżnicowana retencja danych abonenckich jest co do zasady niezgodna z art. 8 EKPC. Warto jednak podkreślić, że ETPC nie zanegował w sposób absolutny dopuszczalności uogólnionej i niezróżnicowanej retencji danych o ruchu/transmisyjnych i danych o lokalizacji oraz danych o lokalizacji. W określonych sytuacjach, w szczególności w związku z realizacją celu w postaci ochrony bezpieczeństwa narodowego, a także w kontekście działań służb wywiadowczych i przechwytywania komunikacji transgranicznej, taki środek może okazać się proporcjonalny i niezbędny w społeczeństwie demokratycznym. Ważne jest jednak to, by prawo krajowe przewidywało system gwarancji dla jednostki, który ograniczy ryzyko niekontrolowanej ingerencji i wykorzystania informacji dla realizacji innych celów (np. zwalczanie przestępczości niezwiązanej w żaden sposób z ochroną bezpieczeństwa narodowego).

Po czwarte, przepisy krajowe powinny uwzględniać to, że intensywność ingerencji w prawo do prywatności jest różna w zależności od kategorii danych niedotyczących treści oraz od tego, jakie wnioski można z nich wyprowadzić. Dane identyfikacyjne abonenta/użytkownika nie wiążą się z tak dużym stopniem ingerencji w prawo do prywatności, jak dane pozwalające rekonstruować aktywność jednostki, sieć jej relacji społecznych lub wzorce przemieszczania się. W odniesieniu do danych lokalizacyjnych prawo krajowe powinno rozróżniać dane lokalizacji historycznej (pozyskiwane *ex post* z danych już zapisanych u operatora) od metod umożliwiających lokalizowanie w czasie rzeczywistym. Te drugie są co do zasady bardziej dolegliwe z perspektywy prawa do prywatności i wymagają wyraźnej podstawy prawnej (w tym także co do metod pozwalających na śledzenie lokalizacji w czasie rzeczywistym) oraz silniejszych gwarancji proceduralnych. Z kolei dane o ruchu/transmisyjne (np. dane billingowe) – po powiązaniu z abonentem – mogą ujawniać intymny obraz życia jednostki, co uzasadnia ostrzejszą ocenę uogólnionej i niezróżnicowanej retencji oraz dostępu do tych danych.

Po piąte, ustawodawca krajowy– wprowadzając przepisy o retencji danych oraz ich udostępnianiu – powinien patrzeć na to zagadnienie systemowo/modelowo. Cały cykl zatrzymywania, przechowywania, przetwarzania i udostępniania danych niedotyczących treści powinien być uregulowany w powszechnie dostępnych i zrozumiałych dla jednostki przepisach prawa. Nie jest wystarczające wskazanie, że dane są przechowywane przez określony czas i mogą być udostępnione „uprawnionym organom". Przepisy powinny precyzować zasady wykorzystania, dalszego

przechowywania i niszczenia danych, tak aby ingerencja była ograniczona do celu, dla którego została wprowadzona, oraz aby minimalizować ryzyko wtórnego, niekontrolowanego wykorzystywania danych.

Po szóste, prawo krajowe powinno przewidywać efektywny nadzór nad dostępem do danych niedotyczących treści i ich wykorzystaniem, w szczególności w sytuacji, gdy wprowadzony stał model tzw. stałego łącza, tj. dostęp do danych niedotyczących treści bez udziału dostawcy usług łączności. Taki model jest szczególnie podatny na nadużycia, jeżeli nie towarzyszą mu gwarancje pozwalające na realną kontrolę, identyfikację osób uzyskujących dostęp oraz weryfikację celowości i proporcjonalności konkretnych operacji. Raportowanie w postaci ogólnych statystyk nie zapewnia realnej kontroli nad tym, kto, kiedy, na jakiej podstawie i w jakim celu uzyskał dostęp do danych, jak te dane zostały wykorzystane itp.

V. Ponadustawowy (konstytucyjny, unijny i strasburski) model retencji i dostępu do danych niedotyczących treści – minimalne wymogi regulacji ustawowej

Łączna analiza standardów ponadustawowych – konstytucyjnego, unijnego i konwencyjnego – prowadzi do wniosku, że nie są to standardy konkurujące, ale komplementarne. Akcenty, w zależności od tego, czy jest to standard wynikający z prawa unijnego, czy konstytucyjnego, czy wyinterpretowany z orzecznictwa strasburskiego, są rozłożone odmiennie. Przykładowo, prawo unijne bardziej koncentruje się na samym obowiązku retencji, standard konstytucyjny – na dostępie do danych retencyjnych. Trybunał strasburski analizuje to zagadnienie z perspektywy poszanowania praw i wolności jednostki[224].

Próbując uporządkować, jakie są minimalne wymogi regulacji ustawowej, można wskazać na następujące elementy, które powinny znaleźć odzwierciedlenie w prawie krajowym. Przepisy krajowe powinny być dostępne dla jednostki (wymóg dostępności prawa), przewidywalne (tj. by można było racjonalnie ocenić, czy dane danej osoby są zatrzymywane) i odpowiednio precyzyjne. Muszą określać:

- jakie dane niedotyczące treści są zatrzymywane (czy wszystkie dane, czy dane abonenckie, czy dane o IP, itp.);

- cele, dla realizacji których dane niedotyczące treści są zatrzymywane (np. dla realizacji celu w postaci zapewnienia bezpieczeństwa narodowego, zwalczania poważnej przestępczości, itd.). Cele nie powinny być określone zbyt szeroko (przepisy nie powinny być blankietowe);

- jakie organy mogą mieć dostęp do danych retencyjnych oraz należy precyzyjnie określić tryb dostępu do danych; tryb dostępu (obejmujący przesłanki dostępu do danych, procedurę dostępu oraz mechanizmy kontroli) do danych powinien chronić przez arbitralnością sięgania po dane niedotyczące treści i nadużywaniem tej metody gromadzenia danych o jednostce;

[224] Warto także zauważyć, że wraz ze zmianami technologicznymi w ostatnich 15 latach, zmieniało się także orzecznictwo trybunałów europejskich. Na tym tle wyrok Trybunału Konstytucyjnego w sprawie K 23/11 może wydawać się zachowawczy. Należy jednak analizować go w kontekście historycznym, z czasu, kiedy to orzeczenie zostało wydane. Przyjmując taką perspektywę, wskazania zawarte w treści uzasadnienia, mają w zasadzie uniwersalny – i bardzo aktualny – charakter.

- czas przechowywania danych niedotyczących treści u dostawców usług łączności;

- mechanizmy nadzoru nad zatrzymywaniem i udostępnianiem danych oraz gwarancje proceduralne dla jednostki, które chroniłby ją przed nadużyciami.

Retencja danych

W kontekście nałożenia na dostawców usług łączności obowiązku zatrzymywania danych niedotyczących treści, **uogólniona, niezróżnicowana i stała retencja danych lokalizacyjnych i transmisyjnych (danych o ruchu) jest co do zasady niedopuszczalna. Możliwe jest czasowe wprowadzenie uogólnionej i niezróżnicowanej retencji danych w sytuacji, gdy na terytorium danego państwa występuje realne zagrożenie dla bezpieczeństwa narodowego. Po ustaniu takiego zagrożenia, dalsze utrzymywanie retencji wszystkich danych, wszystkich użytkowników usług łączności, jest nadmiarowe.** W szczególności niedopuszczalna jest uogólniona i niezróżnicowana retencja danych w związku z potrzebami bezpieczeństwa powszechnego czy zwalczania poważnej przestępczości. TSUE dopuszcza w takiej sytuacji ukierunkowaną retencję danych o ruchu i danych lokalizacyjnych w oparciu o obiektywne i niedyskryminacyjne kryteria (np. w obszarach, gdzie występuje zwiększone ryzyko przestępczości). Cele związane ze zwalczaniem poważnych przestępstw, czy ochroną bezpieczeństwa powszechnego są istotne, ale znajdują się niżej w swoistej „hierarchii celów", jaka wynika z orzecznictwa Trybunału w Luksemburgu.

Dane abonenckie (dane o abonencie) oraz dane o IP nie wiążą się z aż tak poważną ingerencją w prywatność jednostki. Nie pozwalają bowiem na odwzorowanie np. kręgu towarzyskiego, schematów poruszania się, zwyczajów, itp. Możliwe jest zatem – co do zasady – ich uogólnione i niezróżnicowane zatrzymywanie z uwagi na przeważający interes publiczny.

Przepisy o retencji poszczególnych kategorii danych niedotyczących treści powinny wskazywać cel zatrzymywania. TSUE i ETPC podkreślają, że sformułowania nadmiernie ogólnikowe (np. zapobieganie i zwalczanie przestępczości) nie spełniają wymogów „jakości" prawa i przewidywalności dla jednostki. Warto także zwrócić uwagę na stanowisko Komisji Weneckiej, która sygnalizowała, że konkretne regulacje o tym, jakie dane są zatrzymywane powinny być unormowane w akcie prawnym o randze ustawy.

Z orzecznictwa TSUE i ETPC nie wynikają wprost wskazania odnośnie do maksymalnych terminów retencji danych. Oba trybunały kazuistycznie badają określone porządki

prawne biorąc pod uwagę rodzaj danych, cele ich zatrzymywania, okoliczności sprawy, czy potencjalne zagrożenia dla tajemnic prawnie chronionych. W odniesieniu do danych o ruchu i danych o lokalizacji zwracają uwagę, że nawet krótkookresowe (kilku/kilkunastotygodniowe) zatrzymywanie jest już istotną ingerencją w prawo do prywatności, a przechowywanie danych za 14 czy 16 miesięcy w połączeniu z zakresem danych i celem zatrzymywania było uznawane za poważną ingerencję. Jednocześnie, w przypadku zatrzymywania danych abonenckich przez okres 12 miesięcy po rozwiązaniu umowy z dostawcą usług łączności, ETPC nie uznał tego okresu za nadmiarowy. Trudno zatem – poza ogólnymi odniesieniami do proporcjonalności, adekwatności – jednoznacznie wskazać, jakie powinny być okresy przechowywania danych.

Dostęp do danych retencyjnych

W odniesieniu dostępu do danych retencyjnych, to warunki/zasady dostępu powinny być zróżnicowane w zależności od kategorii danych niedotyczących treści. Inne zasady powinny odnosić się do danych abonenckich (najmniej restrykcyjne), danych o IP oraz danych o lokalizacji i o ruchu (najbardziej restrykcyjne). Przepisy regulujące dostęp do danych retencyjnych powinny:

- **wskazywać organ, który jest uprawniony do dostępu do danych**; **dostęp do danych o lokalizacji i danych o ruchu powinien następować dopiero po wyrażeniu uprzedniej zgody przez niezależny organ** (niekoniecznie musi być to sąd). Z orzecznictwa TSUE wynika, że standardu „niezależnego organu" nie spełnia prokurator/prokuratura, z uwagi na późniejsze występowanie w roli oskarżyciela publicznego. W przypadku danych o abonencie i danych o IP dopuszczalne są mniej rygorystyczne warunki dostępu do danych. Nie zwalnia to jednak z obowiązku ustawowego określenia przesłanek dostępu, ograniczeń w zakresie sięgania po te dane oraz mechanizmów kontroli;

- **regulować cele dostępu do danych**; w orzecznictwie TSUE podkreśla się, że dostęp do danych retencyjnych może następować wyłącznie dla realizacji celów, dla których zostały one zatrzymane. Oznacza to, że dane zatrzymane w związku z ochroną bezpieczeństwa narodowego nie mogą być wykorzystane – nie można do nich uzyskać dostępu – dla celu w postaci zwalczania przestępczości. Wykorzystanie danych w innym celu nie może prowadzić do obejścia gwarancji proceduralnych właściwych dla określonego celu i kategorii danych

- **zawierać klauzule subsydiarności, proporcjonalności i konieczności w społeczeństwie demokratycznym/zasadności dostępu do danych** – zwłaszcza w

odniesieniu do danych o lokalizacji i danych o ruchu, tak by sięgano po te informacje, gdy inne metody będą nieskuteczne albo okazałyby się nieskuteczne dla ustalenia okoliczności popełnienia przestępstwa;

- **ograniczać możliwość pozyskania danych osób w żaden sposób niezaangażowanych w jakąkolwiek działalność przestępczą.** Dodatkowo, zwłaszcza w odniesieniu do respektowania tajemnicy dziennikarskiej, ETPC i TSUE zwracają uwagę na zagrożenia – jakie wynikają z pozyskania informacji o ruchu albo o lokalizacji – dla tajemnic prawnie chronionych.

W odniesieniu do mechanizmu „stałego łącza", tj. możliwości dostępu do danych niedotyczących treści bez zaangażowania pracowników dostawców usług łączności, to takie rozwiązanie nie jest niedopuszczalne. Konieczne jest jednak wprowadzenie przepisów, które będą ograniczały możliwość nadużyć i nieuprawnionego dostępu. Kluczowe jest m.in. wprowadzenie pełnej rozliczalności dostępu, tj. obowiązku rejestrowania logowań i operacji oraz identyfikacji osoby, która uzyskuje dostęp.

Uzupełnieniem powyższych elementów ponadustawowego modelu dostępu do danych retencyjnych jest wprowadzenie zewnętrznych mechanizmów kontroli uzyskiwania dostępu do danych – przede wszystkim danych o lokalizacji i danych o ruchu. Zewnętrzny nadzór powinien być efektywny, tj. nie może polegać na przedstawieniu zagregowanych danych statystycznych. Organ nadzorujący (niekoniecznie sąd) powinien mieć możliwość zbadania celu pozyskania danych, okresu ich przechowywania, kategorii danych jakie zostały pozyskane itp. Dodatkowo przepisy krajowe powinny gwarantować możliwość uzyskania przez jednostkę informacji, czy jej dane np. o lokalizacji albo dane o ruchu, zostały przekazane organom ścigania, w jakim celu itp. W zależności od charakteru sprawy (np. w sprawach dotyczących bezpieczeństwa narodowego), możliwe jest wykonywanie uprawnień informacyjnych jednostki pośrednio – przez niezależny organ, który w danym państwie zajmuje się ochroną danych osobowych. W odniesieniu do obowiązku poinformowania jednostki, ETPC dopuszcza tryb wnioskowy – tj. informacji udziela się na wniosek zainteresowanej osoby, a dodatkowo, możliwe jest odroczenie udzielenia informacji ze względu na ochronę interesu publicznego.

VI. Zakres danych podlegających retencji na podstawie przepisów Prawa komunikacji elektronicznej

Obowiązek zatrzymywania określonych danych wynika z art. 47 ust. 1 p.k.e. Zgodnie z tym przepisem, przedsiębiorca telekomunikacyjny ma obowiązek „zatrzymywać i przechowywać dane, o których mowa w art. 49 ust. 1 p.k.e., generowane w publicznej sieci telekomunikacyjnej lub przez niego przetwarzane, na terytorium Rzeczypospolitej Polskiej, przez okres 12 miesięcy, licząc od dnia połączenia lub nieudanej próby połączenia, a z dniem upływu tego okresu dane te niszczyć, z wyjątkiem tych, które zostały zabezpieczone, zgodnie z przepisami odrębnymi". Obowiązkowi zatrzymywania i przechowywania podlegają także „dane o próbach uzyskania połączenia między zakończeniami sieci, w tym dane o nieudanych próbach połączeń, oznaczających połączenia między telekomunikacyjnymi urządzeniami końcowymi lub zakończeniami sieci, które zostały zestawione i nie zostały odebrane przez użytkownika końcowego lub nastąpiło przerwanie zestawianych połączeń" (art. 386 ust. 1 pkt 5 p.k.e. w zw. z art. 47 ust. 2 p.k.e.). Realizowanie obowiązku retencji danych ma następować w sposób, który nie będzie prowadził do ujawnienia komunikatu przesyłanego drogą elektroniczną (art. 47 ust. 3 p.k.e.). Przepis art. 47 p.k.e. nie precyzuje celu (celów), dla realizacji których ustawodawca nałożył na dostawców usług łączności obowiązek zatrzymywania określonych danych. Jedynie z umiejscowienia przepisu, tj. umieszczenia go w rozdziale 5 p.k.e. można wyinterpretować, że obowiązek zatrzymywania danych niedotyczących treści jest jednym z zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

To, jakie dane podlegają obowiązkowi retencji wynika z art. 49 p.k.e. Przepis art. 49 ust. 1 p.k.e. w sposób ogólny wskazuje, jakie kategorie danych niedotyczących treści są zatrzymywane: dane abonenckie, dane o ruchu/dane transmisyjne oraz dane lokalizacyjne odbiorcy i nadawcy połączenia[225]. Szczegółowy wykaz danych, jakie podlegają obowiązkowi retencji powinien wynikać z rozporządzenia. Przepis art. 49 ust.

[225] Przepis precyzuje, że obowiązkiem retencji objęte są dane dotyczące publicznie dostępnych usług telekomunikacyjnych niezbędne do: 1) jednoznacznego zidentyfikowania zakończenia sieci, telekomunikacyjnego urządzenia końcowego oraz użytkownika końcowego: a) inicjującego połączenie, b) do którego kierowane jest połączenie; 2) określenia: a) daty i godziny połączenia oraz czasu jego trwania, b) rodzaju połączenia, c) lokalizacji telekomunikacyjnego urządzenia końcowego.

2 p.k.e.[226] odsyła do rozporządzenia ministra właściwego do spraw informatyzacji[227] wydawanego w porozumieniu z ministrem właściwym do spraw wewnętrznych oraz po zasięgnięciu opinii Ministra - Koordynatora Służb Specjalnych, lecz rozporządzenie takie nie zostało nadal wydane[228]. Obowiązuje zatem rozporządzenie Ministra Infrastruktury z dnia 28 grudnia 2009 r. w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania[229] wydane na podstawie art. 180c ust. 2 ustawy - Prawo telekomunikacyjne[230].

Z aktualnie (nadal) obowiązującego rozporządzenia Ministra Infrastruktury z dnia 28 grudnia 2009 r.[231] wynika, że obowiązkiem retencji objęte są:

1. dane identyfikujące osoby biorące udział w połączeniu, tj. kto inicjował połączenie, łączył się z Internetem i do kogo połączenie było kierowane (czyli numer telefonu, imię i nazwisko albo nazwa oraz adres abonenta (jeżeli zostały podane), identyfikatory przypisane do użytkownika lub urządzenia (np. karta SIM, urządzenie, w tym numer IMEI);

2. dane o samym połączeniu, w szczególności data i godzina rozpoczęcia połączenia, data i godzina zakończenia połączenia, czas trwania połączenia, informacja o nieudanej próbie połączenia (np. nieodebrane połączenie);

---

[226] Warto także wskazać, że odrębna delegacja ustawowa znajduje się w art. 49 ust. 3 p.k.e. Prezes Rady Ministrów powinien wydać rozporządzenie dotyczące szczegółowego sposobu udostępnienia danych niedotyczących treści oraz wymagań co do rodzaju/struktury/formatu udostępnianych danych.

[227] Zgodnie z art. 12a ustawy z dnia 4 września 1997 r. o działach administracji rządowej (t.j. Dz. U. z 2024 r. poz. 1370 z późn. zm.) oraz § 1 pkt 2 rozporządzenia Prezesa Rady Ministrów z dnia 18 grudnia 2023 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz. U. poz. 2720) jest nim Minister Cyfryzacji.

[228] Na stronach Rządowego Centrum Legislacji znajduje się projekt rozporządzenia dostępny na stronie: https://legislacja.gov.pl/projekt/12399801/katalog/13142072#13142072. Projekt rozporządzenia z 9 czerwca 2025 r. nie rozszerza obowiązków w zakresie retencji, ale dostosowuje terminologię do aktualnie obowiązujących przepisów, porządkuje rozporządzenie i przenosi wykaz danych objętych obowiązkowi retencji do załącznika do rozporządzenia. Merytorycznie zmiany są kosmetyczne i terminologiczne. Np. numer portu usługi wyraźnie wskazano jako identyfikator usługi, wyraźnie wyodrębniono telefonię internetową VoIP.

[229] Dz. U. Nr 226, poz. 1828.

[230] Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz. U. z 2024 r. poz. 34 z późn. zm.); ustawa utraciła moc w dniu 10 listopada 2024 r.

[231] Projekt rozporządzenia z 9 czerwca 2025 r. nie rozszerza obowiązków w zakresie retencji, ale dostosowuje terminologię do aktualnie obowiązujących przepisów, porządkuje rozporządzenie i przenosi wykaz danych objętych obowiązkowi retencji do załącznika do rozporządzenia. Merytorycznie zmiany są kosmetyczne i terminologiczne. Np. numer portu usługi wyraźnie wskazano jako identyfikator usługi, wyraźnie wyodrębniono telefonię internetową VoIP.

3. dane o rodzaju usługi, tj. czy skorzystano z połączenia głosowego, SMS, dostępu do Internetu, poczty elektronicznej, telefonii internetowej;

4. dane lokalizacyjne urządzenia, czyli identyfikator stacji bazowej (anteny), z którą łączyło się urządzenie, dane pozwalające określić obszar, w którym znajdowało się urządzenie w chwili połączenia, a w przypadku połączeń realizowanych za granicą – informacje o kraju i sieci, w której połączenie zostało wykonane;

5. dane dotyczące korzystania z Internetu, tj. adres IP przypisany użytkownikowi, identyfikator użytkownika w systemie operatora, data i godzina połączenia z Internetem oraz rozłączenia, dane techniczne pozwalające ustalić, z jakiego punktu sieci nastąpiło połączenie (np. linia abonencka, port, karta sieciowa). Dane te nie obejmują historii przeglądania, treści zapytań w wyszukiwarkach ani adresów URL[232];

6. dane dotyczące poczty elektronicznej i telefonii internetowej, tj. dane identyfikujące użytkownika korzystającego z usługi, dane identyfikujące odbiorcę połączenia lub komunikacji (w zakresie danych technicznych), daty i godziny logowania i wylogowania z usługi, dane techniczne pozwalające ustalić rodzaj wykorzystanej usługi;

7. dane przy przekierowywaniu lub przełączaniu połączeń tj., jeżeli połączenie było przekierowane lub przełączone zatrzymywane są dane identyfikujące użytkownika, do którego połączenie ostatecznie trafiło, bez utrwalania treści rozmowy lub komunikacji.

Przepisy nie wprowadzają żadnego rozróżnienia – w kontekście obowiązku retencji danych i rodzajów danych niedotyczących treści, jakie są zatrzymywane – na dane abonenckie, dane transmisyjne/dane o ruchu i dane o lokalizacji. **Zatrzymywane są wszystkie dane w sposób uogólniony i niezróżnicowany każdego użytkownika usług łączności.**

Obowiązkiem dostawców usług łączności jest „przygotowania technicznych i organizacyjnych warunków udostępniania przetwarzanych przez siebie danych, o których mowa w art. 43 ust. 1 pkt 1 lit. a tiret drugie, art. 386 ust. 1 pkt 1 i 3-5 oraz art. 389 i art. 390 ust. 2" oraz udostępnianie „uprawnionym podmiotom, a także sądowi i prokuratorowi, przetwarzanych przez siebie danych, o których mowa w art. 43 ust. 1

[232] Uniform Resource Locator. Jest to rodzaj identyfikatora, który wskazuje lokalizację zasobu w sieci oraz mechanizm dostępu do niego.

pkt 1 lit. a tiret drugie, art. 386 ust. 1 pkt 1 i 3-5 oraz art. 389 i art. 390 ust. 2" związanych ze świadczoną publicznie dostępną usługą telekomunikacyjną wraz z towarzyszącymi jej powiązanymi usługami, na zasadach i przy zachowaniu procedur określonych w przepisach odrębnych.

Przepis art. 45 ust. 1 p.k.e. obejmuje swoim zakresem następujące dane[233]:

- dane abonentów związanych z komunikatami elektronicznymi przesyłanymi w ramach świadczonej publicznie dostępnej usługi telekomunikacyjnej, obejmujących, w przypadku osób fizycznych imię (imiona) i nazwisko, numer PESEL (jeżeli osoba go posiada), albo nazwę, serię i numer dokumentu potwierdzającego tożsamość, a w przypadku cudzoziemca, który nie jest obywatelem państwa członkowskiego albo Konfederacji Szwajcarskiej - numer paszportu lub karty pobytu; a w przypadku abonenta niebędącego osobą fizyczną nazwę, numer identyfikacyjny REGON lub NIP lub numer w Krajowym Rejestrze Sądowym albo informację o wpisie do Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub innym właściwym rejestrze, a także na żądanie dostawcy usług - dane osób reprezentujących abonenta, umożliwiające dostawcy usług ich weryfikację (w szczególności imię, nazwisko, numer PESEL);

- przydzielony numer abonenta (jeśli został nadany), a w przypadku przyłączenia do stacjonarnej sieci telekomunikacyjnej także adres zakończenia sieci;

- adres korespondencyjny oraz adres wskazany na potrzeby komunikacji elektronicznej, o ile zostały przez abonenta podane; czyli także adres mailowy (art. 43 ust. 1 pkt 1 lit. a tiret drugi p.k.e.);

- dane dotyczące użytkownika (art. 386 ust. 1 pkt 1 p.k.e.);

- dane transmisyjne (dane o ruchu/*traffic data*), które oznaczają dane przetwarzane do celów przekazywania komunikatów elektronicznych w sieciach telekomunikacyjnych lub naliczania opłat za usługi komunikacji elektronicznej i mogą obejmować dane lokalizacyjne, które oznaczają wszelkie dane przetwarzane w sieci telekomunikacyjnej lub w ramach usług komunikacji elektronicznej wskazujące położenie geograficzne telekomunikacyjnego urządzenia końcowego użytkownika usług komunikacji elektronicznej (art. 386 ust. 1 pkt 3 p.k.e.);

[233] Przepis odsyła także do art. 389 i 390 p.k.e., które odnoszą się do podstaw prawnych przetwarzania danych i tajemnicy komunikacji elektronicznej.

- dane o lokalizacji, które oznaczają dane lokalizacyjne wykraczające poza dane niezbędne do transmisji komunikatu elektronicznego lub wystawienia rachunku (art. 386 ust. 1 pkt 4 p.k.e.); dane o lokalizacji obejmują informacje, które wynikają z działania sieci telekomunikacyjnych;

- dane o próbach uzyskania połączenia między zakończeniami sieci, w tym dane o nieudanych próbach połączeń, oznaczających połączenia między telekomunikacyjnymi urządzeniami końcowymi lub zakończeniami sieci, które zostały zestawione i nie zostały odebrane przez użytkownika końcowego lub nastąpiło przerwanie zestawianych połączeń (art. 386 ust. 1 pkt 5 p.k.e.);

- dane pozyskane na podstawie art. 389 ust. 2 w zw. z art. 386 ust. 1 pkt 2-5 p.k.e., które zostały zanonimizowane (art. 389 p.k.e.);

- dane przetwarzane przez dostawcę usług dotyczące użytkownika innego operatora/dostawcy usług łączności oraz dane o wykonanych na jego rzecz usługach komunikacji elektronicznej (art. 390 ust. 2 p.k.e.).

Dodatkowo, jeśli chodzi o dane o lokalizacji (art. 386 ust. 1 pkt 4 p.k.e.), na żądanie uprawnionego podmiotu dostawca usług łączności musi zapewnić, by lokalizacja ta była monitorowana w czasie rzeczywistym. Gromadzenie danych o lokalizacji w czasie rzeczywistym obywa się w okresie wskazanym w żądaniu odpowiedniego organu. Porównując, jaki zakres danych podlega obowiązkowi retencji z art. 47 ust. 1 w zw. z art. 49 p.k.e., a treścią przepisu art. 45 p.k.e., tj. jakie dane mogą być zatrzymywane wyłącznie na żądanie uprawnionego organu, to zasadniczo odnosi się to do danych o lokalizacji gromadzonych w czasie rzeczywistym.

Podsumowując, dane podlegające retencji można podzielić na trzy kategorie: dane dotyczące abonenta (dane abonenckie), tj. dane identyfikujące użytkownika sieci/usługi telekomunikacyjnej lub internetowej, dane transmisyjne/dane o ruchu (*traffic data*), odnoszące się do połączeń, jakie zostały wykonywane (godziny, rodzaju połączenia, odbiorcy połączenia), a także dane o lokalizacji (umiejscawiające połączenie, jaki i użytkownika w określonym obszarze). Na podstawie przepisów krajowych podział na te trzy kategorie danych ma charakter porządkujący, ponieważ prawodawca nie wprowadza żadnego rozróżnienia w zakresie ich zatrzymywania – dane mniej ingerujące w prywatność jednostki, jak dane abonenckie, podlegają takim samym zasadom zatrzymywania jak dane o lokalizacji, czy dane o ruchu. **W krajowym porządku prawnym retencja danych ma charakter uogólniony i niezróżnicowany. Nie jest ograniczona geograficznie (ukierunkowana retencja danych) ani w żaden**

inny sposób limitowana. Dodatkowo, warto zwrócić uwagę, że w ustawie brak jest sprecyzowanego celu retencji danych. Ustawodawca wprowadza jednak bezwzględne ograniczenie czasowe, tj. dane retencyjne muszą zostać usunięte po upływie 12 miesięcy, chyba że w tym okresie uprawnione organy uzyskają dostęp i zabezpieczą dane określonej osoby np. w związku z prowadzonym postępowaniem karnym.

VII. Dostęp do danych niedotyczących treści przez organy ścigania, prokuraturę i sądy

VII.1. Organy uprawnione do pozyskania danych niedotyczących treści i tryb pozyskania tych danych

Dostęp organów państwa do danych niedotyczących treści komunikacji elektronicznej stanowi samodzielną formę ingerencji w prawo do poszanowania życia prywatnego, niezależną od dostępu do treści komunikacji. Ingerencja ta polega na rekonstrukcji aktywności (komunikacji, lokalizacji, schematów dnia codziennego), a nie na możliwości monitorowania w czasie rzeczywistym życia jednostki.

Obecnie, dostęp do danych podlegających retencji, jest możliwy w dwóch trybach:

- w trybie pozaprocesowym, na podstawie ustaw policyjnych i o służbach specjalnych;

- trybie procesowym, tj. na podstawie art. 218 k.p.k., który zobowiązuje m.in. dostawców usług łączności, do udostępnienia danych, o których mowa w art. 45 ust. 1 i art. 49 p.k.e., jeżeli mają znaczenie dla toczącego się postępowania, na żądanie sądu lub prokuratora w postępowaniu przygotowawczym[234].

Aktualnie prawo dostępu do danych telekomunikacyjnych/danych o łączności w trybie pozaprocesowym mają:

1. **Policja**[235], w tym także m.in. Centralne Biuro Zwalczania Cyberprzestępczości (art. 5d ustawy o Policji), Centralne Biuro Śledcze Policji (art. 5a ustawy o Policji), Biuro Spraw Wewnętrznych Policji (art. 5b ustawy o Policji)

    a. na podstawie art. 20c ustawy o Policji - możliwe jest pozyskanie danych wskazanych w art. 45 ust. 1 i art. 49 p.k.e. w celu zapobiegania lub wykrywania przestępstw, przestępstw skarbowych albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych;

[234] Zob. szerzej: M. Rogalski, *WYBRANE ASPEKTY PRAKTYCZNE STOSOWANIA ART. 218 K.P.K.* [w:] *Verba volant, scripta manent. Proces karny, prawo karne skarbowe i prawo wykroczeń po zmianach z lat 2015-2016. Księga pamiątkowa poświęcona Profesor Monice Zbrojewskiej*, red. T. Grzegorczyk, R. Olszewski, Warszawa 2017; M. Rogalski, *PRZEKAZYWANIE WYKAZU POŁĄCZEŃ* [w:] *Państwo prawa i prawo karne. Księga jubileuszowa Profesora Andrzeja Zolla, tom II*, red. P. Kardas, T. Sroka, W. Wróbel, Warszawa 2012.

[235] Ustawa z dnia 6 kwietnia 1990 r. o Policji (t.j. Dz. U. z 2025 r. poz. 636 z późn. zm.).

pozyskiwanie danych podlega kontroli właściwego miejscowo sądu okręgowego na podstawie art. 20ca ustawy o Policji;

b. na podstawie art. 20cb ustawy o Policji[236] możliwe jest pozyskanie danych wskazanych w art. 43 ust. 1 tiret drugi[237] i art. 389 p.k.e.[238] w celu zapobiegania lub wykrywania przestępstw, przestępstw skarbowych albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych. Dane o abonencie, dane o lokalizacji i dane transmisyjne pozyskane w trybie art. 20cb nie podlegają kontroli sądowej;

2. **Agencja Bezpieczeństwa Wewnętrznego**[239]:

a. na podstawie art. 28 ust. 1 ustawy o ABW możliwe jest pozyskanie danych wskazanych w art. 45 ust. 1 i art. 49 p.k.e. w zakresie, w jakim jest to niezbędne do realizacji zadań tej służby określonych w art. 5 ust. 1[240] ustawy o ABW; pozyskiwanie danych podlega kontroli Sądu Okręgowego w Warszawie na podstawie art. 28a ustawy o ABW;

b. na podstawie art. 28b[241] ustawy o ABW możliwe jest pozyskanie danych wskazanych w art. 43 ust. 1 tiret drugi i art. 389 p.k.e. w celu realizacji zadań określonych w art. 5 ust. 1 ustawy o ABW. Dane te są pozyskiwane poza kontrolą sądową;

3. **Straż Graniczna**[242], w tym także Nadwiślański Oddział Straży Granicznej:

---

[236] Przepis art. 20cb ustawy o Policji został dodany ustawą z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz. U. poz. 147).

[237] Nie powielając analizy wskazanej w pkt II, chodzi o dane o abonencie, pozwalające na ustalenie tożsamości, adresu do korespondencji, maila, numeru PESEL i innych danych identyfikujących użytkownika

[238] Chodzi o dane transmisyjne i dane o lokalizacji. Przepis art. 389 ust. 1 p.k.e. odsyła w tym zakresie do art. 386 ust. 1 pkt 2-5 p.k.e.

[239] Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j. Dz. U. z 2025 r. poz. 902 z późn. zm.); dalej: ustawa o ABW.

[240] Przepis art. 5 ust. 1 ustawy o ABW określa zadania ABW jako obejmujące rozpoznawanie, zapobieganie, wykrywanie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa, w szczególności związanych z ochroną integralności terytorialnej, obronności państwa, bezpieczeństwa ekonomicznego oraz bezpieczeństwa systemów teleinformatycznych i infrastruktury krytycznej, a także ściganie przestępstw zagrażających tym dobrom.

[241] Przepis art. 28b ustawy o ABW został dodany ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz. U. poz. 147).

[242] Ustawa z dnia 12 października 1990 r. o Straży Granicznej (t.j. Dz. U. z 2025 r. poz. 914 z późn. zm.); dalej: ustawa o SG.

a. na podstawie art. 10b ustawy o SG możliwe jest pozyskanie danych wskazanych w art. 45 ust. 1 i art. 49 p.k.e w celu zapobiegania lub wykrywania przestępstw oraz przestępstw skarbowych; pozyskiwanie danych podlega kontroli sądu okręgowego właściwego dla siedziby organu SG składającego wniosek na podstawie art. 10ba ustawy o SG;

b. na podstawie art. 10bb[243] ustawy o SG możliwe jest pozyskanie danych wskazanych w art. 43 ust. 1 tiret drugi i art. 389 p.k.e. w celu zapobiegania lub wykrywania przestępstw oraz przestępstw skarbowych. Pozyskanie tych danych nie podlega kontroli sądu.

4. Krajowa Administracja Skarbowa[244]

a. na podstawie art. 114 ustawy o KAS możliwe jest pozyskanie danych wskazanych w art. 45 ust. 1 i art. 49 p.k.e w celu zapobiegania przestępstwom skarbowym lub przestępstwom, o których mowa w art. 2 ust. 1 pkt 14-16 ustawy o KAS[245], lub wykrywania tych przestępstw oraz wykonania zadań, o

[243] Przepis art. 10bb ustawy o SG został dodany ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz. U. poz. 147).

[244] Ustawa z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (t.j. Dz. U. z 2025 r. poz. 1131 z późn. zm.); dalej: ustawa o KAS.

[245] Chodzi o realizowanie przez KAS zadań ustawowych polegających na rozpoznawaniu, wykrywaniu i zwalczaniu przestępstw i wykroczeń związanych z naruszeniem przepisów dotyczących towarów, którymi obrót podlega zakazom lub ograniczeniom na mocy przepisów prawa polskiego, przepisów prawa Unii Europejskiej lub umów międzynarodowych, zapobieganie tym przestępstwom i wykroczeniom oraz ściganie ich sprawców, jeżeli zostały ujawnione przez Służbę Celno-Skarbową (pkt 14); rozpoznawaniu, wykrywaniu i zwalczaniu przestępstw określonych w art. 258, art. 270, art. 270a, art. 271, art. 271a, art. 273, art. 277a, art. 286 § 1 oraz art. 299 k.k. w związku z którymi nastąpiło uszczuplenie lub narażenie na uszczuplenie należności publicznoprawnej, zapobieganie tym przestępstwom oraz ściganie ich sprawców, jeżeli zostały ujawnione przez KAS (pkt 15); rozpoznawaniu, wykrywaniu i zwalczaniu przestępstw określonych w a) art. 228-231 k.k., popełnionych przez osoby zatrudnione w jednostkach organizacyjnych KAS albo funkcjonariuszy, w związku z wykonywaniem czynności służbowych, b) art. 229-230a k.k., popełnionych przez osoby niezatrudnione w jednostkach organizacyjnych KAS albo niebędące funkcjonariuszami, w związku z wykonywaniem czynności służbowych przez osoby zatrudnione w jednostkach organizacyjnych KAS albo funkcjonariuszy, c) art. 190, art. 222, art. 223, art. 226, art. 235, art. 236 i art. 238 k.k., skierowanych przeciwko osobom zatrudnionym w jednostkach organizacyjnych KAS albo funkcjonariuszom podczas pełnienia obowiązków służbowych lub w związku z ich pełnieniem, d) art. 239 k.k. - w przypadku osób pomagających sprawcom przestępstw określonych w lit. a-c oraz zapobieganiu tym przestępstwom i ściganiem ich sprawców.

których mowa w art. 2 ust. 1 pkt 16a[246]; pozyskiwanie danych podlega kontroli sądu okręgowego właściwego dla siedziby organu KAS składającego wniosek na podstawie art. 116 ustawy o KAS;

b. na podstawie art. 115 ust. 1ustawy o KAS możliwe jest pozyskanie danych wskazanych w art. 43 ust. 1 tiret drugi i art. 389 p.k.e. w celu zapobiegania przestępstwom skarbowym lub przestępstwom, o których mowa w art. 2 ust. 1 pkt 14-16, lub wykrywania tych przestępstw oraz wykonania zadań, o których mowa w art. 2 ust. 1 pkt 16a. Pozyskanie danych w tym trybie jest wyłączę spod kontroli sądowej (art. 116 ust. 5 ustawy o KAS);

5. Służba Ochrony Państwa[247]

a. na podstawie art. 57 ust. 1 ustawy o SOP możliwe jest pozyskanie danych wskazanych w art. 45 ust. 1 i art. 49 p.k.e. w celu rozpoznania, zapobiegania i wykrywania przestępstw, o których mowa w art. 42 ust. 1 ustawy o SOP[248], pozyskiwanie danych podlega kontroli Sądu Okręgowego w Warszawie na podstawie art. 58 ustawy o SOP;

b. na podstawie art. 59 ust. 1 ustawy o SOP możliwe jest pozyskanie danych wskazanych w art. 43 ust. 1 tiret drugi i art. 389 p.k.e. w celu realizacji zadań określonych w art. 42 ust. 1 ustawy o SOP. Dane te są pozyskiwane poza kontrolą sądową, zgodnie z art. 59 ust. 3 ustawy o SOP;

6. Centralne Biuro Antykorupcyjne[249]

a. na podstawie art. 18 ust. 1 ustawy o CBA możliwe jest pozyskanie danych wskazanych w art. 45 ust. 1 i art. 49 p.k.e., jeśli jest to niezbędne do realizacji

[246] Chodzi o ujawnianie i odzyskiwanie mienia zagrożonego przepadkiem w związku z przestępstwami, które wskazano we wcześniejszym przypisie albo art. 33 § 2 k.k.s., ale także w szerszym zakresie wynikającym z art. 2 ust. 1 pkt 13 ustawy o KAS, który zakres przedmiotowy działań KAS określa szerzej, jako rozpoznawanie, wykrywanie i zwalczanie przestępstw skarbowych i wykroczeń skarbowych, zapobieganie tym przestępstwom i wykroczeniom oraz ściganie ich sprawców.

[247] Ustawa z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (t.j. Dz. U. z 2025 r. poz. 34 z późn. zm.); dalej: ustawa o SOP

[248] Ustawa o SOP zawęża możliwość pozyskiwania danych retencyjnych wyłącznie do spraw, w których SOP może prowadzić czynności operacyjne.

[249] Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (t.j. Dz. U. z 2025 r. poz. 712); dalej: ustawa o CBA.

zadań, o których mowa w art. 2 ustawy o CBA[250], pozyskiwanie danych podlega kontroli Sądu Okręgowego w Warszawie na podstawie art. 18a ustawy o CBA;

b. na podstawie art. 18b ust. 1[251] ustawy o CBA możliwe jest pozyskanie danych wskazanych w art. 43 ust. 1 tiret drugi i art. 389 p.k.e. w celu realizacji zadań określonych w art. 2 ustawy o CBA. Dane te są pozyskiwane poza kontrolą sądową (art. 18a ust. 5 ustawy o CBA);

7. Żandarmeria Wojskowa[252]

a. na podstawie art. 30 ust. 1 ustawy o ŻW możliwe jest pozyskanie danych wskazanych w art. 45 ust. 1 i art. 49 p.k.e. w celu zapobiegania przestępstwom lub wykrywania przestępstw, w tym przestępstw skarbowych, popełnionych przez osoby, o których mowa w art. 3 ust. 2 ustawy o ŻW[253], albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych; pozyskiwanie danych podlega kontroli wojskowego sąd okręgowy właściwego dla siedziby organu Żandarmerii Wojskowej, któremu udostępniono te dane, na podstawie art. 30b ustawy o ŻW;

b. na podstawie art. 30c[254] ustawy o ŻW możliwe jest pozyskanie danych wskazanych w art. 43 ust. 1 tiret drugi i art. 389 p.k.e. w celu zapobiegania przestępstwom lub wykrywania przestępstw, w tym przestępstw skarbowych, popełnionych przez osoby, o których mowa w art. 3 ust. 2 ustawy o ŻW, albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań

[250] Przepis ten określa zadania CBA. Z perspektywy pozyskiwania danych retencyjnych problematyczne jest to, że CBA może pozyskiwać dane o abonentach, dane lokalizacyjne i transmisyjne **bez żadnego związku z podejrzeniem popełnienia przestępstwa.** Skoro działaniem są objęte np. kontrole oświadczeń majątkowych, czy partnerstwo publiczno-prawne, niezależnie od jakiegokolwiek podejrzenia, czy przypuszczenia, że mogło dojść do popełnienia przestępstwa, to taka ingerencja jest trudno akceptowalna. O ile w przypadku służb specjalnych – ABW, czy SKW – takie uniezależnienie od podejrzenia popełnienia przestępstwa może być uzasadnione bezpieczeństwem narodowym, o tyle w przypadku CBA – służby stricte policyjnej – trudno jest wytłumaczyć tak szeroko zakreślony zakres dopuszczalnej ingerencji w prawo do prywatności jednostki.

[251] Przepis art. 18b ustawy o CBA został dodany ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz. U. poz. 147).

[252] Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (t.j. Dz. U. z 2025 r. poz. 12 z późn. zm.); dalej: ustawa o ŻW.

[253] Przepis ten wskazuje, jaki jest zakres podmiotowo-przedmiotowy działań Żandarmerii Wojskowej.

[254] Przepis art. 30c ustawy o ŻW został dodany ustawą z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz. U. poz. 147).

poszukiwawczych lub ratowniczych. Dane te są pozyskiwane poza kontrolą sądową (art. 30b ust. 5 ustawy o ŻW);

8. **Służba Kontrwywiadu Wojskowego**[255]

   a. na podstawie art. 32 ust. 1 ustawy o SKW możliwe jest pozyskanie danych wskazanych w art. 45 ust. 1 i art. 49 p.k.e. niezbędnych do realizacji zadań, o których mowa w art. 5 ustawy o SKW[256], pozyskiwanie danych podlega kontroli Wojskowego Sądu Okręgowego w Warszawie na podstawie art. 32a ustawy o SKW;

   b. na podstawie art. 32b ust. 1[257] ustawy o SKW możliwe jest pozyskanie danych wskazanych w art. 43 ust. 1 tiret drugi i art. 389 p.k.e. w celu realizacji zadań określonych w art. 5 ust. 1 ustawy o SKW. Dane te są pozyskiwane poza kontrolą sądową, zgodnie z art. 32a ust. 5 ustawy o SKW;

9. **Generalny Inspektor Informacji Finansowej Ministerstwa Finansów**[258] na podstawie art. 76 ust. 1 pkt 5 ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu może uzyskać dostęp do adresów IP, z których następowało połączenie z systemem teleinformatycznym instytucji obowiązanej, oraz czasów połączeń z tym systemem. Wykonywanie tych zadań odbywa się pod nadzorem Sądu Okręgowego w Warszawie (art. 98 ust. 1 ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu).

Od strony technicznej, służby policyjne i służby specjalne mogą pozyskiwać dane niedotyczące treści na dwa sposoby:

1) przy zaangażowaniu operatora usług łączności/telekomunikacyjnych oraz

2) bez wiedzy i zgody tego podmiotu.

[255] Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (t.j. Dz. U. z 2024 r. poz. 1405 z późn. zm.); dalej: ustawa o SKW.
[256] Przepis mówi o zadaniach SKW, które wiążą się nie tylko ze zwalczaniem przestępczości, ale szerzej – z zapewnieniem bezpieczeństwa powszechnego i bezpieczeństwa narodowego.
[257] Przepis art. 32b ustawy o SKW został dodany ustawą z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz. U. poz. 147).
[258] Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz. U. z 2025 r. poz. 644).

Udostępnianie danych, przy zaangażowaniu dostawców usług, jest możliwe o ile funkcjonariusz Policji[259]/ Agencji Bezpieczeństwa Wewnętrznego[260]/ Centralnego Biura Antykorupcyjnego[261]/ Służby Kontrwywiadu Wojskowego[262]/ Krajowej Administracji Skarbowej[263]/ Żandarmerii Wojskowe[264]/ Straży Granicznej[265]/ Służby Ochrony Państwa [266] posiada upoważnienie szefa danej służby lub komendanta. Dane są udostępniane nieodpłatnie drogą elektroniczną albo za pośrednictwem sieci telekomunikacyjnej. Jednocześnie ustawodawca wprowadził dodatkowy, uproszczony tryb udostępnienia danych niedotyczących treści na podstawie porozumień zawartych z dostawcami usług łączności/usług telekomunikacji. Zgodnie z art. 20c ust. 3 ustawy o Policji[267] udostępnianie danych niedotyczących treści może także odbywać się bez udziału pracowników przedsiębiorcy telekomunikacyjnego, operatora pocztowego lub usługodawcy świadczącego usługi drogą elektroniczną lub przy niezbędnym ich udziale, jeżeli możliwość taka jest przewidziana w porozumieniu zawartym pomiędzy Komendantem Głównym Policji a tym podmiotem. **Swoiste „stałe łącze" pomiędzy służbami policyjnymi i służbami specjalnymi a dostawcami usług sprawia, że nie ma żadnej kontroli zewnętrznej – kontroli uprzedniej organu sądowego albo chociaż organu innego niż przełożony służby, która sięga po dane niedotyczące treści – nad tym, czyje dane są pozyskiwane, czy są niezbędne, a także – czy organy policyjne/służby specjalne nie ingerują np. w tajemnicę dziennikarską i na podstawie danych z bilingów oraz danych o lokalizacji nie próbują ustalić np. dziennikarskich źródeł informacji.**

Dostęp do danych o abonencie, danych o lokalizacji, danych transmisyjnych w trybie procesowym jest możliwy na podstawie art. 218 k.p.k. Chociaż regulacja jest dość lakoniczna – przepis brzmi bowiem: „urzędy, instytucje i podmioty prowadzące działalność w dziedzinie poczty lub działalność telekomunikacyjną, urzędy celno-skarbowe oraz instytucje i przedsiębiorstwa transportowe obowiązane są wydać sądowi lub prokuratorowi, na żądanie zawarte w postanowieniu, korespondencję i przesyłki oraz dane, o których mowa w art. 45 ust. 1 i art. 49 ustawy z dnia 12 lipca 2024

[259] Art. 20c ust. 2 pkt 1 i 2 ustawy o Policji.
[260] Art. 28 ust. 2 pkt 1 i 2 ustawy o ABW.
[261] Art. 18 ust. 2 pkt 1 i 2 ustawy o CBA.
[262] Art. 32 ust. 2 pkt 1 i 2 ustawy o SKW.
[263] Art. 114 ust. 2 pkt 1 i 2 ustawy o KAS.
[264] Art. 30 ust. 2 pkt 1 i 2 ustawy o ŻW.
[265] Art. 10b ust. 2 pkt i 2 ustawy o SG.
[266] Art. 57 ust. 2 pkt 1 i 2 ustawy o SOP.
[267] Oraz: art. 28 ust. 3 ustawy o ABW; art. 18 ust. 3 ustawy o CBA; art. 32 ust. 3 ustawy o SKW; art. 114 ust. 3 ustawy o KAS; art. 30 ust. 3 ustawy o ŻW; art. 10b ust. 3 ustawy o SG; art. 57 ust. 3 ustawy o SOP.

r. - Prawo komunikacji elektronicznej (Dz. U. poz. 1221), jeżeli mają znaczenie dla toczącego się postępowania. Tylko sąd lub prokurator mają prawo je otwierać lub zarządzić ich otwarcie." – to należy ją czytać w kontekście systemowym przepisów k.p.k. Oznacza to, że organem właściwym do wystąpienia z wnioskiem do operatorów/dostawców usług telekomunikacyjnych jest prokurator w postępowaniu przygotowawczym – co do zasady – oraz sąd w postępowaniu jurysdykcyjnym. Od strony technicznej, dostęp prokuratora lub sądu do danych niedotyczących treści jest regulowany w rozporządzeniu wydanym na podstawie art. 218b k.p.k.[268]. Nie wdając się szczegółowo w tę problematykę, podkreślenia wymaga fakt, że ani sąd, ani prokurator nie mogą uzyskać dostęp do danych niedotyczących treści bez zaangażowania operatora/dostawcy usług łączności lub usług telekomunikacyjnych. Każdorazowo, muszą się zwrócić do odpowiedniego dostawcy – wydając postanowienie w trybie art. 218 k.p.k., a niekiedy – uzyskując uprzednie zwolnienie z tajemnicy, zwłaszcza w odniesieniu np. do tajemnicy dziennikarskiej z art. 180 § 2 k.p.k. – o przekazanie danych o abonencie, danych o lokalizacji lub danych transmisyjnych/danych o ruchu. Należy także podkreślić, że z możliwości pozyskania danych z art. 218 k.p.k. organy procesowe mogą skorzystać **tylko w toku prowadzonego postępowania karnego**. Oznacza to, że niedopuszczalne jest wystąpienie przez prokuratora z wnioskiem np. o dostęp do danych o abonencie w toku tzw. czynności sprawdzających prowadzonych na podstawie art. 307 k.p.k. Konieczne jest wydanie decyzji o wszczęciu śledztwa lub dochodzenia (art. 303 k.p.k.; art. 325e k.p.k.). Prokurator nie może „delegować" kompetencji do wystąpienia z żądaniem z art. 218 k.p.k. W sprawach, w których śledztwo zostało powierzone w całości do prowadzenia organom z art. 312 k.p.k., i tak tylko prokurator może skorzystać z kompetencji z art. 218 k.p.k. Jednocześnie organy te – Policja, CBA, ABW, Żandarmeria Wojskowa[269], itp. – posiadają „własne" uprawnienia do pozyskania danych niedotyczących treści. Łatwiejsze wydaje się zatem skorzystanie z „własnych" uprawnień przez odpowiednie służby w trybie pozaprocesowym na podstawie ich własnego uprawnienia wynikającego np. z art. 20c czy 20cb ustawy o Policji (oraz analogicznych przepisów w przypadku pozostałych służb), niż zwracanie się do prokuratora, by ten wystąpił z żądaniem z art. 218 k.p.k. Dodatkowo, nic nie stoi na przeszkodzie, by prokurator prowadzący postępowanie zwrócił się do funkcjonariusza

[268] 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).

[269] Zob. art. 312 k.p.k. o organach uprawnionych do prowadzenia śledztwa.

odpowiedniej służby – wydając np. polecenie w trybie art. 15 k.p.k.[270] – uzyskał dostęp do danych niedotyczących treści. Przepisy pozwalają zatem na „wyprowadzanie" klasycznych czynności dowodowych, tj. przeprowadzany na podstawie przepisów k.p.k., do czynności operacyjnych[271]. Dostęp do danych jest możliwy tylko w sprawach o przestępstwa lub o przestępstwa skarbowe[272].

Warto przypomnieć, że TSUE w wyroku w sprawie C-746/18, H.K. przeciwko Prokuratuur [273] wskazał, że prokurator (prokuratura), która prowadzi postępowanie przygotowawcze, nie może być uznany za niezależny organ, który byłby uprawniony do przeprowadzenia uprzedniej kontroli zasadności dostępu do danych niedotyczących treści. Krajowe – polskie – przepisy na płaszczyźnie dostępu w trybie pozaprocesowym nie przewidują żadnej uprzedniej kontroli, zaś organy, które mogą mieć dostęp do danych retencyjnych trudno uznać za „niezależny organ administracyjny" albo organ sądowy. W trybie procesowym, gdy to prokurator, żąda dostępu do danych niedotyczących treści, rozwiązania także nie są zgodne z wymaganiami, jakie wynikają z orzecznictwa Trybunału w Luksemburgu.

Porządkując powyższe rozważania odnoszące do się do organów, które mogą pozyskać dane niedotyczące treści warto zwrócić uwagę na pięć kwestii.

Po pierwsze, dane retencyjne (abonenckie, IP, o ruchu oraz dane o lokalizacji) mogą być pozyskiwane w dwóch trybach: pozaprocesowym (operacyjnym) na podstawie ustaw policyjnych i o służbach specjalnych oraz procesowym na podstawie art. 218 k.p.k. (na żądanie sądu lub prokuratora w ramach toczącego się postępowania).

Po drugie, w trybie pozaprocesowym szeroki katalog służb (Policja, ABW, Straż Graniczna, Krajowa Administracja Skarbowa, Służba Ochrony Państwa, CBA, Żandarmeria Wojskowa, Służba Kontrwywiadu Wojskowego; w wąskim zakresie także

---

[270] Przepis ten brzmi: „Policja i inne organy w zakresie postępowania karnego wykonują polecenia sądu, referendarza sądowego i prokuratora oraz prowadzą pod nadzorem prokuratora śledztwo lub dochodzenie w granicach określonych w ustawie.". Zob. także art. 326 k.p.k.

[271] O problemie zacierania się różnic między czynnościami dowodowymi a czynnościami operacyjnymi, dowodami ścisłymi i swobodnymi, była także mowa w raporcie dotyczącym kontroli operacyjnej. Problem ten jest istotny, bo uprawnienia prokuratora są węższe niż służb, które prowadzą czynności operacyjne, zaś nadzór jest ograniczony. raport RPO dotyczący wykonania wyroku Pietrzak, Bychawska – Siniarska i inni przeciwko Polsce dostępny na stronie: https://bip.brpo.gov.pl/sites/default/files/2025-08/Za%C5%82%C4%85cznik%20Wykonanie%20wyroku%20Europejskiego%20Trybuna%C5%82u%20Praw%20Cz%C5%82owieka%20w%20sprawie%20Pietrzak%20i%20Bychawska-Siniarska%20i%20inni%20przeciwko%20Polsce.pdf.

[272] Zob. jednak art. 122 § 1 pkt 1 k.k.s.

[273] Zob. szerzej uwagi w pkt III.2.4.

GIIF) ma dostęp do danych retencyjnych. Dane te mogą być pozyskiwane w dwóch trybach – podlegającym sprawozdawczej kontroli sądowej, oraz poza kontrolą sądową.

Po trzecie, w trybie pozaprocesowym, dostęp do danych retencyjnych może odbywać się z udziałem pracowników operatora usług łączności albo w modelu tzw. „stałego łącza", tj. bez udziału pracowników operatora usług łączności na podstawie porozumień zawieranych pomiędzy operatorami a konkretnymi służbami policyjnymi albo specjalnymi, co ogranicza realną zewnętrzną weryfikację celów sięgania po dane.

Po czwarte, w trybie **procesowym**, na podstawie art. 218 k.p.k., przepisy wymagają działania **w ramach formalnie wszczętego postępowania** (nie np. w trakcie czynności sprawdzających z art. 307 k.p.k.) i **zaangażowania operatora** dostawcy usług łączności. Przepisy procesowe nie przewidują dostępu w ramach tzw. stałego łącza, a uprawniony organ – prokurator w postępowaniu przygotowawczym lub sąd w postępowaniu sądowym – musi zwrócić się z wnioskiem do operatora o przekazanie konkretnych danych. W sprawach objętych tajemnicami (np. dziennikarską) może być konieczne uprzednie zwolnienie z tajemnicy.

Po piąte, konstrukcja przepisów sprzyja „wyprowadzaniu" czynności dowodowych, podejmowanych w toku prowadzonego postępowania karnego, do trybu pozaprocesowego (operacyjnego): służbom często łatwiej skorzystać z własnych uprawnień pozaprocesowych niż prokuratorowi sięgać po mechanizm przewidziany w art. 218 k.p.k. Zaakcentować należy, że obecnie nie ma formalnych przeszkód, by prokurator zlecił uzyskanie danych retencyjnych funkcjonariuszom Policji, ABW, CBA, itp., na podstawie odpowiednich dla każdej z tych służb przepisów z ustaw szczególnych.

VII.2. Zakres przedmiotowy

Co do zasady dostęp do danych niedotyczących treści – w trybie procesowym i pozaprocesowym – jest możliwy w sytuacjach, gdy istnieje podejrzenie popełnienia przestępstwa. Krajowa Administracja Skarbowa może dodatkowo pozyskiwać dane o abonentach, dane o lokalizacji i dane transmisyjne także w sprawach o niektóre wykroczenia skarbowe[274]. Dodatkowo, Policja[275] i Żandarmeria Wojskowa[276] mogą uzyskać dostęp do tych danych w celu ratowania życia lub zdrowia ludzkiego bądź

[274] Art. 114 ust. 1 w zw. z art. 2 ust. 1 pkt 14 ustawy o KAS.
[275] Art. 20c ust. 1 i art. 20cb ust. 1 ustawy o Policji.
[276] Art. 30 ust. 1 i art. 30c ust. 1 ustawy o ŻW.

wsparcia działań poszukiwawczych lub ratowniczych, co niekoniecznie może wiązać się z podejrzeniem popełnienia jakiegoś przestępstwa (np. poszukiwanie dziecka, które nie wróciło do domu, czy prowadzenie akcji ratowniczej na zamkniętych akwenach).

W kontekście przestępstw skarbowych warto zwrócić uwagę na stanowisko Trybunału Konstytucyjnego wyrażone w wyroku o sygn. K 23/11. Trybunał wskazał, że nie każde przestępstwo skarbowe jest na tyle poważne, by uzasadniało to ingerencję w sferę prywatności jednostki[277]. W tym orzeczeniu postulowano ograniczenie zakresu przedmiotowego przestępstw skarbowych, ale postulat ten nie został wdrożony. Zamiast tego, dodatkowo rozszerzono w ustawie o KAS katalog czynów zabronionych w sprawach, o które można uzyskać dostęp do danych o abonencie, danych o lokalizacji i danych transmisyjnych, także na niektóre wykroczenia skarbowe.

W zdaniu odrębnym do wyroku o sygn. K 23/11 sędzia Wojciech Hermeliński zwrócił uwagę, że orzeczenie Trybunału Konstytucyjnego nie oceniało otwartego katalogu przestępstw, w sprawach, o które można pozyskać dane niedotyczące treści. **W praktyce prowadzi to do sytuacji, że w sprawie o każde przestępstwo w polskim systemie prawnym uprawniony organ może uzyskać dane o abonentach, lokalizacji, transmisji i na tej podstawie próbować zrekonstruować styl życia, zwyczaje i krąg znajomych dowolnej osoby. Jest to możliwe w sprawach o przestępstwa prywatnoskargowe**[278], **a w przypadku przestępstw publicznoskargowych – niezależnie od stopnia ich społecznej szkodliwości, a także przydatności pozyskania danych niedotyczących treści dla ustalenia faktów istotnych dla przyszłego lub prowadzonego postępowania karnego**. Przykładowo, obecnie możliwe jest uzyskanie dostępu do danych niedotyczących treści w sprawach o nielegalną hodowlę chartów[279], celowego utrudniania polowania[280], niezamieszczenia stopki redakcyjnej[281], czy nierzetelne prowadzenie ksiąg rachunkowych[282]. Co więcej,

[277] Zob. pkt 10.11.4 wyroku TK z dnia 30 lipca 2014 r. w sprawie K 23/11.
[278] Czyli takie, które co do zasady godzą w dobra osobiste określonej osoby, a nie w porządek publiczny. Są to: lekkie uszkodzenie ciała (art. 157 k.k.), zniesławienie (art. 212 k.k.), znieważenie (art. 216 k.k.) i naruszenie nietykalności cielesnej (art. 217 k.k.).
[279] Art. 52 pkt 4 ustawy z dnia 13 października 1995 r. - Prawo łowieckie (t.j. Dz. U. z 2025 r. poz. 539). Przestępstwo jest zagrożone karą grzywny, ograniczenia wolności albo pozbawienia wolności do 1 roku.
[280] Art. 52 pkt 8 ustawy z dnia 13 października 1995 r. - Prawo łowieckie (t.j. Dz. U. z 2025 r. poz. 539). Przestępstwo jest zagrożone karą grzywny, ograniczenia wolności albo pozbawienia wolności do 1 roku.
[281] Art. 49 ustawy z dnia 26 stycznia 1984 r. Prawo prasowe (t.j. Dz. U. z 2018 r. poz. 1914). Przestępstwo zagrożone karą grzywny lub ograniczenia wolności.
[282] Art. 77 ustawy z dnia 29 września 1994 r. o rachunkowości (t.j. Dz. U. z 2023 r. poz. 120 z późn. zm.). Przestępstwo zagrożone jest karą pozbawienia wolności do lat 2 albo karze grzywny albo obu tym karom łącznie.

analizując zakres przedmiotowy działań SOP, ŻW, CBA, KAS, SG można zauważyć, że zakres przestępstw i przestępstw skarbowych, w sprawach, o które formacje te mogą mieć dostęp do danych niedotyczących treści, niekoniecznie odpowiada ich specyfice. Przykładowo, KAS co do zasady prowadzi postępowania dotyczące przestępczości finansowej, ale jednocześnie w zakresie działań tej służby znajduje się czyn z art. 190 k.k. (groźby karalne), o ile groźby karalne były skierowane przeciwko osobom zatrudnionym w jednostkach organizacyjnych KAS albo funkcjonariuszom podczas pełnienia obowiązków służbowych lub w związku z ich pełnieniem[283]. Tymczasem porównując specyfikę postępowania w sprawach o charakterze finansowym, a „klasyczną" przestępczość, taką jak groźby karalne, poplecznictwo (art. 239 k.k.), czy składanie fałszywych zeznań (art. 233 k.k.), to jest ona różna.

Poza szerokim zakresem przestępstw, przestępstw skarbowych i wykroczeń skarbowych w sprawach, o które możliwe jest pozyskanie danych niedotyczących treści komunikatu przesyłanego drogą elektroniczną, niektóre służby policyjne i służby specjalne, mogą pozyskiwać te dane niezależnie od podejrzenia popełnienia przestępstwa. O ile w przypadku służb specjalnych – ABW[284] i SKW[285] – takie rozwiązanie można uzasadnić ochroną bezpieczeństwa narodowego, integralności terytorialnej państwa, przeciwdziałaniu działaniom szpiegowskim itp., to w przypadku np. CBA tak szerokie zakreślenie uprawnienia pozyskania danych retencyjnych jest mocno dyskusyjne. CBA może bowiem pozyskiwać dane o abonencie, dane lokalizacyjne i transmisyjne/dane o ruchu w związku z kontrolą oświadczeń majątkowych (art. 2 ust. 1 pkt 5 ustawy o CBA), kontrolą prawidłowości realizacji umów dotyczących partnerstwa publiczno-prywatnego (art. 2 ust. 1 pkt 4a ustawy o CBA), ale także w związku z prowadzoną działalnością analityczną dotyczącą zjawisk występujących w obszarze właściwości CBA[286], a także w sprawach o przewinienia służbowe (art. 2 ust. 1 pkt 2 ustawy o CBA w zw. z art. 13 ustawy z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne[287]). Dodatkowo, trudno jest jednoznacznie ustalić, w jakich okolicznościach CBA może sięgać po dane niedotyczące treści, ponieważ art. 2 ust. 1 pkt 7 ustawy o CBA otwiera katalog ustawowych działań. Wskazany przepis stanowi, że CBA jest właściwe w sprawie

[283] Art. 2 ust. 1 pkt 16 lit. c ustawy o KAS.
[284] Zob. art. 5 ust. 1 ustawy o ABW.
[285] Zob. art. 5 ust. 1 ustawy o SKW.
[286] Przepis art. 2 ust. 1 pkt 6 ustawy o CBA brzmi: „prowadzenie działalności analitycznej dotyczącej zjawisk występujących w obszarze właściwości CBA oraz przedstawianie w tym zakresie informacji Prezesowi Rady Ministrów, Prezydentowi Rzeczypospolitej Polskiej, Sejmowi oraz Senatowi".
[287] T.j. Dz. U. z 2025 r. poz. 499.

podejmowanie innych działań określonych w odrębnych ustawach i umowach międzynarodowych.

Podobnie ukształtowane kompetencje ma Straż Graniczna. Przepis art. 1 ust. 2 pkt 14 ustawy o SG wskazuje, że do zadań Straży Granicznej należy „wykonywanie zadań określonych w innych ustawach". Jednocześnie, jeśli chodzi o pozyskiwanie danych niedotyczących treści, to art. 10b ust. 1 i art. 10bb ust. 1 ustawy o SG zawężają ten zakres do pozyskania tych danych „w celu zapobiegania lub wykrywania przestępstw oraz przestępstw skarbowych". Nie każda realizacja zadań przez określoną służbę uzasadnia ingerencję w prawo do prywatności jednostki.

Kolejną wątpliwość może budzić fakt, że wszystkie kategorie danych niedotyczących treści mogą być pozyskane w każdej sprawie, znajdującej się w zakresie przedmiotowym danej służby. Oznacza to, że dane abonenckie, transmisyjne/dane o ruchu i lokalizacyjne mogą być w takim samym zakresie (za 12 miesięcy wstecz) pozyskane w sprawie o zabójstwo (art. 148 § 1 k.k.), sprowadzenie bezpośredniego niebezpieczeństwa katastrofy w ruchu lądowym, wodnym lub powietrznym (art. 174 § 1 k.k.), jak i w sprawie o nielegalną hodowlę chartów, a także w sprawie o wykroczenie skarbowe z art. 56 § 3 k.k.s. Tymczasem, nie w każdej sprawie o przestępstwo, czy przestępstwo skarbowe konieczne jest – z perspektywy ochrony prywatności jednostki – pozyskanie danych transmisyjnych/danych o ruchu, czy lokalizacyjnych, zwłaszcza wiele miesięcy wstecz (maksymalnie 12 miesięcy wstecz). Szeroki zakres pozyskania danych abonenckich nie budzi zasadniczych zastrzeżeń[288], ale pozostałe kategorie danych – w szczególności lokalizacja i dane transmisyjne – pozwalają na zrekonstruowanie życia jednostki oraz wyciągnięcie precyzyjnych wniosków o sposobie jej funkcjonowania.

W raporcie Najwyższej Izby Kontroli z 2013 r. proponowano, by zakres przedmiotowy pozyskania danych niedotyczących treści ograniczyć do przestępstw zagrożonych karą co najmniej 3 lat pozbawienia wolności oraz tych, które zostały popełnione przy wykorzystaniu środków komunikowania się na odległość[289]. Proponowano także wprowadzenie enumeratywnego katalogu wykroczeń, w sprawach, o które będzie możliwe pozyskanie takich danych. Jednocześnie w doktrynie proponowano stworzenie katalogu przestępstw, w sprawach, o które można byłoby pozyskać dane niedotyczące

[288] Por. uwagi w pkt IV.2.1. dotyczące wyroku Breyer przeciwko Niemcom.
[289] Zob. Raport NIK, *Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180c i d ustawy Prawo telekomunikacyjne*, KPB-P/12/191, Warszawa 2013, s. 65; https://www.nik.gov.pl/plik/id,5421,vp,7038.pdf.

treści[290]. Biorąc pod uwagę wyważenie interesu publicznego i prywatnego, wydaje się, że tworzenie katalogu przestępstw jest niecelowe – ingerencja w prywatność jednostki, jaka jest możliwa na podstawie przepisów o kontroli operacyjnej oraz procesowej kontroli i utrwalaniu rozmów jest jednak bardziej dolegliwa niż pozyskanie danych niedotyczących treści *ex post.* Stworzenia katalogu przestępstw nie wymaga także ani prawo unijne ani orzecznictwo strasburskie. Dodatkowo, przy obecnych, bardzo szerokich katalogach przestępstw[291], oraz tendencji do ich rozszerzania, niekoniecznie katalog przestępstw może spełniać swój cel. Ponadto, **przestępczość cyfrowa stale się rozwija i przepisy powinny być na tyle elastyczne, by móc odpowiednio i szybko reagować – dla swojej efektywności przepisy nie mogą być wyłącznie reaktywne.**

Z tych powodów ograniczenie rodzajowe do przestępstw, których górna granica wynosi co najmniej 3 lata pozbawienia wolności oraz tych, które zostały popełnione przy wykorzystaniu środków komunikowania się na odległość zdaje się wyważać interes publiczny z prawem do prywatności jednostki[292]. Zagrożenie karą nie może być jednak wyłącznym wyznacznikiem uzyskania dostępu do danych niedotyczących treści, zwłaszcza danych o lokalizacji i danych transmisyjnych/danych o ruchu. Każdorazowo konieczne powinno być dokonanie oceny proporcjonalności ingerencji w okolicznościach konkretnej sprawy[293]. Dodatkowo, w przypadku np. znieważenia za pośrednictwem środków komunikowania się na odległość, dostęp do danych o ruchu/danych transmisyjnych może okazać się istotny dla oceny okoliczności popełnienia przestępstwa (np. w zakresie dotyczącym danych z IP, danych o logowaniu w sieci lub pozyskanie informacji o subskrypcjach). Dotyczy to w takim samym stopniu znieważenia z art. 212 § 1 k.k., jak i znieważenia ze względów narodowościowych, rasowych lub religijnych – art. 257 k.k., czy znieważenia funkcjonariusza publicznego lub konstytucyjnego organu państwa (art. 226 k.k.). Zagrożenie karą w przypadku tych

[290] M. Rogalski, *Model zbierania i udostępniania danych telekomunikacyjnych* [w:] P. Brzeziński, B. Opaliński, M. Rogalski, *Gromadzenie i udostępnianie danych telekomunikacyjnych*, Warszawa 2016.

[291] Zob. raport RPO dotyczący wykonania wyroku Pietrzak, Bychawska – Siniarska i inni przeciwko Polsce dostępny na stronie: https://bip.brpo.gov.pl/sites/default/files/2025-08/Za%C5%82%C4%85cznik%20Wykonanie%20wyroku%20Europejskiego%20Trybuna%C5%82u%20Praw%20Cz%C5%82owieka%20w%20sprawie%20Pietrzak%20i%20Bychawska-Siniarska%20i%20inni%20przeciwko%20Polsce.pdf.

[292] Zob. także art. 5 ust. 3 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. U. UE. L. z 2023 r. Nr 191, str. 118) oraz opinię Komisji Kodyfikacyjnej Prawa Karnego do projektu nowelizacji Kodeksu postępowania karnego wykonującej wyrok TSUE z dnia 30 kwietnia 2024 r. C – 178/22 dostępną na stronie: https://www.gov.pl/web/sprawiedliwosc/opinie-komisji-kodyfikacyjnej-prawa-karnego2.

[293] Por. uwagi w pkt III.2.7.

czynów zabronionych jest łagodniejsze niż 3 lata pozbawienia wolności. Podobnie w przypadku przestępstwa tzw. groomingu z art. 200a § 2 k.k., które jest zagrożone karą do 2 lat pozbawienia wolności. W tych sprawach – mimo stosunkowo łagodnej sankcji karnej – organy ścigania (oraz organy procesowe) powinny mieć możliwość sięgnięcia po dane niedotyczące treści. Alternatywnym rozwiązaniem wydaje się możliwość dostępu do danych niedotyczących treści w sprawach zagrożonych karą łagodniejszą niż 3 lata pozbawienia wolności wyłącznie w trybie procesowym, tj. po wszczęciu postępowania karnego, na podstawie art. 218 k.p.k.

Poza służbami specjalnymi – ABW i SKW – do których zadań należy ochrona bezpieczeństwa narodowego, integralności państwa, przeciwdziałanie zagrożeniom terrorystycznym, szpiegostwu itd., pozostałe organy powinny mieć możliwość pozyskania danych abonenckich, danych lokalizacyjnych i transmisyjnych wyłącznie w sprawach o przestępstwa i przestępstwa skarbowe. Pozyskanie informacji o jednostce w celach analitycznych czy prewencyjne – w formie kontroli oświadczeń majątkowych, czy analizy partnerstwa publiczno-prawnego, gdy nie ma nawet przypuszczenia popełnienia czynu zabronionego, jest w demokratycznym państwie prawa nadmiarowe[294]. Dodatkowo, zasadą powinna być niedopuszczalność dostępu do danych o ruchu/danych transmisyjnych oraz danych lokalizacyjnych, jeśli osoba nie ma żadnego związku z popełnieniem przestępstwa.

Rozważenia wymaga zakres uprawnienia Policji i Żandarmerii Wojskowej dostępu do danych niedotyczących treści dla prowadzenia działań poszukiwawczych lub ratowniczych. Dostęp do tych danych musi być limitowany celem – tzn. konieczne jest wprowadzenie rozwiązań normatywnych, które ograniczą możliwość wykorzystania danych pozyskanych w celach ratowniczych, do realizacji np. celu w postaci zwalczania przestępczości.

Rozważenia i analizy wymaga ewentualne rozróżnienie kategorii danych, które byłby możliwe do uzyskania w sprawach o różnym ciężarze gatunkowym. Dane lokalizacyjne i transmisyjne mogą dostarczać precyzyjnych informacji, zwłaszcza jeśli organy państwa miałyby możliwość prześledzenia aktywności jednostki do 12 miesięcy wstecz. Być może w sprawach o średniej społecznej szkodliwości, przykładowo zagrożonych karą do 5 lat

[294] Takie działanie może przypominać „*fishing expedition*", tj. takie działania o charakterze prewencyjnym, które polegają na rozpoczęciu działań inwigilacyjnych bez uprzedniego podejrzenia popełnienia czynu zabronionego, bardziej na zasadzie „a może coś znajdziemy". Jest to niedopuszczalne w państwie prawa. Takie działania są zabronione. Zob. uwagi ETPC w wyroku z dnia 4 października 2022 r. w sprawie De Lege przeciwko Holandii, skarga nr 58342/15.

pozbawienia wolności, zakres pozyskania danych powinien być węższy temporalnie (np. maksymalnie do 3 lub 6 miesięcy wstecz od popełnienia czynu/daty żądania). Przepisy powinny zostać uzupełnione o klauzulę proporcjonalności, subsydiarności i konieczności. Chociaż można te zasady wyinterpretować z art. 31 ust. 3 Konstytucji, to wydaje się celowe wyrażenie ich wprost w konkretnych przepisach k.p.k. jak i ustawach pozaprocesowych. Brak wyraźnie wskazanych klauzul w przepisach szczególnych przenosi ciężar ochrony na analizę *ex post* (np. analizę dopuszczalności dowodu w postępowaniu karnym), co jest nieadekwatne przy ingerencjach niejawnych. **Sięganie po dane niedotyczące treści nie powinno być traktowane jako „ułatwienie" pracy służb policyjnych i prokuratury, ale jak środek, z którego można skorzystać, gdy jest to rzeczywiście niezbędne dla wyjaśnienia okoliczności sprawy.** Dodatkowo, jeśli sięganie po te dane wiąże się z podejrzeniem popełnienia przestępstwa, organy procesowe powinny mieć weryfikowalną, wiarygodną informację o możliwości popełnienia czynu zabronionego. Konieczne jest także wprowadzenie ograniczenia związanego z celem dostępu do danych niedotyczących treści. Jeśli uogólniona i niezróżnicowana retencja danych może być dopuszczalna tylko w przypadku ochrony bezpieczeństwa narodowego, to służby nie powinny mieć dostępu do danych niedotyczących treści w związku np. ze zwalczaniem drobnej i powszechnej przestępczości.

Podsumowując tę część analizy można wskazać na cztery węzłowe kwestie.

Po pierwsze, co do zasady, dostęp do danych niedotyczących treści (w trybie procesowym i pozaprocesowym) jest dopuszczalny, gdy istnieje podejrzenie popełnienia przestępstwa. Ustawy regulujące działalność służb specjalnych i policyjnych przewidują jednak wyjątki. Krajowa Administracja Skarbowa może pozyskiwać te dane także w sprawach o niektóre wykroczenia skarbowe, a Centralne Biuro Antykorupcyjne – bez jakiegokolwiek związku z podejrzeniem popełnienia czynu zabronionego, ale np. w związku z kontrolą oświadczeń majątkowych, czy analizą partnerstwa publiczno-prywatnego. W odniesieniu do przestępstw skarbowych w orzeczeniu TK o sygn. K 23/11 wskazano, że nie każde przestępstwo skarbowe ma ciężar uzasadniający ingerencję w prywatność; postulowane w tym wyroku ograniczenie zakresu przedmiotowego nie zostało wdrożone, a katalog w ustawie o Krajowej Administracji Skarbowej został rozszerzony także na część wykroczeń skarbowych.

Po drugie, konsekwencją szeroko zakreślonego zakresu przedmiotowego, jest to, że dane abonenckie, dane o ruchu i dane lokalizacyjne mogą być pozyskiwane także w

sprawach o drobne (błahe) czyny zabronione, niezależnie od ich społecznej szkodliwości i rzeczywistej przydatności tych danych dla ustaleń w danej sprawie.

Po trzecie, brak różnicowania kategorii danych (dane abonenckie, dane o ruchu, dane o lokalizacji[295]) oraz zakresu temporalnego w zależności od ciężaru sprawy może umożliwiać odtworzenie aktywności nawet do 12 miesięcy wstecz, zarówno w sprawach poważnych, jak i błahych.

Po czwarte, wyłącznie służby odpowiedzialne za bezpieczeństwo państwa i bezpieczeństwo narodowe powinny mieć możliwość sięgania po dane niedotyczące treści nie tylko w związku z podejrzeniem popełnienia przestępstwa. W przypadku pozostałych służb zasadne jest ograniczenie możliwości sięgania po dane bez podejrzenia przestępstwa (np. w celach analitycznych lub kontrolnych) oraz wprowadzenia reguł, które uniemożliwią wtórne wykorzystywanie danych pozyskanych w celach ratowniczych do innych celów (np. stricte ścigania).

VII.3. Zakres podmiotowy

Biorąc pod uwagę otwarty zakres przedmiotowy trudno jest ustalić, w jakich okolicznościach jednostka może realnie zakładać, że jej dane abonenckie, o lokalizacji i transmisyjne zostaną pozyskane od dostawcy usług i przekazane organom państwowym. Obecne przepisy o zakresie podmiotowym sprawiają, że założenie o możliwym pozyskaniu danych dotyczących każdej osoby, nie jest kontrfaktyczne czy absurdalne. Brak jest bowiem powiązania dostępu do danych z podejrzeniem popełnienia przestępstwa lub związku osoby z popełnionym przestępstwem. Policja i inne służby, prokurator i sąd mogą zatem mieć dostęp do danych dotyczących nie tylko osoby podejrzewanej o popełnienie przestępstwa, czy pokrzywdzonego, ale każdej osoby, którą uznaje się za w jakimś stopniu związaną z działalnością przestępczą (np. można pozyskać dane dotyczące świadka).

Przepisy k.p.k., jak i przepisy pozwalające na dostęp do danych niedotyczących treści służbom policyjnym i służbom specjalnym, nie ograniczają w żaden sposób zakresu podmiotowego. Można sięgać po dane podejrzanych, oskarżonych i osób podejrzanych, w takim samym stopniu jak pokrzywdzonych, świadków lub innych osób, z którymi mógł się kontaktować domniemany sprawca czynu zabronionego lub domniemany pokrzywdzony. Szeroki zakres przedmiotowy np. w ustawie o CBA, który uniezależnia możliwość pozyskania danych abonenckich, lokalizacyjnych i transmisyjnych od

[295] Por. uwagi w rozdziale VI.

możliwości popełnienia przestępstwa, sprawia, że dane te mogą być pozyskane w formie sprawdzenia prewencyjnego „na wypadek", gdyby „coś" udało się znaleźć. Tymczasem działania inwigilacyjne – nawet w wymiarze łagodniejszym niż monitoring życia osoby w czasie rzeczywistym wraz z dostępem do komunikatów przesyłanych drogą elektroniczną – powinny być podejmowane w reakcji na jakieś niepożądane społecznie (albo niebezpieczne) zachowanie jednostki.

Brak jakiegokolwiek ograniczenia podmiotowego w dostępie do danych abonenckich, lokalizacyjnych i transmisyjnych sprawia, tajemnice zawodowe tracą na znaczeniu.

Przepisy art. 20c i 20cb ustawy o Policji[296] nie odsyłają do przepisów k.p.k. regulujących procedurę zwolnienia z tajemnicy[297]. Ponadto:

- istnienie „stałego łącza" umożliwiającego dostęp do danych niedotyczących treści bez udziału operatora/dostawcy usług łączności,

- połączone z ograniczoną[298] i stricte formalną kontrolą sądową *ex post* oraz

- brakiem procedury informowania jednostki o pozyskaniu jej danych,

sprawiają, że nawet gdyby odpowiednie przepisy odsyłające do art.180 § 1 i 2 k.p.k. oraz art. 178 i 178a k.p.k., zostały wprowadzone, trudno byłoby zweryfikować, czy są stosowane w praktyce.

[296] Oraz art. 28 ust. 1 i 28b ustawy o ABW; art. 10b i 10bb ustawy o SG; art. 114 i 115 ust. 1 ustawy o KAS; art. 57 ust. 1 i art. 59 ust. 1 ustawy o SOP; art. 18 ust. 1 i art. 18b ust. 1 ustawy o CBA; art. 30 ust. 1 i art. 30c ustawy o ŻW; art. 32 ust. 1 i art. 32b ust. 1 ustawy o SKW.

[297] Zob. szerzej: raport RPO w sprawie wykonania wyroku Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce: www.bip.brpo.gov.pl/sites/default/files/2025-08/Załącznik%20Wykonanie%20wyroku%20Europejskiego%20Trybunału%20Praw%20Człowieka%20w%20sprawie%20Pietrzak%20i%20Bychawska-Siniarska%20i%20inni%20przeciwko%20Polsce.pdf.

[298] Z uwagi na możliwość pozyskania danych niedotyczących treści w procedurze niepodlegającej kontroli sądowej. Warto także zauważyć, że krajowy system dostępu do danych niedotyczących treści sprawia, że funkcjonariusze Policji i innych służb pełnią w zasadzie rolę „gatekeeperów". Tj. oni kontrolują ostęp do zasobów, informacji, są w zasadzie odpowiedzialni za „filtrowanie" dostępu do danych niedotyczących treści. Nie taka powinna być ich rola, na co zwracała uwagę Komisja Wenecka w opinii o nowelizacji ustawy o Policji z 2016 r. Zob. pkt 121 opinii Komisji Weneckiej dostępnej na stronie: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL(2016)019-e.

Może to prowadzić do nieuprawnionej ingerencji np. w tajemnicę dziennikarską i prowadzić do ujawnienia dziennikarskich źródeł informacji[299]. Na podstawie danych transmisyjnych, w tym danych z billingów, możliwe jest ustalenie, z kim kontaktował się dziennikarz w interesującym służby policyjne lub służby specjalne czasie, orientacyjnie ustalenie, w jakich miejscach i z kim (np. pozyskując dane transmisyjne osób, z którymi często się kontaktował w danym okresie)[300]. Zestawienie danych jednego dziennikarza z danymi osób trzecich zwielokrotnia ingerencję, obejmując także osoby, które nie są przedmiotem żadnego postępowania, a jedynie „przy okazji" znalazły się w sferze zainteresowania organów państwa. W wyroku ETPC w sprawie Big Brother Watch i inni przeciwko Wielkiej Brytanii (wyrok Izby)[301] Trybunał stwierdził naruszenie art. 10 EKPC w sytuacji, kiedy przepisy krajowe odnoszące się do zatrzymywania i uzyskiwania dostępu do danych niedotyczących treści mogły prowadzić do ujawnienia dziennikarskich źródeł informacji[302]. ETPC odnotował, że w porównaniu ze „standardową"[303] retencją danych, w przypadku możliwości ujawnienia źródeł informacji, działania inwigilacyjne były możliwe wyłącznie w związku ze zwalczaniem „poważnej przestępczości" *(serious crimes)*. Zwrócił ponadto uwagę, że przepisy szczególne, wprowadzające wyższy stopień społecznej szkodliwości czynu, mają zastosowanie wyłącznie w przypadku, gdy celem wniosku jest ustalenie źródła informacji. Nie mają zatem zastosowania w każdym przypadku uzyskania/sformułowania żądania dostępu do danych niedotyczących treści dziennikarza, co prowadzi do naruszenia art. 10 EKPC[304].

Możliwość ujawnienia tożsamości dziennikarskich źródeł informacji – realna na podstawie obowiązujących przepisów o dostępie do danych niedotyczących treści – wymusza poszukiwanie alternatywnych form kontaktu, co może zniechęcać osoby,

[299] O ochronie dziennikarskich źródeł informacji zob. także: W. Jasiński, *Gromadzenie dowodów w procesie karnym a ochrona dziennikarskich źródeł informacji w świetle orzecznictwa Europejskiego Trybunału Praw Człowieka*, EPS 2018, nr 8, s. 12-17; a także uwagi w pkt IV.2.2. dotyczące wyroku Sedletska przeciwko Ukrainie.

[300] Jako przykład można podać sprawę dziennikarza Mariusza Gierszewskiego i dziennikarki Dominiki Długosz-Gierszewskiej: https://www.press.pl/tresc/62526,dziennikarze-zlozyli-zazalenia-na-umorzenie-sledztwa-ws_-ich-inwigilacji; https://www.wirtualnemedia.pl/podsluchy-dziennikarzy-sledztwo-umorzone,7170053449062017a.

[301] Wyrok ETPC (Wyrok Izby) z dnia 13 września 2018 r. w sprawie *Big Brother Watch i inni przeciwko Zjednoczonemu Królestwu,* skargi nr 58170/13, 62322/14, 24960/15.

[302] Wyrok ETPC (Wyrok Izby) z dnia 13 września 2018 r. w sprawie *Big Brother Watch i inni przeciwko Zjednoczonemu Królestwu,* skargi nr 58170/13, 62322/14, 24960/15; § 496-498.

[303] Wyrok ETPC (Wyrok Izby) z dnia 13 września 2018 r. w sprawie *Big Brother Watch i inni przeciwko Zjednoczonemu Królestwu,* skargi nr 58170/13, 62322/14, 24960/15; Por. § 460-468.

[304] Wyrok ETPC (Wyrok Izby) z dnia 13 września 2018 r. w sprawie *Big Brother Watch i inni przeciwko Zjednoczonemu Królestwu,* skargi nr 58170/13, 62322/14, 24960/15; § 499.

które mają wiedzę o nieprawidłowościach w instytucjach państwowych, samorządowych, społecznych, czy przedsiębiorstwach prywatnych itp. do kontaktu z mediami[305].

Na gruncie przepisów procesowych – art. 218 § 1 k.p.k. w zw. z art. 180 § 3 k.p.k. – wątpliwości budzi możliwość uzyskania dostępu do danych z bilingów (danych transmisyjnych) w celu ustalenia dziennikarskich źródeł informacji. Część autorów wskazuje, że jest to niedopuszczalne ze względu na bezwzględny zakaz dowodowy[306]. Inni – że skoro art. 218 k.p.k. nie zawiera ograniczeń w tym zakresie, to można pozyskać takie dane[307]. To stanowisko zwraca uwagę na brak dostępu do treści komunikacji elektronicznej i że zakaz dowodowy nie ma aż tak szerokiego zakresu, by obejmować inne informacje. Stanowisko – jak się wydaje kompromisowe – wskazuje, że organy procesowe mogą uzyskać dostęp do danych transmisyjnych każdej osoby, ale w przypadku dziennikarskich źródeł informacji nie będzie możliwe wykorzystanie tak pozyskanego dowodu z uwagi na system zakazów dowodowych (art. 226 k.p.k. w zw. z art. 180 § 3 k.p.k.)[308]. Przy obecnym ukształtowaniu przepisów ustaw policyjnych i o służbach specjalnych oraz utworzeniu „stałego łącza" dostępu do danych telekomunikacyjnych, spór doktrynalny w kwestii pozyskania danych utracił na znaczeniu. Odrębną kwestią jest jednak ocena dopuszczalności dowodowego wykorzystania takich materiałów.

Szeroki zakres dostępu do danych niedotyczących treści może negatywnie wpływać na prowadzenie obrony w sprawach karnych. Adwokat lub radca prawny muszą bowiem liczyć się z możliwością, że ich dane lokalizacyjne, transmisyjne i abonenckie znajdują się albo mogą się znaleźć w posiadaniu organów lub funkcjonariuszy służb specjalnych albo policyjnych.

Dziennikarze, adwokaci, radcowie prawni i inne osoby zobowiązane do poszanowania tajemnic z art. 180 § 2 k.p.k. nie powinny być wyłączone z mechanizmu dostępu do

[305] Ogranicza też ochronę sygnalistów, zwłaszcza jeśli mieliby oni informować o nieprawidłowościach w działalności służb czy organów procesowych.
[306] Zob. A. Bojańczyk, *Billingi na specjalnych prawach*, Rzeczposp. PCD 2004, nr 12, s. 3; A. Bojańczyk, *Billingi jednak na specjalnych prawach*, Rzeczposp. PCD 2005, nr 1, s. 12.
[307] Zob. J. Śliwa, *Billingi pod specjalnym nadzorem*, Rzeczposp. PCD 2004, nr 12, s. 28.
[308] Por. M. Rusinek, *4.3. Wykorzystanie dokumentów w procesie* [w:] *Tajemnica zawodowa i jej ochrona w polskim procesie karnym*, Warszawa 2007.

danych retencyjnych[309]. Przeciwnie, jeśli dostęp do tych danych jest niezbędny z uwagi na bezpieczeństwo państwa albo dotyczy to najpoważniejszych przestępstw (np. wskazanych w art. 240 § 1 k.k.), to niecelowe byłoby pozbawianie się przez organy państwa cennych źródeł informacji (zwłaszcza jeśli nie wiąże się to z dostępem do treści komunikacji). Konieczne jest jednak wyważenie proporcji, ograniczenie zakresu spraw, w których można pozyskać dane wrażliwe od tych kategorii podmiotów oraz wprowadzenie efektywnego, uprzedniego nadzoru sądu lub organu sądowego nad dostępem do danych niedotyczących treści. Niekoniecznie taki nadzór musi być sprawowany przez sąd – nie chodzi przecież o dostęp do treści komunikatów przesyłanych drogą elektroniczną, co daje większą swobodę w ukształtowaniu przepisów – wystraczające jest, by był to niezależny od władzy wykonawczej organ sądowy[310].

Podsumowując.

Po pierwsze, otwarty zakres podmiotowy i przedmiotowy dostępu do danych retencyjnych powoduje, że trudno przewidzieć, kiedy i w jakich okolicznościach dane abonenckie, lokalizacyjne i dane o ruchu zostaną pozyskane i przekazane organom procesowym albo organom policyjnym lub służbom specjalnym. W konsekwencji, założenie, że dostęp może dotyczyć praktycznie każdej osoby, nie jest nierealne. Przepisy nie wprowadzają bowiem żadnych ograniczeń podmiotowych: po dane można sięgać wobec osób podejrzanych, podejrzanych lub oskarżonych, ale także wobec pokrzywdzonych, świadków oraz osób trzecich, które mogły jedynie incydentalnie kontaktować się z oskarżonym, czy pokrzywdzony.

Po drugie, przy szeroko zakreślonych zadaniach niektórych służb, a zwłaszcza Centralnego Biura Aantykorupcyjnego dostęp do danych może być realizowany niezależnie od podejrzenia przestępstwa, co sprzyja pozyskiwaniu informacji w trybie „sprawdzenia na wypadek", zamiast jako reakcji na konkretne, społecznie niepożądane zachowanie.

---

[309] Por.: raport RPO w sprawie wykonania wyroku Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce: www.bip.brpo.gov.pl/sites/default/files/2025-08/Załącznik%20Wykonanie%20wyroku%20Europejskiego%20Trybunału%20Praw%20Człowieka%20w%20sprawie%20Pietrzak%20i%20Bychawska-Siniarska%20i%20inni%20przeciwko%20Polsce.pdf w kontekście ochrony tajemnic i braku wyłączeń podmiotowych w tym zakresie. Skoro można prowadzić działania inwigilacyjne w klasycznej formie, obejmującej treść komunikatów przesyłanych drogą elektroniczną, to tym bardziej można pozyskać dane z bilingów.

[310] Tak również: M. Kiziński, *Retencja danych telekomunikacyjnych*, Prok.i Pr. 2016, nr 1, s. 138-155.

Po trzecie, brak ograniczeń podmiotowych osłabia praktyczną ochronę tajemnic zawodowych z art. 180 § 2 k.p.k. Przepisy (np. art. 20c i 20cb ustawy o Policji oraz analogiczne przepisy w pozostałych ustawach policyjnych i o służbach specjalnych) nie odsyłają do przepisów k.p.k. dotyczących zwolnienia z tajemnicy (art. 180 § 2 k.p.k.). Dodatkowo mechanizm „stałego łącza", wyłącznie formalna kontrola sądowa *ex post* i brak informowania osoby o pozyskaniu danych utrudniają weryfikację, czy prowadzono działania, które mogłyby ingerować w tajemnice prawnie chronione. W konsekwencji realne jest ryzyko ingerencji w tajemnicę dziennikarską i ujawnienia dziennikarskich źródeł informacji. Z danych z billingów i danych lokalizacyjnych można odtworzyć sieć kontaktów i okoliczności spotkań, a zestawianie danych dziennikarza z danymi osób trzecich zwielokrotnia zakres ingerencji.

Po czwarte, szeroki dostęp do danych może wywoływać efekt mrożący (zniechęcać do kontaktu z mediami, utrudniać sygnalizowanie nieprawidłowości) oraz wpływać na wykonywanie funkcji zawodowych, w tym na prowadzenie obrony w sprawach karnych (ryzyko pozyskania danych adwokatów i radców). Dane grup osób z art. 180 § 2 k.p.k., m.in. np. dziennikarzy, adwokatów, radców prawnych nie powinny być całkowicie wyłączone z kręgu podmiotów, do których danych abonenckich, lokalizacyjnych i transmisyjnych, uprawnione organy mogą pozyskać dostęp. Konieczne jest jednak zawężenia zakresu spraw, w których można sięgać po dane szczególnie wrażliwe, oraz wprowadzenia efektywnego uprzedniego nadzoru organu niezależnego od władzy wykonawczej.

VII.4. Zasady dostępu, wykorzystania i niszczenia danych

VII.4.1. Zasady dostępu

Nie powielając uwag wskazanych w pkt VII.1. odnoszących się do organów uprawnionych do pozyskania danych abonenckich, transmisyjnych i o lokalizacji w trybie procesowym i pozaprocesowym, warto dokonać analizy dwóch trybów dostępu do tych danych w trybie pozaprocesowym. Ustawą z dnia z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw[311] dodano przepisy pozwalające na uzyskanie dostępu do danych niedotyczących treści w trybie, który nie podlega kontroli sądowej[312]. W uzasadnieniu do projektu ww. ustawy nie wyjaśniono, dlaczego – wprowadzając kontrolę sądową *ex post* pozyskania danych telekomunikacyjnych –

[311] Ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz. U. poz. 147).
[312] Por. część VII.1.

utworzono alternatywny tryb dostępu wyjęty spod jakiegokolwiek nadzoru niezależnego organu[313]. W opinii Krajowej Izby Radców Prawnych do druku sejmowego Sejmu VIII kadencji nr 154 wskazano, że kształt projektowanych przepisów prowadzi „jednoznacznego wniosku, iż **proponowana regulacja nie tylko nie przystaje do demokratycznych standardów, wyznaczonych w wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r. (sygn. akt K 23/11), ale dodatkowo poszerza zakres rozwiązań niezgodnych z Konstytucją Rzeczypospolitej Polskiej z 2 kwietnia 1997 r. Jest również co najmniej wątpliwa z punktu widzenia prawa unijnego oraz orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej**"[314]. W odniesieniu do art. 20cb ustawy o Policji[315] na wadliwość tej regulacji zwracała uwagę Pierwsza Prezes Sądu Najwyższego, podkreślając szeroki zakres danych, jakie są wyłączone spod jakiegokolwiek nadzoru sądowego[316], Biuro Analiz Sejmowych, w odniesieniu do pozyskania danych niedotyczących treści, sygnalizowało niezgodność projektowanych rozwiązań z prawem UE[317].

Zakres danych, jaki może zostać pozyskany w trybie art. 20c ustawy o Policji został omówiony w części II. Zakres danych, jaki może zostać pozyskany w trybie art. 20cb ustawy o Policji[318] to:

- na podstawie art. 43 ust. 1 pkt 1 lit. a tiret drugi

  - dane abonentów związanych z komunikatami elektronicznymi przesyłanymi w ramach świadczonej publicznie dostępnej usługi telekomunikacyjnej, obejmujących:

  - dane, o których mowa w art. 296 ust. 1 p.k.e.,

---

[313] Zob. Uzasadnienie do poselskiego projektu ustawy o zmianie ustawy o Policji i niektórych innych ustaw, druk sejmowy Sejmu VIII kadencji nr 154, s. 12; https://orka.sejm.gov.pl/Druki8ka.nsf/0/B1A37C48E0F8ECBAC1257F290035A6B5/%24File/154.pdf.

[314] Zob. Stanowisko Ośrodka Badań, Studiów i Legislacji Krajowej Rady Radców Prawnych dotyczące poselskiego projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk sejmowy Nr 154), https://orka.sejm.gov.pl/Druki8ka.nsf/0/9E317D85E84BDE3DC1257F310041F2E8/%24File/154-002.pdf; s. 8 i 9.

[315] A zatem i analogicznych przepisów w pozostałych ustawach.

[316] Opinia w sprawie poselskiego projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw Pierwszej Prezes Sądu Najwyższego, s. 10; https://orka.sejm.gov.pl/Druki8ka.nsf/0/6DD6555FEF040B65C1257F4700373DF8/%24File/154-004.pdf.

[317] Zob. Opinia w sprawie zgodności z prawem Unii Europejskiej poselskiego projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw; https://orka.sejm.gov.pl/Druki8ka.nsf/0/B30BB05699C73CE8C1257F310040516D/%24File/154-001.pdf.

[318] Oraz art. 28b ustawy o ABW; art. 10bb ustawy o SG; art. 115 ust. 1 ustawy o KAS; art. 59 ust. 1 ustawy o SOP; art. 18b ust. 1 ustawy o CBA; art. 30c ustawy o ŻW; art. 32b ust. 1 ustawy o SKW.

- przydzielony numer, o ile został przydzielony, a w przypadku przyłączenia do stacjonarnej sieci telekomunikacyjnej także adres zakończenia sieci,

- adres korespondencyjny oraz adres wskazany na potrzeby komunikacji elektronicznej, o ile zostały przez abonenta podane.

Przepis art. 43 ust. 1 pkt 1 lit. a tiret drugi odsyła do art. z art. 296 ust. 1 p.k.e., który dotyczy uzyskania informacji o abonencie (danych abonenckich) takich jak:

1) w przypadku abonenta będącego osobą fizyczną:

a) imię (imiona) i nazwisko,

b) numer PESEL, jeżeli go posiada albo nazwę, serię i numer dokumentu potwierdzającego tożsamość, a w przypadku cudzoziemca, który nie jest obywatelem państwa członkowskiego albo Konfederacji Szwajcarskiej - numer paszportu lub karty pobytu;

2) w przypadku abonenta niebędącego osobą fizyczną:

a) nazwę,

b) numer identyfikacyjny REGON lub NIP lub numer w Krajowym Rejestrze Sądowym albo informację o wpisie do Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub innym właściwym rejestrze,

c) na żądanie dostawcy usług - dane osób reprezentujących abonenta, umożliwiające dostawcy usług ich weryfikację, w szczególności dane określone w pkt 1;

- na podstawie art. 389 p.k.e., który odsyła do art. 386 ust. 1 pkt 2-5 p.k.e.[319] możliwy jest dostęp do danych objętych tajemnicą komunikacji elektronicznej, takich jak:

- dane transmisyjne,

- dane o lokalizacji,

[319] Przepis art. 386 ust. 1 pkt 2 mówi o treści komunikatów przesyłanych drogą elektroniczną, zatem, nie „danych niedotyczących treści", a komunikatów przesyłanych drogą elektroniczną. Do treści komunikatów można mieć dostęp jedynie na podstawie przepisów o kontroli operacyjnej. Stąd poniżej zawężenie do pkt 3-5, ponieważ one dotyczą metadanych.

- dane o próbach uzyskania połączenia między zakończeniami sieci, w tym dane o nieudanych próbach połączeń, oznaczających połączenia między telekomunikacyjnymi urządzeniami końcowymi lub zakończeniami sieci, które zostały zestawione i nie zostały odebrane przez użytkownika końcowego lub nastąpiło przerwanie zestawianych połączeń.

Dostęp do danych z art. 386 ust. 1 pkt 3-5 p.k.e. jest możliwy przez odesłanie z art. 389 ust. 1 p.k.e. Udostępnienie na żądanie uprawnionego podmiotu w trybie poza kontrolą sądową mieści się bowiem w zakresie przetwarzania danych objętych tajemnicą komunikacji elektronicznej w innych celach niż świadczenie usługi dopuszczalnym na podstawie innych przepisów ustawowych.

Na szeroki zakres danych, które mogą być uzyskane w trybie wyłączonym spod kontroli sądowej z art. 20cb ustawy o Policji, zwracała uwagę Pierwsza Prezes Sądu Najwyższego[320]. Pojawia się jednak pytanie, jakie dane mogą być wyłącznie uzyskane w trybie art. 20c ustawy o Policji[321], tj. w trybie, gdzie możliwa jest kontrola sądowa w trybie art. 20ca ustawy o Policji[322].

Przepis art. 20c ust. 1 ustawy o Policji[323] uprawnia do dostępu do danych niedotyczących treści określonych w art. 45 ust. 1 i art. 49 p.k.e. Przepis art. 45 ust. 1 p.k.e. odsyła zaś do art. 43 ust. 1 pkt 1 lit. a tiret drugi, art. 386 ust. 1 pkt 1 i 3-5 oraz art. 389 i art. 390 ust. 2 p.k.e., czyli – poza art. 390 ust. 2 p.k.e. – do danych, które mogą być pozyskane w trybie wyłączonym spod kontroli sądowej. Jeśli chodzi o przepis art. 49 p.k.e., to on odnosi się przede wszystkim do danych transmisyjnych, tj. klasycznych danych z bilingów i danych o lokalizacji. Jednocześnie – w trybie wyłączonym spod kontroli sądowej – dane transmisyjne mogą zostać pozyskane na podstawie art. 389 ust. 1 zd. 2 p.k.e. w zw. z art. 386 ust. 1 pkt 5 p.k.e.

Niemal tożsamy zakres danych niedotyczących treści może być pozyskany w trybie poddanym kontroli sądowej, co w trybie wyłączonym spod kontroli sądowej. Dane z billingów (wykazy połączeń), dane lokalizacyjne, dane abonenckie mogą być pozyskane w takim samym zakresie w trybie art. 20c

[320] Opinia w sprawie poselskiego projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw Pierwszej Prezes Sądu Najwyższego, s. 10; https://orka.sejm.gov.pl/Druki8ka.nsf/0/6DD6555FEF040B65C1257F4700373DF8/%24File/154-004.pdf.

[321] Oraz art. 28 ust. 1 ustawy o ABW; art. 10b ustawy o SG; art. 114 ustawy o KAS; art. 57 ust. 1 ustawy o SOP; art. 18 ust. 1 ustawy o CBA; art. 30 ust. 1 ustawy o ŻW; art. 32 ust. 1 ustawy o SKW.

[322] Oraz art. 28a ustawy o ABW; art. 10ba ustawy o SG; art. 116 ustawy o KAS; art. 58 ustawy o SOP; art. 18a ustawy o CBA; art. 30b ustawy o ŻW; art. 32a ustawy o SKW.

[323] Oraz analogiczne przepisy w ustawach o innych służbach wskazane we wcześniejszym przypisie.

ustawy o Policji, jak i w trybie z art. 20cb ustawy o Policji. Jedyną zamkniętą kategorią danych zastrzeżoną dla art. 20c ustawy o Policji są dane spoza art. 386 ust. 1 pkt 3–5 p.k.e., w szczególności dane z art. 390 ust. 2 p.k.e. Przepis ten pozwala przedsiębiorcom komunikacji elektronicznej świadczących usługę na rzecz użytkownika innego przedsiębiorcy komunikacji elektronicznej przetwarzać dane dotyczące tego użytkownika oraz dane o wykonanych na jego rzecz usługach komunikacji elektronicznej. Chodzi m.in. o dane techniczne, które zostały wytworzone w związku z konkretną usługą.

Porządkując powyższe rozważania, warto zwrócić uwagę na poniższe kwestie.

Po pierwsze, od 2016 r. funkcjonują w Policji dwa pozaprocesowe tryby dostępu do danych niedotyczących treści: z kontrolą sądową *ex post* oraz tryb wyłączony spod kontroli sądowej. Przepisy wyłączające określone kategorie danych spod kontroli sądowej wprowadzono w związku z implementacją wyroku o sygn. K 23/11, ale w uzasadnieniu zmian nie wyjaśniono, dlaczego obok kontroli *ex post* wprowadzono równoległy tryb bez nadzoru.

Po drugie, pozasądowy tryb dostępu do danych retencyjnych pozwala na pozyskanie szerokiego zestawu danych: danych abonenckich (identyfikacyjnych, adresowych, numerów, danych rejestrowych) oraz – przez odesłania w ustawie - Prawo komunikacji elektronicznej – również danych objętych tajemnicą komunikacji elektronicznej, w tym danych transmisyjnych, lokalizacyjnych i danych o próbach połączeń (także nieudanych).

Po trzecie, w efekcie zakres danych dostępnych w obu trybach jest niemal tożsamy, co dodatkowo osłabia wprowadzony mechanizm sprawozdawczej kontroli sądowej.

VII.4.2.Zasady wykorzystania

Dane niedotyczące treści mogą być przetwarzane i wykorzystane wyłącznie w związku z realizacją celów, do jakich zostały pozyskane. **O ile jednak dane niedotyczące treści nie zostaną przekazane prokuratorowi w związku z prowadzonym lub przyszłym postępowaniem karnym, nie jest możliwe zweryfikowanie, czy faktycznie tak się stało**[324] (tj. np. czy dane pozyskane formalnie w związku z podejrzeniem popełnienia przestępstwa przez inną osobę, zostały następnie wykorzystane, by ustalić dziennikarskie źródła informacji). Dane niedotyczące treści mogą – zgodnie z art. 20c

[324] Zob. pkt VII.5 o mechanizmach kontroli.

ust. 8 ustawy o Policji[325] - zostać udostępnione organom ścigania państw członkowskich Unii Europejskiej i innych państw, agencjom Unii Europejskiej zajmującymi się zapobieganiem i zwalczaniem przestępczości oraz Międzynarodowej Organizacji Policji Kryminalnej - Interpol na ich wniosek, jeżeli następuje to w celu wykrywania przestępstw oraz ścigania ich sprawców, ratowania życia lub zdrowia ludzkiego albo poszukiwania osób zaginionych.

Co więcej, nawet wykorzystanie danych niedotyczących treści zgodnie z celami ich pozyskania określonymi w ustawie, nie oznacza, że z perspektywy norm ponadustawowych, ingerencja w prywatności jednostki była uzasadniona. Jeśli dane transmisyjne/dane o ruchu, czy lokalizacyjne uzyskano w związku z np. wykroczeniem skarbowym (do czego uprawniona jest KAS) albo prewencyjną i profilaktyczną kontrolą oświadczeń majątkowych funkcjonariuszy publicznych (a takie kompetencje posiada CBA), to nie jest spełniony wymóg proporcjonalności i konieczności w państwie demokratycznym. W sprawach o wykroczenia skarbowe oraz w czynnościach o charakterze prewencyjnym i kontrolnym brak jest wystarczającego uzasadnienia dla stosowania tego rodzaju środków. Cele tych postępowań mogą – co do zasady – zostać osiągnięte przy wykorzystaniu instrumentów mniej ingerujących w sferę prywatności. W konsekwencji ingerencja ta nie może zostać uznana za niezbędną w demokratycznym państwie prawa, nawet jeżeli znajduje podstawę w przepisach prawa krajowego.

Wykorzystanie procesowe danych transmisyjnych, lokalizacyjnych i abonenckich, które uzyskały służby policyjne lub służby specjalne, jest możliwe. W takiej sytuacji, jeśli pozyskane informacje mają znaczenie dla postępowania karnego, komendant Główny Policji, Komendant CBŚP, Komendant BSWP, Komendant CBZC albo komendant wojewódzki Policji przekazują prokuratorowi właściwemu miejscowo lub rzeczowo[326]. O zakresie i sposobie wykorzystania danych decyduje prokurator.

Prokurator (albo w zależności od służby – Prokurator Krajowy w przypadku ABW – art. 28 ust. 6 ustawy o AWB – i CBA – art. 18 ust. 6 ustawy o CBA – albo Prokurator Generalny w przypadku SKW – art. 32 ust. 8 ustawy o SKW) może podjąć decyzję o wykorzystaniu

[325] Oraz art. 10b ust. 8 ustawy o SG.

[326] Por. art. 20c ust. 6 ustawy o Policji. W odniesieniu do innych służb i organów zob.: art. 28 ust. 6 ustawy o ABW (decyzję o wykorzystaniu danych podejmuje Prokurator Krajowy); art. 18 ust. 6 ustawy o CBA (decyzję o wykorzystaniu danych podejmuje Prokurator Krajowy); art. 32 ust. 8 ustawy o SKW (decyzję o wykorzystaniu danych podejmuje Prokurator Generalny); art. 10b ust. 6 ustawy o SG (decyzję o wykorzystaniu danych podejmuje prokurator); art. 30 ust. 6 ustawy o ŻW (decyzję o wykorzystaniu danych podejmuje prokurator); art. 57 ust. 6 ustawy o SOP (decyzję o wykorzystaniu danych podejmuje prokurator).

wyników czynności operacyjnych, pozaprocesowych w postępowaniu przygotowawczym. Tylko bowiem w tym stadium postępowania prokurator jest organem procesowym i decyduje o dopuszczalności dowodu. **Wykorzystanie danych niedotyczących treści jako podstawy wyrokowania należy jednak do decyzji sądu.** W akcie oskarżenia, względnie innej skardze oskarżycielskiej (wniosku o umorzenie postępowania i zastosowanie środka zabezpieczającego, wniosku o rozpoznanie sprawy w trybie przyspieszonym)[327], prokurator ma obowiązek przedstawić wykaz dowodów do przeprowadzenia na rozprawie (art. 333 § 1 pkt 2 k.p.k.). Wykaz dowodów to w istocie wykaz wniosków dowodowych, jakie oskarżyciel publiczny składa wraz ze skargą oskarżycielską. Sąd ma obowiązek ocenić z perspektywy art. 170 § 1 k.p.k., wszystkie wnioski dowodowe stron postępowania, w tym wniosek prokuratora o dopuszczenie jako dowodu materiałów pozyskanych od dostawców usług łączności – zarówno w sytuacji, gdy dane niedotyczące treści zostały pozyskane w trybie procesowym z art. 218 k.p.k., jaki i w trybie pozaprocesowym.

Pojawia się pytanie, czy sąd może uznać dane niedotyczące treści za dowód niedopuszczalny w procesie karnym na podstawie art. 170 § 1 pkt 1 k.p.k. M. Rojszczak proponuje, by – z uwagi na niezgodność krajowych przepisów z prawem unijnym – odmówić dopuszczenia dowodów. Wskazuje, że „zapewnienie skuteczności wykładni TS wymaga pominięcia niezgodnych przepisów prawa krajowego. Dlatego w obecnym stanie prawnym wszystkie dowody z retencji danych telekomunikacyjnych włączane do akt spraw karnych na podstawie decyzji (postanowienia) oskarżyciela publicznego należałoby uznać za uzyskane z naruszeniem prawa (bezprawne)”[328]. Autor ten zwraca uwagę na systemowe nieprawidłowości w pozyskiwaniu danych niedotyczących treści, które nie powinny być ignorowane w jednostkowych postępowaniach karnych. Sąd, analizując znaczenie przedstawionych dowodów, „powinien nie tylko rozważyć ich wpływ i znaczenie w kontekście okoliczności faktycznej danej sprawy, ale również ocenić stopień ingerencji związany ze stosowaniem bezprawnej procedury gromadzenia i udostępniania danych dla całego modelu zabezpieczeń prawnych, stanowiących podstawę rzetelnego procesu”[329].

[327] We wniosku o skazanie bez rozprawy – art. 335 k.p.k. oraz wniosku o warunkowe umorzenie postępowania – art. 336 k.p.k. nie zamieszcza się wykazu dowodów do przeprowadzenia na rozprawie, ponieważ te skargi oskarżycielskie rozpoznawane są na posiedzeniu (art. 343 k.p.k. i art. 342 k.p.k.).
[328] M. Rojszczak, *Wadliwe dowody z retencji danych telekomunikacyjnych a polska procedura karna*, PiP 2023, nr 2, s. 48.
[329] M. Rojszczak, *Wadliwe dowody z retencji danych telekomunikacyjnych a polska procedura karna*, PiP 2023, nr 2, s. 50.

W wyroku ETPC w sprawie *Škoberne przeciwko Słowenii* Trybunał badał zgodność systemu retencji danych w Słowenii z art. 8 EKPC. Stwierdzając naruszenie art. 8 EKPC z uwagi na niespełnienie wymogów „jakości prawa"[330], nie ETPC nie odniósł się jednak do kwestii ewentualnego naruszenia art. 6 EKPC z powodu wykorzystania jako podstawy wyroku skazującego danych uzyskanych z naruszeniem art. 8 EKPC[331]. Kwestia dopuszczalności dowodów powinna być rozstrzygana zgodnie z mającym zastosowanie prawem krajowym.

Wydaje się, że zachowawcze stanowisko ETPC w kwestii oceny dopuszczalności dowodów z danych niedotyczących treści (danych telekomunikacyjnych i danych lokalizacyjnych) wynika z dwóch przyczyn. Po pierwsze, kwestia dopuszczalności dowodów jest domeną prawa krajowego. ETPC nie kreuje zasad dopuszczalności dowodów ani ich niedopuszczalności. Wyjątek dotyczy tzw. konwencyjnych zakazów dowodowych sensu stricto, tj. dowodów uzyskanych bezpośrednio z naruszeniem art. 3 EKPC (wolność od tortur lub nieludzkiego lub poniżającego traktowania) albo w wyniku przekroczenia granic prowokacji policyjnej (art. 6 ust. 1 EKPC)[332]. Po drugie, wykorzystanie danych podlegających retencji w sprawach karnych może dotyczyć spraw z zakresu bezpieczeństwa narodowego lub bezpieczeństwa powszechnego. W tych kategoriach spraw, państwa korzystają z szerokiego marginesu swobody. ETPC przypomina, że „jeżeli chodzi o kwestię tego, czy ingerencja była „konieczna w demokratycznym społeczeństwie" w celu realizacji uzasadnionego celu, władze krajowe korzystają z marginesu uznania przy wyborze środków służących osiągnięciu uzasadnionych celów, w tym między innymi ochrony bezpieczeństwa narodowego lub

[330] Wyrok ETPC z 15.02.2024 r. w sprawie Škoberne przeciwko Słowenii, skarga nr 19920/20. Jeśli chodzi o wymóg jakości prawa, to Trybunał wskazał, że obejmuje on nie tylko dostępność i przewidywalność prawa krajowego, ale także zapewnienie odpowiednich gwarancji przed nadużyciami, systemu zabezpieczeń – skutecznych w praktyce – by metody niejawnej inwigilacji były stosowane wyłącznie wtedy, gdy jest to konieczne w demokratycznym społeczeństwie. Zob. Wyrok ETPC z 15.02.2024 r. w sprawie Škoberne przeciwko Słowenii, skarga nr 19920/20, § 120 i cytowane tam orzecznictwo ETPC.

[331] Wyrok ETPC z 15.02.2024 r. w sprawie Škoberne przeciwko Słowenii, skarga nr 19920/20, § 146. ETPC odwołał się do wyroku w sprawie Bykov przeciwko Rosji. Zob. wyrok ETPC z dnia 10 marca 2009 r. w sprawie Bykov przeciwko Rosji, skarga nr 4378/02, § 89-91.

[332] Zob. szerzej: M. Wąsek-Wiaderek, *Model zakazów dowodowych z perspektywy Konwencji i orzecznictwa ETPCz* [w:] J. Skorupka, A. Drozd (red.), *Nowe spojrzenie na model zakazów dowodowych w procesie karnym*, Warszawa 2015; D. Czerniak, *Należyta staranność w zabezpieczeniu, gromadzeniu i ocenie dowodów* [w:] *Europeizacja postępowania dowodowego w polskim procesie karnym. Wpływ standardów europejskich na krajowe postępowanie dowodowe*, Warszawa 2021.

zapobiegania i ścigania przestępstw”[333]. W sprawach dotyczących bezpieczeństwa narodowego margines oceny jest szczególnie szeroki[334].

Co do zasady, w większości przypadków sąd powinien odmówić dopuszczenia dowodu obejmującego dane niedotyczące treści pozyskane w trybie pozaprocesowym, dokonując oceny proporcjonalności ingerencji oraz uwzględniając systemowe wadliwości krajowego mechanizmu retencji danych. Niemniej, nie sposób wykluczyć, że w wąskiej kategorii spraw, obejmujących bezpieczeństwo narodowe, przeważający interes publiczny, konieczność ochrony interesów narodowych, będzie jednak przemawiał za dopuszczalnością tak pozyskanych materiałów. Podstawą wykluczenia dowodu powinien być art. 170 § 1 pkt 1 k.p.k. **Niedopuszczalność dowodu wynika z niezgodności krajowego systemu pozyskania danych niedotyczących treści i nieproporcjonalnej ingerencji w prawo do prywatności (art. 47 i 49 Konstytucji, art. 8 EKPC, art. 7 KPP), a wykorzystanie takich materiałów w procesie karnym skutkowałoby naruszeniem prawa do rzetelnego procesu (art. 45 ust. 1 Konstytucji, art. 6 ust. 1 EKPC, art. 47 KPP).**

Warto także zwrócić uwagę, że mechanizm dostępu do danych niedotyczących treści z art. 218 § 1 k.p.k. także budzi wątpliwości z perspektywy standardów europejskich. Jeśli bowiem materiały pozyskano na podstawie decyzji prokuratora – oskarżyciela publicznego – to nie jest to zgodne z prawem unijnym. Prokurator nie jest bowiem niezależnym organem[335], który może sprawować efektywny nadzór nad pozyskaniem danych o lokalizacji, transmisyjnych, itp.

Podsumowując tę część rozważań, warto zwrócić uwagę na kilka zagadnień.

Po pierwsze, nawet jeśli przepisy krajowe przewidują określone cele i podstawy pozyskania danych niedotyczących treści przez Policję i inne organy, poza sytuacją, kiedy materiały te zostaną przekazane prokuratorowi i włączone do akt postępowania karnego, trudno jest realnie zweryfikować, w jaki sposób dane zostały następnie wykorzystane i czy nie doszło do ich użycia w innym celu niż deklarowany.

Po drugie, zakres możliwego „obrotu”, czy przetwarzania danych niedotyczących treści obecnie nie ogranicza się wyłącznie do krajowych organów. Przepisy m.in. art. 20 ust. 8 ustawy o Policji, dopuszczają ich udostępnianie także podmiotom zagranicznym (w tym organom ścigania państw UE i innych państw, agencjom UE oraz Interpolowi) na

[333] Wyrok ETPC z 15.02.2024 r. w sprawie *Škoberne przeciwko Słowenii,* skarga nr 19920/20; § 124.
[334] Wyrok ETPC z 25.05.2021 r. w sprawie *Centrum för rättvisa przeciwko Szwecji*, skarga 35252/08; § 252.
[335] Por. uwagi w pkt III.2.4. i wyrok TSUE z dnia 2 marca 2021 r., H.K. przeciwko Prokuratuur, C-746/18.

potrzeby wykrywania i ścigania przestępstw, ratowania życia i zdrowia lub poszukiwania zaginionych.

Po trzecie, zgodność działania z celem ustawowym, tj. dostęp do danych niedotyczących treści w celu zwalczania przestępczości, nie przesądza jeszcze o zgodności ingerencji ze standardami ponadustawowymi. W szczególności pozyskiwanie danych transmisyjnych/danych o ruchu lub lokalizacyjnych w sprawach o wykroczenia skarbowe, drobne czyny zabronione albo w ramach czynności prewencyjno-kontrolnych budzi wątpliwości z perspektywy przesłanek konieczności i proporcjonalności w społeczeństwie demokratycznym.

Po czwarte, sąd orzekający w sprawie karnej powinien dokonać oceny dopuszczalności dowodu z danych niedotyczących treści (albo pozyskanych w trybie art. 218 k.p.k. albo wprowadzonych do procesu karnego wyników czynności operacyjnych) z perspektywy art. 170 § 1 pkt 1 k.p.k. Konieczne jest uwzględnienie zasady proporcjonalności i konieczności w społeczeństwie demokratycznym przy ocenie dopuszczalności tej kategorii dowodów oraz wzięcie pod uwagę wadliwości całego krajowego systemu retencji danych. W konkretnej sprawie niedopuszczalność dowodu będzie wynikała z niezgodności krajowego systemu pozyskania danych niedotyczących treści i nieproporcjonalnej ingerencji w prawo do prywatności (art. 47 i 49 Konstytucji, art. 8 EKPC, art. 7 KPP) oraz braku przeważającego interesu publicznego, przez co wykorzystanie takich materiałów w procesie karnym skutkowałoby naruszeniem prawa do rzetelnego procesu (art. 45 ust. 1 Konstytucji, art. 6 ust. 1 EKPC, art. 47 KPP).

VII.4.3.Zasady niszczenia

Dane, które nie zostały przekazane prokuratorowi, powinny zostać niezwłocznie zniszczone. Zgodnie z art. 20c ust. 7 ustawy o Policji „dane, o których mowa w ust. 1, które nie mają znaczenia dla postępowania karnego, podlegają niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu”[336]. **Brak jest jednak jakiegokolwiek nadzoru zewnętrznego nad zniszczeniem zbędnych danych.** Komendant Główny Policji, Komendant CBŚP, Komendant BSWP, Komendant CBZC albo komendant wojewódzki Policji, względnie ich zastępcy[337], nie mają obowiązku informować o tym ani

[336] Por. także: art. 28 ust. 7 ustawy o ABW; art. 18 ust. 7 ustawy o CBA; art. 32 ust. 9 ustawy o SKW; art. 10b ust. 7 ustawy o SG; art. 30 ust. 7 ustawy o ŻW; art. 57 ust. 7 ustawy o SOP; art. 123 ustawy o KAS.
[337] A także odpowiednie organy w pozostałych ustawach o służbach policyjnych i służbach specjalnych.

prokuratora, ani sądu. Zniszczenie materiałów nie podlega sądowej kontroli z art. 20ca ustawy o Policji[338].

Organem, który sprawuje pieczę nad zniszczeniem materiałów niemożliwych do wykorzystania w postępowaniu karnym, jest organ policyjny lub służb specjalnych, który uprzednio zaakceptował dostęp do danych niedotyczących treści. Nie daje to gwarancji, że dane o jednostce nie zostaną wykorzystane sprzecznie z celem ich pozyskania albo że nie będą przechowywane – mimo ich zbędności – w dalszym ciągu.

Właściwe byłoby wprowadzenie zmian, które przyznają organowi zewnętrznemu względem Policji, ABW i innych służb specjalnych i policyjnych, nadzór nad zniszczeniem materiałów. Wydaje się, że wystarczające byłoby rozszerzenie uprawnień innych niezależnych organów uprawnionych do przestrzegania prawidłowości przetwarzania danych osobowych, np. Urzędu Ochrony Danych Osobowych, czy ewentualnie – właściwego miejscowo prokuratora okręgowego, który o zniszczeniu danych informowałby sąd. Organ kontrolujący prawidłowość niszczenia zbędnych danych, powinien mieć możliwość nakazania zniszczenia określonych materiałów, jeśli – po przeprowadzonej kontroli – okaże się, że dalsze ich przechowywanie jest nieproporcjonalne.

W raporcie z 2013 r. Najwyższa Izba Kontroli wśród stwierdzonych nieprawidłowości wskazała nieusuwanie zbędnych danych. W ocenie NIK „konieczne jest pilne wprowadzenie przepisów w zakresie obowiązku niszczenia zbędnych danych telekomunikacyjnych będących w posiadaniu służb. Przepisy powinny nie tylko określić sam obowiązek niszczenia danych, ale również precyzować tryb i sposób jego realizacji”[339].

Podsumowując tę część analizy.

Po pierwsze, przepisy przewidują obowiązek niezwłocznego, komisyjnego i protokolarnego zniszczenia danych, które nie mają znaczenia dla postępowania karnego (art. 20c ust. 7 ustawy o Policji), jednak mechanizm ten działa w praktyce bez zewnętrznego nadzoru.

---

[338] Analogiczne rozwiązanie znajduje się w pozostałych przepisach o służbach specjalnych i służbach policyjnych. Por. art. 28a ustawy o ABW; art. 18a ustawy o CBA; art. 32a ustawy o SKW, art. 10ba ustawy o SG; art. 30a ustawy o ŻW; art. 58 ustawy o SOP, art. 116 ustawy o KAS.

[339] Raport NIK, *Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180c i d ustawy Prawo telekomunikacyjne*, KPB-P/12/191, Warszawa 2013, s. 16; https://www.nik.gov.pl/plik/id,5421,vp,7038.pdf.

Po drugie, decyzja o zniszczeniu pozostaje w gestii tej samej formacji, która wcześniej akceptowała dostęp do danych, a brak obowiązku informowania prokuratora lub sądu oraz brak objęcia niszczenia kontrolą sądową *ex post* osłabiają weryfikowalność tego procesu.

Po trzecie, obowiązujący model nie daje wystarczających gwarancji, że dane nie będą przechowywane, mimo zbędności lub wykorzystywane w sposób wykraczający poza cel ich pozyskania.

Po czwarte, wskazywanym kierunkiem zmian jest wprowadzenie nadzoru organu zewnętrznego względem organów policyjnych i służb specjalnych (np. poprzez rozszerzenie kompetencji UODO albo mechanizm udziału prokuratora okręgowego z informowaniem sądu), w tym z możliwością nakazania zniszczenia materiałów, gdy dalsze ich przechowywanie jest nieproporcjonalne.

VII.5. Istnienie zewnętrznych mechanizmów kontrolnych i ich efektywność[340]

Ponownie odwołując się do raportu Najwyższej Izby Kontroli[341] warto przypomnieć, że już w 2013 r. NIK zwracał uwagę na brak jakichkolwiek mechanizmów kontroli zewnętrznej nad pozyskiwaniem billingów (danych niedotyczących treści). Raport został przygotowany przed wprowadzeniem regulacji z art. 20ca ustawy o Policji[342].

---

[340] Por. także raport RPO w sprawie wykonania wyroku Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce: www.bip.brpo.gov.pl/sites/default/files/2025-08/Załącznik%20Wykonanie%20wyroku%20Europejskiego%20Trybunału%20Praw%20Człowieka%20w%20sprawie%20Pietrzak%20i%20Bychawska-Siniarska%20i%20inni%20przeciwko%20Polsce.pdf.

[341] Wskazano tam m.in., że „Brak jest również mechanizmów kontroli o charakterze zewnętrznym, które pozwoliłyby na weryfikację zakresu wykorzystywania danych telekomunikacyjnych przez uprawnione podmioty, a w szczególności zasadności ich pozyskiwania i przetwarzania.". Tak: Raport NIK, *Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180c i d ustawy Prawo telekomunikacyjne*, KPB-P/12/191, Warszawa 2013, s. 8; https://www.nik.gov.pl/plik/id,5421,vp,7038.pdf.

[342] Przepis został dodany ustawą z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz. U. poz. 147). Analogiczne regulacje dodano w m.in. w ustawie o ABW, CBA, ŻW itd. A w nowych ustawach – wprowadzonych po 2016 r. – tj. w ustawie o SOP i KAS, analogiczne przepisy znalazły się „od razu". Zob. także uwagi w pkt II.2. w zakresie opinii Komisji Weneckiej o ustawie z dnia 15 stycznia 2016 r. oraz pkt VII.1.

Na etapie prac legislacyjnych posłowie – będący wnioskodawcami projektu[343] wskazywali, że ta regulacja stanowi wykonanie wyroku Trybunału Konstytucyjnego w sprawie o sygn. K 23/11. Problem jednak w tym, że kontrola sądowa została zaprojektowana tak, by nie dawała realnych narzędzi nadzorczych nad działalnością operacyjną Policji i innych służb w zakresie uzyskiwania dostępu do danych niedotyczących treści.

Wynika to z dwóch kwestii.

Po pierwsze, kontrola sądowa polega na przekazaniu do odpowiedniego sądu[344] sprawozdania obejmującego:

1) liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych, pocztowych lub internetowych oraz rodzaj tych danych;

2) kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne, pocztowe lub internetowe, albo informacje o pozyskaniu danych w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych.

Dane są przekazywane z zachowaniem przepisów o ochronie informacji niejawnych. W początkowej fazie obowiązywania przepisów ustawy o Policji, Fundacja Panoptykon w jednym z raportów zaprezentowała, w jaki sposób dane zostały przekazane do sądów, tj. w formie tabel, bez wskazania, np. celu pozyskania danych telekomunikacyjnych[345]. Warto wskazać, że sąd, przeprowadzając kontrolę w trybie art. 20ca ustawy o Policji[346] nie zapoznaje się z materiałami uzasadniającymi skorzystanie z czynności operacyjnej w postaci pozyskania danych o lokalizacji, danych o abonencie lub danych

[343] Zob. uzasadnienie do projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw, druk sejmowy Sejmu VIII kadencji nr 154 dostępny na stronie: https://orka.sejm.gov.pl/Druki8ka.nsf/0/B1A37C48E0F8ECBAC1257F290035A6B5/%24File/154.pdf.

[344] Co do zasady, do sądu okręgowego we właściwości którego odpowiednie służby pozyskały dane niedotyczące treści (tak: art. 116 ust. 1 ustawy o KAS; art. 10ba ust. 1 ustawy o SG; art. 30b ust. 1 ustawy o ŻW; art. 20ca ust. 1 ustawy o Policji). Ale niektóre przepisy ustaw przewidują wyłączną właściwość Sądu Okręgowego w Warszawie (por. art. 28 ust. 1 ustawy o ABW; art. 18a ust. 1 ustawy o CBA; art. 32a ust. 1 ustawy o SKW; art. 58 ust. 1 ustawy o SOP).

[345] Zob. raport Fundacji Panoptykon „Rok z ustawą inwigilacyjną" dostępny na stronie: https://panoptykon.org/inwigilacyjna.

[346] Por. także: art. 116 ustawy o KAS; art. 10ba ustawy o SG; art. 30b ustawy o ŻW; art. 28 ustawy o ABW; art. 18a ustawy o CBA; art. 32a ustawy o SKW; art. 58 ustawy o SOP).

transmisyjnych. Zgodnie z art. 20ca ust. 3 ustawy o Policji[347] „sąd okręgowy **może** zapoznać się z materiałami uzasadniającymi udostępnienie Policji danych telekomunikacyjnych, pocztowych lub internetowych". **Zapoznanie się z materiałami uzasadniającymi udostępnienie danych telekomunikacyjnych jest jedynie fakultatywne.** Pojawia się zatem pytanie, w jaki sposób możliwa jest rzetelna kontrola pozyskiwania danych niedotyczących treści, jeśli sąd nie sprawdza przyczyn sięgnięcia po tę inwazyjną metodę operacyjną (zwłaszcza jeśli chodzi o dostęp do danych o lokalizacji i danych transmisyjnych/danych o ruchu).

Po drugie, wprowadzając ograniczoną kontrolę sądową, jednocześnie istotnie osłabiono ten mechanizm. Dodano bowiem przepisy art. 20b ustawy o Policji wraz z analogicznymi przepisami w pozostałych ustawach policyjnych i o służbach specjalnych, które umożliwiały uzyskanie dostępu do danych niedotyczących treści poza kontrolą sądową. Zakres danych, jak to zostało wskazane w punkcie VI.4.3, jest niemal tożsamy w obu trybach. Zarówno w trybie podlegającym kontroli sądowej, jak i wyłączonym spod kontroli sądowej, można pozyskać dane o lokalizacji, dane transmisyjne i dane abonenckie.

W konsekwencji wyrok Trybunału Konstytucyjnego w sprawie o sygn. K 23/11 nadal nie został wdrożony. Co więcej niezgodność krajowego systemu nadzoru nad pozyskiwaniem danych niedotyczących treści się pogłębiła w związku z wejściem w życie dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW[348]. Dane niedotyczące treści, a zwłaszcza dane abonenckie, to dane

[347] [347] Por. także: art. 116 ust. 3 ustawy o KAS; art. 10ba ust. 3 ustawy o SG; art. 30b ust. 3 ustawy o ŻW; art. 28 ust. 3 ustawy o ABW; art. 18a ust. 3 ustawy o CBA; art. 32a ust. 3 ustawy o SKW; art. 58 ust. 3 ustawy o SOP.

[348] Dz. U. UE. L. z 2016 r. Nr 119, str. 89 z późn. zm.

osobowe[349]. Dane abonenckie, czy dane o IP mogą w łatwy sposób zostać powiązane z danymi o ruchu i danymi o lokalizacji. **Krajowe przepisy nie przewidują żadnej procedury informowania osoby, której dane zostały pozyskane i były/są przetwarzane (przechowywane) przez służby policyjne lub służby specjalne.** Zgodnie z art. 13 ust. 3, art. 15 i art. 16 ust. 4 dyrektywy 2016/680 możliwe jest ograniczenie prawa do uzyskania informacji o przetwarzaniu danych osobowych, ale w zakresie niezbędnym i proporcjonalnym w społeczeństwie demokratycznym oraz z należytym uwzględnieniem praw podstawowych i uzasadnionych interesów danej osoby fizycznej. Ograniczenie prawa do uzyskania informacji o przetwarzaniu danych osobowych jest możliwe, by:

„a) uniemożliwić utrudnianie czynności postępowań urzędowych lub sądowych, postępowań przygotowawczych lub procedur;

b) uniemożliwić zakłócanie zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar;

c) chronić bezpieczeństwo publiczne;

d) chronić bezpieczeństwo narodowe;

e) chronić prawa i wolności innych osób” (tak: art. 15 ust. 1 dyrektywy 2016/680).

Jeśli prawo do informacji zostało ograniczone, dyrektywa 2016/680 przewiduje wykonywanie uprawnień jednostki za pośrednictwem niezależnego organu. Przepis art. 17 ust. 1 dyrektywy 2016/680 nakazuje przyjęcie odpowiednich środków przewidujących, że osoba, której dane osobowe pozyskano w związku z zapobieganiem i zwalczaniem przestępczości, może wykonywać swoje prawa także za pośrednictwem właściwego organu nadzorczego. O prawie do pośredniego wykonywania uprawnień w zakresie informacji o przetwarzaniu danych osobowych, należy pouczyć jednostkę. Jeśli prawo do informacji o przetwarzaniu danych osobowych jest wykonywane za pośrednictwem niezależnego organu nadzorczego, organ ten ma obowiązek poinformować o przeprowadzeniu przeglądów lub weryfikacji. Dodatkowo,

[349] Definicja danych osobowych z art. 3 pkt 1 dyrektywy 2016/680 przez dane osobowe rozumie wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy bądź jeden lub kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

obowiązkiem krajowego ustawodawcy jest stworzenie mechanizmów pozwalających na zaskarżenie decyzji organu nadzorczego do sądu (art. 17 ust. 3 dyrektywy 2016/680).

Wdrażając dyrektywę 2016/680 w ustawie z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości [350] ustawodawca wprowadził możliwość wyłączenia informowania jednostki o przetwarzaniu jej danych osobowych w art. 26 wyżej wskazanej ustawy. To bardzo szeroka interpretacja art. 14 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości pozwalającego na ograniczenie prawa dostępu do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowych dotyczących jednostki[351]. Ograniczenie wprowadzone w art. 26 ustawy o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości jest tak szerokie, że prowadzi do wyłączenia uprawnienia z art. 14 dyrektywy 2016/680. Jednocześnie ustawodawca nie implementował art. 17 dyrektywy 2016/680. **W konsekwencji, pominięty został jeden z „najważniejszych przepisów dyrektywy 2016/680, którego istota tkwi w możliwości dokonywania przez organ nadzorczy (w Polsce PUODO) niezależnej oceny zasadności przetwarzania danych przez podmioty objęte zakresem dyrektywy"[352].**

W sytuacji, kiedy przepisy ustaw policyjnych i o służbach specjalnych nie przewidują obowiązku notyfikacji jednostki o pozyskaniu danych niedotyczących treści, ustawodawca wprowadził w art. 26 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości możliwość wyłączenia prawa dostępu do informacji o przetwarzaniu danych osobowych, a dodatkowo wyłączono pośrednie wykonywanie tego uprawnienia

[350] Dz. U. z 2023 r. poz. 1206.

[351] Zgodnie z art. 14 dyrektywy 2016/680 osobie, której dane osobowe były przetwarzane przysługuje prawo do informacji o: a) celu i podstawie prawnej przetwarzania; b) kategoriach odnośnych danych osobowych; c) informacjach o odbiorcach lub kategoriach odbiorców, których dane osobowe zostały ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych; d) w miarę możliwości planowanych okresach przechowywania danych osobowych lub, gdy nie jest to możliwe, kryteriach służących określeniu tego okresu; e) prawie do żądania od administratora sprostowania lub usunięcia danych osobowych lub ograniczenia przetwarzania danych osobowych dotyczących tej osoby; f) prawie wniesienia skargi do organu nadzorczego oraz dane kontaktowe organu nadzorczego; g) tym, jakie dane osobowe są przetwarzane, oraz wszelkich dostępnych informacjach o ich pochodzeniu.

[352] M. Kusak, P. Wiliński, *4.1.4. Prawo krajowe* [w:] M. Kusak, P. Wiliński, *Ochrona danych osobowych w ściganiu przestępstw. Standardy krajowe i unijne*, Warszawa 2020.

za pośrednictwem niezależnego organu, przetwarzanie danych osobowych nie podlega żadnej kontroli niezależnego organu[353]**.**

Podsumowując tę część analizy, w obecnym stanie prawnym, pozaprocesowe pozyskanie danych niedotyczących treści częściowo jest dokonywane pod nadzorem właściwego sądu okręgowego. **Nadzór ten trudno uznać za efektywny, a co równie istotne – przepisy nie zapewniają całościowego nadzoru nad dostępem do danych niedotyczących treści. Jednocześnie, ustawodawca nie implementował art. 17 dyrektywy 2016/680, ograniczając, a w zasadzie pozbawiając, uprawnień nadzorczych inny niezależny organ, tj. Prezesa Urzędu Ochrony Danych Osobowych.**

Wcześniej zostało wskazane, że przepisy ustaw policyjnych i o służbach specjalnych nie przewidują mechanizmu notyfikacji o uzyskaniu dostępu do danych telekomunikacyjnych, danych abonenckich oraz danych o lokalizacji. Osoba, której dane zostały pozyskane w celach wskazanych w poszczególnych ustawach, nie ma możliwości dowiedzenia się, czy np. Policja kontrolowała jej bilingi (dane transmisyjne) w związku z prowadzeniem czynności operacyjnych w sprawie o przestępstwo, itp. Tymczasem, co do zasady, każdy powinien mieć prawo uzyskania informacji o pozyskaniu jego/jej danych telekomunikacyjnych, wraz ze wskazaniem celu pozyskania danych, czasu ich pozyskania, przechowywania, itd., zgodnie z art. 14 dyrektywy 2016/680 oraz z art. 51 Konstytucji. Prawo do informacji mogłoby zostać odroczone na czas niezbędny ze względu na dobro wymiaru sprawiedliwości, np. do czasu zakończenia wszystkich czynności operacyjnych w sprawie, w której pozyskano dostęp do danych lokalizacyjnych, abonenckich lub transmisyjnych określonej osoby. W wąskiej kategorii spraw, dotyczących bezpieczeństwa narodowego (np. w sprawach o szpiegostwo), prawo do informacji mogłoby zostać wyłączone**. Jednakże, w sprawach, gdzie wyłączono możliwość bezpośredniego wykonywania uprawnienia z art. 14 dyrektywy 2016/680, musi zostać zapewnione pośredni nadzór prawidłowości przetwarzania danych osobowych (danych lokalizacyjnych, transmisyjnych i abonenckich) sprawowany w trybie art. 17 dyrektywy 2016/680.** Konieczne jest także wprowadzenie indywidualnego nadzoru sądowego w tych sytuacjach, gdy jednostka kwestionuje zasadność, legalność lub prawidłowość ingerencji w jej prawo do prywatności.

[353] Por. także wystąpienie generalne RPO, znak pisma: VII.501.315.2014.AG; https://bip.brpo.gov.pl/sites/default/files/opinia%20do%20uododo%2022.11.2018.pdf.

Jeśli chodzi o dostęp do danych niedotyczących treści w trybie procesowym, na podstawie art. 218 k.p.k., to przepisy k.p.k. gwarantują zarówno prawo do informacji o pozyskaniu danych, jak i kontrolę sądową w sprawach indywidualnych. Przepis art. 218 § 2 k.p.k. stanowi, że postanowienie o żądaniu uzyskania dostępu do danych z art. 45 ust. 1 i art. 49 p.k.e. doręcza się adresatom korespondencji oraz abonentom telefonu lub nadawcy, którego wykaz połączenia lub innych przekazów informacji został wydany. Doręczenie postanowienia można odroczyć na czas niezbędny ze względu na dobro sprawy, ale nie później niż do czasu prawomocnego zakończenia postępowania. Po doręczeniu postanowienia z art. 218 § 1 k.p.k. podlega ono zaskarżeniu na zasadach ogólnych z art. 236 k.p.k.[354]. Podmiotami uprawnionymi do wniesienia zażalenia są osoby, których prawo do tajemnicy korespondencji naruszono, abonentowi telefonu, którego wykaz połączeń, dane lokalizacyjne, transmisyjne zostały wydane, oraz podmiotom wydającym. Zażalenie, jeśli postanowienie z art. 218 § 1 k.p.k. zostało wydane przez prokuratora, przysługuje do sądu rejonowego, w okręgu, którego prowadzi się postępowanie. Jeśli zażalenie zostało wydane przez sąd, w postępowaniu sądowym, stosuje się zasady ogólne dotyczące zażalenia w postępowaniu sądowym. Zgodnie z art. 463 § 1 k.p.k., sąd, który wydał zaskarżone postanowienie, może je uwzględnić, jeśli orzeka w tym samym składzie. W innych wypadkach, zażalenie przekazuje się do sądu powołanego do rozpoznania zażalenia (co do zasady do sądu wyższej instancji).

Przepisy k.p.k. przewidują zatem obowiązek notyfikacji (informowania o uzyskaniu dostępu do danych niedotyczących treści). Warto jednak wskazać, że jedną z nieprawidłowości, na jaką zwróciła uwagę Najwyższa Izba Kontroli w raporcie z 2013 r., było nieprzestrzeganie procedur i niedoręczanie postanowień z art. 218 k.p.k.[355] Niedoręczenie postanowienia uniemożliwia sprawowanie kontroli sądowej – nie można bowiem zaskarżyć decyzji, która nie została ogłoszona jednostce. W praktyce możliwa jest sytuacja, kiedy strona, mając dostęp do akt sprawy karnej na zasadzie art. 156 § 1 (w postępowaniu sądowym) lub 5 (w postępowaniu przygotowawczym) k.p.k., może zapoznać się z postanowieniem, ale równocześnie – z uwagi na brak formalnego doręczenia – nie może kwestionować prawidłowości, legalności i zasadności pozyskania danych niedotyczących treści. Jedyną możliwością w takiej sytuacji jest kwestionowanie

[354] K. Sychta [w:] *Kodeks postępowania karnego. Komentarz*, red. J. Zagrodnik, Warszawa 2024, art. 218.

[355] Nieprawidłowości w zakresie doręczania decyzji z art. 218 k.p.k. stwierdzono w Prokuraturze Okręgowej w Rzeszowie, Warszawie i Katowicach, czyli w trzech z czterech kontrolowanych jednostek prokuratury. Raport NIK, *Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180c i d ustawy Prawo telekomunikacyjne*, KPB-P/12/191, Warszawa 2013, s. 80-81; https://www.nik.gov.pl/plik/id,5421,vp,7038.pdf.

dowodowego wykorzystania danych z art. 218 k.p.k. i dążenie do wyeliminowania tych materiałów z podstawy faktycznej orzeczenia. Taka pośrednia kontrola sądowa jest możliwa tylko wtedy, gdy prokurator skierował sprawę do sądu wraz ze skargą oskarżycielską.

Na marginesie, wydaje się, że termin notyfikacji wskazany w art. 218 § 2 k.p.k. jest wadliwie określony w odniesieniu do postępowania przygotowawczego. W przypadku procesowej kontroli i utrwalania rozmów, środka o wiele bardziej ingerującego w sferę prywatności jednostki, doręczenie postanowienia o zastosowaniu tzw. podsłuchu procesowego, może zostać odroczone na okres niezbędny ze względu na dobro postępowania, ale nie później niż do czasu zakończenia postępowania przygotowawczego (art. 239 § 2 k.p.k.). W przypadku danych niedotyczących treści, ten okres jest dłuższy, tj. do prawomocnego zakończenia postępowania karnego – jako całości. Osobie, której dane pozyskano, przysługuje zażalenie na postanowienie z art. 218 § 1 k.p.k. W tym kontekście, warto zwrócić uwagę na potencjalne problemy wynikające z dowodowego wykorzystania danych pozyskanych w trybie art. 218 § 1 k.p.k. jako podstawy wyroku skazującego. Jeśli sąd orzekający co do istoty – sąd meriti – dopuści dowody z art. 218 k.p.k. i wykorzysta je jako podstawę faktyczną orzeczenia, a sąd orzekający w przedmiocie zażalenia wniesionego w trybie art. 236 k.p.k. w zw. z art. 218 § 2 k.p.k., uzna, że doszło do naruszenia legalności lub zasadności uzyskania dostępu do danych niedotyczących treści, to w obrocie prawnym mogą istnieć dwie wykluczające się decyzje dotyczące materiału dowodowego. Jeśli bowiem nielegalnie lub niezasadnie uzyskano dostęp do danych niedotyczących treści, to sąd orzekający w sprawie co do istoty (a w zasadzie sądy – sąd I instancji albo sąd odwoławczy) powinien oddalić wniosek dowodowy prokuratora na podstawie art. 170 § 1 pkt 1 k.p.k.

Obok sądowej kontroli zewnętrznej (ogólnej i generalnej) oraz sądowej kontroli w sprawach indywidualnych, nadzoru nad pozyskaniem danych niedotyczących treści sprawowanym przez niezależny organ (Prezesa UODO), ważna jest także kontrola społeczna. Społeczeństwo, opinia publiczna, powinni mieć dostęp do rzetelnej informacji o pozyskiwaniu danych telekomunikacyjnych. Najwyższa Izba Kontroli w 2013 r. zaproponowała, by mechanizm sprawozdawczości obejmował w szczególności:

- „liczbę przypadków, w których uprawnione organy uzyskiwały od przedsiębiorców telekomunikacyjnych wyłącznie dane osobowe użytkownika;

- liczbę przypadków (rozumianych jako liczbę numerów telefonicznych lub numerów IP), w których uprawnione organy uzyskiwały dane telekomunikacyjne (z wyłączeniem ustaleń danych abonenckich);

- łączną liczbę przypadków, w których wniosek uprawnionego podmiotu nie mógł być zrealizowany (w rozbiciu na 2 ww. kategorie);

- liczbę osób, których dane telekomunikacyjne były pozyskiwane i wykorzystywane przez uprawnione organy (z wyłączeniem ustaleń danych abonenckich)"[356].

Propozycja ta jest co do zasady warta do rozważenia (i ewentualnego wprowadzenia), ale celowe byłoby rozbicie danych telekomunikacyjnych na dane transmisyjne (dane z bilingów) oraz na dane o lokalizacji. Wydaje się także, że warto byłoby wskazać, jaki był cel uzyskania dostępu do danych niedotyczących treści. Jeśli celem było pozyskanie tych danych w związku z zapobieganiem lub zwalczaniem przestępstw (a nie np. w związku z działaniami ratunkowymi lub poszukiwawczymi) rozważenia wymaga uzupełnienie sprawozdań publicznie dostępnych o rodzaj (kwalifikację prawną) przestępstwa. Dodatkowo, sprawozdawczość powinna być pełna – obejmować dane uzyskane w trybie pozaprocesowym i procesowym (art. 218 k.p.k.).

Podsumowując tę część analizy, warto uwypuklić cztery problemy.

Po pierwsze, sądowa kontrola pozaprocesowego pozyskiwania danych retencyjnych ma w praktyce charakter sprawozdawczo-statystyczny. Opiera się na informacjach o liczbie przypadków i kwalifikacjach czynów, przedstawionymi w formie tabelarycznej. Zapoznanie się przez sąd z materiałami uzasadniającymi sięgnięcie po dane retencyjne jest jedynie fakultatywne, co utrudnia ocenę konieczności i proporcjonalności w konkretnych sytuacjach.

Po drugie, obok tego – niedoskonałego mechanizmu kontroli sądowej *ex post* – funkcjonuje równolegle tryb dostępu do danych niedotyczących treści wyłączony spod kontroli sądowej, przy zbliżonym zakresie danych (abonent, dane transmisyjne, lokalizacja). Nadzór sądowy nie ma charakteru całościowego i można go w praktyce omijać.

[356] Raport NIK, *Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180c i d ustawy Prawo telekomunikacyjne*, KPB-P/12/191, Warszawa 2013, s. 71; https://www.nik.gov.pl/plik/id,5421,vp,7038.pdf.

Po trzecie, na poziomie ochrony danych osobowych problemem jest brak realnego mechanizmu informowania osoby o pozyskaniu i przetwarzaniu jej danych (m.in. numeru telefonu, numeru IP) w trybach pozaprocesowych oraz brak efektywnej ścieżki pośredniego wykonywania praw za pośrednictwem niezależnego organu, np. Prezesa UODO. W rezultacie ogranicza to możliwość weryfikacji legalności i zasadności ingerencji przez organ „zewnętrzny" względem służb policyjnych i służb specjalnych.

Po czwarte, w trybie procesowym z art. 218 k.p.k. przewidziano co do zasady notyfikację oraz kontrolę zażaleniową. Jednak odroczenie doręczenia do momentu prawomocnego zakończenia postępowania (art. 218 § 2 k.p.k.) wydłuża moment, w którym kontrola indywidualna staje się realna. Rozwiązanie to jest niespójne systemowo, uwzględniając fakt, że notyfikacja w przypadku procesowej kontroli i utrwalania rozmów może zostać odroczona do momentu zakończenia postępowania przygotowawczego (art. 239 § 2 k.pk.). W przypadku środka mniej ingerującego w prawo do prywatności, decyzję procesową doręcza się uprawnionemu podmiotowi później, niż w przypadku środka bardziej dolegliwego.

VIII. Wnioski i zalecenia

Obecny model retencji danych, jaki i dostępu do danych retencyjnych, jest wadliwy na wielu poziomach. Zasadniczym problemem – z perspektywy zgodności krajowych rozwiązań ustawowych z normami prawnymi wyższego rzędu – jest uogólniona i niezróżnicowana retencja danych o ruchu i danych o lokalizacji *by default* (z założenia, jako model „wyjściowy"), a także brak precyzyjnie określonych celów zatrzymywania danych niedotyczących treści. Cele te bowiem można wyinterpretować z umiejscowienia przepisu art. 47 p.k.e., nie zaś z treści tej regulacji. **W odniesieniu do celów pozyskania danych, należy podkreślić, że cel w postaci ochrony bezpieczeństwa narodowego pozwala na dalej idące ograniczenia prawa do prywatności. Wyjątkowo, w tej sytuacji, dopuszczalna jest także uogólniona i niezróżnicowana retencja danych, ale wyłącznie pod warunkiem ograniczenia jej w czasie, a dane zatrzymane dla realizacji celu w postaci bezpieczeństwa narodowego nie mogą być wykorzystane np. dla zwalczania przestępstw niezwiązanych z tym bezpieczeństwem.** Przepisy krajowe powinny wprowadzać efektywne gwarancje zabezpieczające przed taką zmianą/niekompatybilności celu zatrzymania danych, z tym, do jakiej sprawy (do realizacji jakiego celu) zostały wykorzystane.

Problematyczne jest także uregulowanie zasad dostępu do danych retencyjnych (pozyskanie danych w formie „stałego łącza", bez zaangażowania pracowników dostawców usług łączności, możliwość dostępu do danych niedotyczących treści osób, które nie są w żaden sposób zaangażowane w jakąkolwiek działalność przestępczą), brak realnego nadzoru zewnętrznego nad dostępem do danych o ruchu, danych o lokalizacji, itd.: w formie kontroli sądowej następczej, w formie „społecznej" kontroli, w formie skarg indywidualnych, jeśli pozyskano dane konkretnej osoby. Próbując uporządkować wnioski *de lege ferenda,* jakie wynikają z analizy standardu konstytucyjnego, konwencyjnego i unijnego, z uwagi na liczbę zidentyfikowanych wadliwości krajowego systemu, podzielone one zostały na trzy grupy:

- zmiany w przepisach o retencji danych;

- zmiany w przepisach o dostępie do danych retencyjnych;

- zewnętrzna kontrola - kontrola społeczna, dostępu do danych retencyjnych oraz notyfikacja, jeśli organy ścigania lub organy procesowe uzyskały dostęp do danych retencyjnych.

Ad. 1. Zmiany w przepisach o retencji danych niedotyczących treści:

- należy „rozbić" dane niedotyczące treści na odrębne kategorie, tj. dane o abonencie, dane o IP, dane o ruchu (dane transmisyjne) i dane o lokalizacji. Prawo unijne i orzecznictwo ETPC różnicuje te kategorie danych biorąc pod uwagę ich „potencjał" ingerencyjny w prawo do prywatności i możliwość odtworzenia/stworzenia „intymnego portretu" danej osoby. Najmniejszy potencjał ingerencyjny mają dane o abonencie, największy – dane o ruchu i dane o lokalizacji;

- w związku z powyższym, konieczna jest zmiana systemowa i odejście od uogólnionej i niezróżnicowanej retencji danych o lokalizacji, danych o ruchu, danych o IP i danych o abonencie na takich samych zasadach. Takie ukształtowanie systemu krajowego – nawet jeśli służy zwalczaniu i zapobieganiu poważnej przestępczości – wiąże się z nieproporcjonalną ingerencją w prawo do prywatności. TSUE różnicuje zasady retencji danych, co powinno znaleźć odzwierciedlenie w prawie krajowym, czyli:

- niedopuszczalna jest uogólniona i niezróżnicowana retencja danych o ruchu i danych o lokalizacji. TSUE dopuszcza taką możliwość wyłącznie w przypadku realnego zagrożenia dla bezpieczeństwa narodowego. Rozwiązanie to ze swojej istoty musi być jednak rozwiązaniem czasowym – przejściowym – i obowiązującym jedynie do ustania realnego i rzeczywistego dla bezpieczeństwa narodowego, i nie może obowiązywać jako „domyślny", czy podstawowy system zatrzymywania danych. Zgodna z prawem unijnym jest natomiast ukierunkowana retencja danych o ruchu i o lokalizacji pod warunkiem, że kryteria ukierunkowanej retencji są obiektywne, niedyskryminacyjne, ograniczone czasowo i obszarowo (np. wprowadzono retencję danych każdej osoby znajdującej się na dworcach kolejowych, lotniskach itp.);

- dopuszczalna jest uogólniona i niezróżnicowana retencja danych o abonencie i danych o IP pod warunkiem, że przepisy wprost wskazują cele zatrzymywania danych, okres ich przechowywania;

- konieczne jest wskazanie celów retencji danych niedotyczących treści. W zależności od kategorii danych, dostęp do nich może być uzasadniony zwalczaniem poważnej przestępczości (np. jak w przypadku danych o ruchu i danych o lokalizacji), jeśli zostały zatrzymane w wyniku ukierunkowanej retencji danych albo ochroną bezpieczeństwa narodowego. Określenie celu retencji danej kategorii danych zapobiegałoby sytuacji, kiedy dane zatrzymane w celu bezpieczeństwa narodowego, byłyby wykorzystywane np. dla realizacji celu w postaci zwalczania przestępczości. Wprowadzając przepisy konkretyzujące cele retencji danych, należy uwzględnić „hierarchię celów", na którą

zwraca uwagę przede wszystkim TSUE (celem o najwyższej randze jest ochrona bezpieczeństwa narodowego, bezpieczeństwo powszechne i zwalczanie poważnej przestępczości są celami istotnymi, ale znajdującymi się niżej w hierarchii celów; dostęp do danych o lokalizacji i ruchu/transmisyjnych nie powinien być możliwy w sprawach, które należą do kategorii „drobnej" przestępczości z uwagi na brak proporcjonalności ingerencji w prawo do prywatności).

Obecnie, mimo tego, że ustawa - Prawo komunikacji elektronicznej weszła w życie 10 listopada 2024 r., nie zostały wydane rozporządzenia wykonawcze, o których mowa w art. 49 ust. 2 i 3 p.k.e. Rozporządzenie z art. 49 ust. 2 p.k.e. dotyczy określenia konkretnych kategorii danych, jakie podlegają obowiązkowi retencji. Z uwagi na niewydanie nowego rozporządzenia, w mocy pozostaje poprzednio obowiązujące – wydane na podstawie uchylonej ustawy - Prawo telekomunikacyjne – ale nie jest ono w pełni spójne (zwłaszcza jeśli chodzi o terminologię) z nowymi przepisami. Warto także zwrócić uwagę, że Komisja Wenecka krytycznie odniosła się do modelu, w którym zakres danych retencyjnych jest precyzowany w akcie prawnym wykonawczym (rozporządzeniu), a nie w ustawie. Uregulowanie tego rodzaju kwestii w rozporządzeniu stwarza ryzyko nadużyć i rozszerzania kategorii danych retencyjnych.

Ad. 2. Zmiany w przepisach o dostępie do danych retencyjnych

- dostęp do danych o ruchu i danych o lokalizacji powinien być możliwy wyłącznie po uzyskaniu uprzedniej zgody niezależnego organu. Kontrola uprzednia powinna mieć merytoryczny charakter (nie sprowadzać się do analizy spełnienia przesłanek formalnych np. prawidłowości sformułowania żądania), a organ, który podejmuje decyzję powinien mieć możliwość odmówić dostępu albo ograniczyć zakres żądania (np. skrócić okres/liczbę miesięcy za które służby/prokurator żądają dostępu do danych). W wypadkach niecierpiących zwłoki, służby specjalne i policyjne powinny móc niezwłocznie zabezpieczyć dane lokalizacyjne i dane transmisyjne/dane o ruchu, ale konieczne jest następcza zgoda niezależnego organu udzielana *post factum;*

- przepisy o dostępie do danych retencyjnych, tj. art. 20c ustawy o Policji i analogiczne przepisy w pozostałych ustawach o służbach specjalnych i służbach policyjnych oraz art. 218 k.p.k. powinny zawierać przesłanki ograniczające możliwość „łatwego" sięgania po dane retencyjne. Konieczne jest dodanie przesłanki subsydiarności (dostęp do danych o ruchu/transmisyjnych i danych o lokalizacji jest możliwy wtedy, gdy inne środki, mniej inwazyjne, są bezskuteczne albo okazałyby się bezskuteczne), proporcjonalności i

konieczności oraz wprowadzenie wymogu, by osoba, o dane której służby się zwracają, miała związek z popełnieniem/popełnianiem przestępstwa;

- w odniesieniu do spraw, kiedy służby mogą uzyskać dostęp do danych retencyjnych, konieczne jest wprowadzenie ograniczeń przedmiotowych – zwłaszcza w ustawie o CBA. Służby nie mogą sięgać po dane niedotyczące treści – zwłaszcza dane o lokalizacji i dane o ruchu – w związku z oceną partnerstwa publiczno-prywatnego, czy kontrolą oświadczeń majątkowych. W przypadku przestępstw i przestępstw skarbowych należy również ograniczyć zakres dopuszczalnego dostępu do danych o lokalizacji i danych o ruchu. Co do zasady służby mogłyby pozyskać ww. dane wyłącznie w sprawach zagrożonych karą co najmniej 3 lat pozbawienia wolności oraz w tych sprawach, zagrożonych karą łagodniejszą, które popełniono przy wykorzystaniu środków komunikowania się na odległość/przy wykorzystaniu Internetu. Nowe regulacje powinny zatem obejmować także m.in. art. 200a § 2 k.k., art. 257 k.k., art. 212 k.k., art. 216 k.k., art. 226 k.k. Alternatywnie, można rozważyć wprowadzenie rozwiązań w k.p.k., które pozwalają na dostęp do danych retencyjnych w sprawach zagrożonych karą łagodniejszą niż 3 lata pozbawienia wolności wyłącznie w trybie procesowym. W sprawach o średniej społecznej szkodliwości, np. zagrożonych karą do 5 lat pozbawienia wolności można rozważyć wprowadzenie ograniczenia w zakresie temporalnym żądania o dostęp do danych o lokalizacji i danych o ruchu. Pozyskanie danych za 12 miesięcy wstecz, w sprawach o średniej społecznej szkodliwości, może być środkiem nadmiernie nieproporcjonalnym;

- należy wzmocnić kontrolę sądową/organu sądowego. Konieczne jest zatem usunięcie – ze wszystkich ustaw – trybu dostępu do danych poza kontrolą sądową, o którym mowa w art. 20cb ustawy o Policji i analogicznych przepisach pozostałych ustaw policyjnych i o służbach specjalnych. Pojawia się jednak pytanie o kształt kontroli sądowej następczej. Z rozwiązań prawnomiędzynardowych wynika, że konieczna byłaby uprzednia kontrola dostępu do danych lokalizacyjnych i danych transmisyjnych/danych o ruchu. Następcza kontrola sądowa mogłaby znaleźć zastosowanie wyłącznie w odniesieniu do danych o abonencie i danych o IP;

- konieczne jest wprowadzenie pełnej rozliczalności dostępu do danych retencyjnych, w szczególności w sytuacji korzystania ze „stałego łącza", tj. dostępu bez zaangażowania dostawców usług łączności. Rozliczalność dostępu do danych, zwłaszcza danych o ruchu i danych o lokalizacji, nie może ograniczać się do ewidencji liczby zapytań lub logowań, ale powinna obejmować rejestry operacji pozwalające ustalić: kto, kiedy, w jakim trybie, w jakiej sprawie, w jakim celu i w jakim zakresie pozyskał dane. Rejestry powinny

uniemożliwiać modyfikowanie ich treści po fakcie, a jeśli taka modyfikacja nastąpiła – powinna być odnotowana w systemie, żeby możliwe było prześledzenie i przeanalizowanie wersji aktualnej i wersji historycznej;

- przepisy powinny wprowadzać obowiązek dokumentowania „ścieżki decyzyjnej" po stronie służb, tj. nie tylko samego żądania dostępu do danych, ale również decyzji wewnętrznej o wyborze kategorii danych, zakresu czasowego (tj. czy 6 czy 12 miesięcy wstecz); celem jest zapewnienie, by organ kontrolujący miał do dyspozycji materiał pozwalający na rekonstrukcję procesu decyzyjnego, a nie wyłącznie końcowy „efekt" w postaci pozyskanych danych;

- konieczne jest wprowadzenie w ustawach policyjnych i o służbach specjalnych oraz wprost w przepisach k.p.k. (np. w art. 218 k.p.k.) odrębnych gwarancji chroniących tajemnice prawnie chronione, zwłaszcza tajemnicę dziennikarską, w obszarze metadanych, tj. rozwiązań, które zapobiegają obejściu ochrony tajemnic przez sięganie po dane o ruchu i dane o lokalizacji (np. w celu identyfikacji źródeł dziennikarskich albo ustalenia kontaktów obrońcy z klientem).

- konieczne jest wprowadzenie do k.p.k. regulacji, które uniemożliwią „obchodzenie" przepisów o postępowaniu dowodowym przez „wyprowadzanie" czynności dowodowych do czynności operacyjnych. Jeżeli dane retencyjne są pozyskiwane w związku z toczącym się postępowaniem karnym, tj. na potrzeby prowadzonego postępowania przygotowawczego lub sądowego, ich pozyskanie powinno następować co do zasady w trybie procesowym przewidzianym w k.p.k., a nie w trybach właściwych dla czynności operacyjno-rozpoznawczych. Cel ten może zostać osiągnięty tylko w sytuacji, kiedy uprawnienia prokuratora w postępowaniu karnym będą „lustrzanym" odbiciem uprawnień, jakie ma Policja, czy inne służby. Sytuacja, w której prokurator ma mniejsze możliwości działania niż funkcjonariusze służb, a dodatkowo, nadzór zewnętrzny nad działalnością służb jest mocno ograniczony, skłania do „wyprowadzania" czynności dowodowych do czynności operacyjnych;

- doręczenie postanowienia z art. 218 k.p.k. może zostać odroczone, ale obecny termin z art. 218 § 2 k.p.k. pozwalający na odroczenie doręczenie postanowienia aż do prawomocnego zakończenia postępowania jest nieproporcjonalnie długi (zwłaszcza jak uwzględni się okoliczność, że odroczenie postanowienia o procesowej kontroli i utrwalaniu rozmów może nastąpić najpóźniej do czasu zakończenia postępowania przygotowawczego – art. 239 § 2 k.p.k.). Odroczenie doręczenia postanowienia z art. 218 § 1 k.p.k. w postępowaniu przygotowawczym powinno być możliwe do czasu

zakończenia postępowania przygotowawczego. W postępowaniu sądowym – taka decyzja powinna być ogłaszana niezwłocznie stronom postępowania. Na tym etapie procesu, z uwagi na pełną jawność akt postępowania – art. 156 § 1 k.p.k. – niecelowe jest odroczenie doręczenia decyzji procesowej, z którą treścią strona będzie mogła się zapoznać uzyskując dostęp do akt sprawy karnej, a jednocześnie nie będzie mogła jej zaskarżyć.

Ad. 3. Zewnętrzna kontrola - kontrola społeczna, dostępu do danych retencyjnych oraz notyfikacja, jeśli organy ścigania lub organy procesowe uzyskały dostęp do danych retencyjnych:

- konieczne jest wprowadzenie realnego mechanizmu notyfikacji jednostki o tym, że jej dane zostały pozyskane przez Policję lub inne służby. Możliwe jest przyjęcie rozwiązania analogicznego do mechanizmu funkcjonującego przy pozyskiwaniu danych w trybie procesowym (218 k.p.k.), tj. jednostka zostałaby poinformowana o tym, że jej dane zostały pozyskane od dostawców usług łączności przez organy ścigania po upływie odpowiedniego okresu np. 1 roku albo 2 lat od pozyskania danych retencyjnych. **W wąskiej kategorii spraw – np. tych dotyczących bezpieczeństwa narodowego – możliwe byłoby wyłączenie obowiązku notyfikacji z uwagi na przeważający interes publiczny;**

- równocześnie konieczne jest pełne wdrożenie art. 17 dyrektywy 2016/680, tj. zapewnienie jednostce możliwości wykonywania praw w trybie pośrednim w sytuacjach, gdy – z przyczyn dopuszczalnych w dyrektywie – ogranicza się jej prawo do informacji lub odmawia się udzielenia informacji o przetwarzaniu/pozyskaniu danych osobowych. Tryb pośredni powinien polegać na tym, że niezależny organ (organ nadzorczy) dokonuje weryfikacji legalności i zasadności przetwarzania oraz informuje jednostkę co najmniej o tym, że weryfikacja została przeprowadzona i czy stwierdzono naruszenia, a także zapewnia skuteczny środek zaskarżenia. Brak implementacji art. 17 dyrektywy 2016/680 w praktyce uniemożliwia wykonywanie praw jednostki w sytuacjach, w których notyfikacja jest odraczana albo ograniczana (w tym wyłączona dla ochrony bezpieczeństwa narodowego). Pełna implementacja dyrektywy 2016/680 wzmocniłaby nadzór nad czynnościami operacyjnymi i zwiększyłaby kompetencje Prezesa UODO;

- konieczne jest wprowadzenie standardów raportowania/sprawozdawczości, które pozwolą ocenić nie tylko „skalę" korzystania z danych retencyjnych. Sprawozdawczość powinna być pełna – obejmować informacje nie tylko o dostępie pozaprocesowym, ale

także całościowo dostęp w trybie art. 218 k.p.k. Sprawozdania, oprócz danych obecnie prezentowanych, powinny obejmować:

- liczbę przypadków, w których uprawnione organy uzyskiwały od przedsiębiorców telekomunikacyjnych wyłącznie dane osobowe użytkownika;

- liczbę przypadków (rozumianych jako liczbę numerów telefonicznych lub numerów IP), w których uprawnione organy uzyskiwały dane telekomunikacyjne (z wyłączeniem ustaleń danych abonenckich) z podzieleniem na odpowiednie kategorie (np. dane transmisyjne, dane o lokalizacji);

- łączną liczbę przypadków, w których wniosek uprawnionego podmiotu nie mógł być zrealizowany;

- liczbę osób, których dane telekomunikacyjne były pozyskiwane i wykorzystywane przez uprawnione organy (z wyłączeniem ustaleń danych abonenckich)"[357].

Warto byłoby wskazać, jaki był cel uzyskania dostępu do danych niedotyczących treści. Jeśli celem było pozyskanie tych danych w związku z zapobieganiem lub zwalczaniem przestępstw (a nie np. w związku z działaniami ratunkowymi lub poszukiwawczymi) rozważenia wymaga uzupełnienie sprawozdań publicznie dostępnych o rodzaj (kwalifikację prawną) przestępstwa.

Opracowała:

Dominika Czerniak

Ekspert prawny

/-wydano i podpisano elektronicznie/

[357] Raport NIK, *Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180c i d ustawy Prawo telekomunikacyjne*, KPB-P/12/191, Warszawa 2013, s. 71; https://www.nik.gov.pl/plik/id,5421,vp,7038.pdf.