



Warszawa, 07-04-2026 r.

RZECZNIK PRAW OBYWATELSKICH

Marcin Wiącek

II.519.1068.2022.DC

**Pan
Krzysztof Gawkowski
Wiceprezes Rady Ministrów - Minister Cyfryzacji
ePUAP**

**Pan
Waldemar Żurek
Minister Sprawiedliwości
Prokurator Generalny
ePUAP**

**Pan
Marcin Kierwiński
Minister Spraw Wewnętrznych i Administracji
ePUAP**

**Pan
Tomasz Siemoniak
Minister Koordynator Służb Specjalnych
ePUAP**

**Szanowny Panie Premierze,
Szanowni Panowie Ministrowie,**

wyrok Europejskiego Trybunału Praw Człowieka z dnia 28 maja 2024 r. w sprawie Pietrzak i Bychawska-Siniarska i inni przeciwko Polsce¹ w swojej zasadniczej części odnosił się do problematyki kontroli operacyjnej i wadliwości systemowych w tej sferze niejawnej inwigilacji. Aspekt ten został zaprezentowany w moim wystąpieniu z dnia 7

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

sierpnia 2025 r., którym wskazano niezbędne – i zasadnicze – kierunki zmian. Wystąpienie to przesyłam uprzejmie w załączeniu (załącznik nr 2), wraz z opracowaniem pt. „Wykonanie wyroku Europejskiego Trybunału Praw Człowieka w sprawie Pietrzak i Bychawska-Siniarska i inni przeciwko Polsce (sprawa nr 72038/17 i 25237/18). Raport w przedmiocie koniecznych zmian w przepisach regulujących pozaprosesową oraz procesową kontrolę i utrwalanie rozmów” (załącznik nr 3).

W odpowiedzi z dnia 28 października 2025 r. Minister Sprawiedliwości zapewnił, że obecnie prowadzone są prace legislacyjne nad wdrożeniem tego orzeczenia², jednak dotychczas żaden projekt, czy założenia do projektu przepisów nie zostały publicznie zaprezentowane. Minister Koordynator Służb Specjalnych w piśmie z dnia 6 października 2025 r.³ oraz Minister Spraw Wewnętrznych i Administracji w piśmie z dnia 9 września 2025 r.⁴, podkreślili konieczność uwzględnienia aspektu bezpieczeństwa narodowego oraz sytuacji, w jakiej obecnie się znajdujemy z uwagi na toczącą się wojnę Rosji z Ukrainą. Część postulatów, na jakie wskazano w wystąpieniu generalnym dotyczącym problematyki kontroli operacyjnej i procesowej kontroli i utrwalania rozmów, znalazło jednak odzwierciedlenie w projekcie ustawy o zmianie niektórych ustaw w celu wzmocnienia nadzoru sądowego nad kontrolą operacyjną (UD278)⁵, przede wszystkim ten odnoszący się do konieczności uzasadniania decyzji sądu w przedmiocie zgody na niejawną inwigilację. W protokole rozbieżności z dnia 13 lutego 2026 r. sporządzonym po przeprowadzeniu konsultacji międzyresortowych wskazano,

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 Pismo Ministra Koordynatora Służb Specjalnych z dnia 6 października 2025 r., DBN.WP.414.96.2025, dostępne na stronie: https://bip.brpo.gov.pl/sites/default/files/2025-10/Odpowiedz_koordinatora_sluzb_kontrola_operacyjna_zasady_6_10_2025.pdf.

⁴ Pismo Ministra Spraw Wewnętrznych i Administracji z dnia 9 września 2025 r., BMP.0790.3.5.2025(9), dostępne na stronie: https://bip.brpo.gov.pl/sites/default/files/2025-09/Odpowiedz_MSWiA_kontrola_operacyjna_zasady_9_09_2025.pdf.

⁵ Projekt dostępny na stronach Rządowego Centrum Legislacji: <https://legislacja.rcl.gov.pl/projekt/12404202>.

że „Na tym tle⁶ należy wskazać, że poszczególne rozwiązania zawarte w projekcie mogą odpowiadać na problemy dostrzeżone przez Europejski Trybunał Praw Człowieka w przywoływanym wyroku w sprawie Pietrzak i Bychawska-Siniarska i inni p. Polsce. Niemniej, sam projekt ustawy nie aspiruje do miana regulacji wykonującej to orzeczenie. Prace koncepcyjne w tym zakresie prowadzone są pod auspicjami innego resortu.”

Ufam, że wkrótce zostaną zaprezentowane kompleksowe założenia ustawy w pełni wdrażające wyżej wspomniane orzeczenie oraz uwzględniające postulaty wcześniej przeze mnie zgłoszone. Pracując nad implementacją wyroku ETPC w sprawie Pietrzak i Bychawska-Siniarska i inni przeciwko Polsce nie można pominąć jeszcze jednego aspektu - problematyki retencji danych i dostępu do danych retencyjnych.

Retencja danych telekomunikacyjnych często jest zagadnieniem poruszonym „na uboczu” zagadnień związanych z niejawną inwigilacją. Dostęp, pozyskiwanie i przechowywanie danych nie dotyczących 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

⁶ Było to odniesienie się do uwagi Ministerstwa Spraw Zagranicznych. MSZ wskazało, że „Proponowana nowelizacja ustaw (UD278) będzie jednym ze środków mających na celu rozwiązanie zidentyfikowanego przez Trybunał w ww. wyroku problemu systemowego. Niemniej jednak, nie będzie to wystarczająca interwencja legislacyjna, mając na uwadze zakres zmian koniecznych do wykonania wspomnianego wyroku. W tym miejscu należy podnieść, że kluczowa i pożądana zmiana powinna dotyczyć, oprócz wzmocnienia nadzoru nad stosowaniem kontroli operacyjnej, również kwestii powiadamiania osoby, względem której prowadzona była taka kontrola oraz umożliwienia jej zakwestionowania tego środka z mocą wsteczną, a także kwestii ukształtowania zasad retencji danych komunikacyjnych w sposób spełniający wymogi Konwencji. W oparciu o wstępną analizę przedstawionego OSR pragnę zaproponować rozważenie uzupełnienia nowelizacji w powyższym zakresie.”. Z protokołem rozbieżności, stanowiskiem MSZ można zapoznać się na stronach RCL: <https://legislacja.rcl.gov.pl/projekt/12404202>.

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. Analiza danych statystycznych w zakresie szeroko rozumianego pozyskiwania danych z bilingów (danych telekomunikacyjnych) jest alarmująca. Zgodnie z informacją przedstawianą przez Ministra Sprawiedliwości⁷ w 2024 r. uprawnione organy⁸ w trybie pozaprocesowym⁹ 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 nie dotyczących 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 karnych¹⁰.

ETPC w wyroku Pietrzak, Bychawska-Siniarska i inni przypomniał, że „w wyniku postępu technologicznego w komunikacji elektronicznej w ciągu ostatnich dwóch dekad, taka komunikacja może obecnie ujawniać dużą ilość danych osobowych. (...) 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

⁷ Druk sejmowy nr 1464; <https://sejm.gov.pl/Sejm10.nsf/druk.xsp?nr=1464>,

⁸ 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 Kontrywiadu Wojskowego, Żandarmeria Wojskowa, Inspektorat Wewnętrzny Służby Więziennej oraz Centralne Biuro Zwalczania Cyberprzestępczości.

⁹ Tryb procesowy, tj. na podstawie art. 218 k.p.k.

¹⁰ 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.

regulującymi przetwarzanie treści komunikatów”¹¹. Krajowy system retencji danych również został uznany za niespełniający wymogów wynikających z art. 8 EKPC. 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 wolności¹². 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. Problematyka retencji danych, dostępu do danych retencyjnych w aspekcie zgodności krajowych rozwiązań ze standardem konstytucyjnym (wynikającym przede wszystkim z wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., sygn. akt K 23/11), unijnym oraz strasburskim została omówiona w raporcie „Raport w przedmiocie retencji danych i dostępu do danych retencyjnych w świetle konstytucyjnych, unijnych i konwencyjnych standardów ochrony praw jednostki”, który również przesyłam uprzejmie w załączeniu (załącznik nr 1).

Ochrona bezpieczeństwa narodowego, integralności terytorialnej państwa ma nadrzędne znaczenie. Dlatego też, wyjątkowo w tej sytuacji dopuszczalna jest uogólniona i nieodróżnicowana retencja danych, ale pod warunkiem ograniczenia jej w czasie, a dane zatrzymane dla realizacji celu w postaci bezpieczeństwa narodowego nie mogą być wykorzystane np. dla zwalczania przestępstw. Przepisy krajowe powinny wprowadzać efektywne gwarancje zabezpieczające przed taką zmianą/niekompatybilnością celu zatrzymania danych.

Zasadniczym problemem – z perspektywy zgodności krajowych rozwiązań ustawowych z normami prawnymi wyższego rzędu – jest zaprojektowanie całego systemu retencji danych niejako „na wzór” standardu dopuszczalnego wyłącznie dla ochrony bezpieczeństwa narodowego. Krajowe przepisy pozwalają na uogólnioną i nieodróżnicowaną retencję danych o ruchu i danych o lokalizacji *by default*, tj. z założenia, jako model „wyjściowy”. Problematiczne jest także uregulowanie zasad dostępu do danych retencyjnych (pozyskanie danych w formie „stałego łącza”, bez zaangażowania pracowników dostawców usług łączności, możliwość dostępu do danych dotyczących osób, które nie są w żaden

¹¹ Wyrok ETPC z 28 maja 2024 r. w sprawie *Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce*, skargi nr 72038/17 i 25237/18; § 249.

¹² Dz. U. UE. L. z 2023 r. Nr 191, str. 118.

sposób zaangażowane w jakąkolwiek działalność przestępczą), brak realnego nadzoru zewnętrznego nad dostępem do danych o ruchu, danych o lokalizacji, itp.: w formie kontroli sądowej następczej, w formie „społecznej” kontroli czy też w formie skarg indywidualnych, jeśli pozyskano dane konkretnej osoby. W konsekwencji nie jest dalekie od prawdy stwierdzenie, że każdy może zostać poddany „soft” inwigilacji, niezależnie od jakiegokolwiek związku z działalnością przestępczą, a system został zaprojektowany tak, by jednostka nie dowiedziała się o pozyskaniu jej danych telekomunikacyjnych.

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 nieodróżnicowanej 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 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 nieodróżnicowana 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 nie dotyczących 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 konieczna 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, w których przestępstwo 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 dostępu 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/organy 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 prawnomiędzynarodowych 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 i tajemnicę obrończą, 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 doręczenia 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 której 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 wnioski uprawnionego podmiotu nie mógł być zrealizowany;
 - liczbę osób, których dane telekomunikacyjne były pozyskiwane i wykorzystywane przez uprawnione organy (z wyłączeniem ustaleń danych abonenckich)¹³.

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.

¹³ 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>.

Mając na uwadze przedłożone racje, stosownie do art. 16 ust. 2 pkt 1 ustawy z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich¹⁴, zwracam się do Pana Premiera i Panów Ministrów z uprzejmą prośbą o dokonanie analizy wskazanych w niniejszym stanowisku problemów i rozważenie zainicjowania zmian legislacyjnych w Kodeksie postępowania karnego¹⁵ oraz w następujących ustawach: Prawo komunikacji elektronicznej¹⁶, o Policji¹⁷, o Straży Granicznej¹⁸, o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu¹⁹, o Centralnym Biurze Antykorupcyjnym²⁰, o Służbie Wywiadu Wojskowego i Służbie Kontrwywiadu Wojskowego²¹, o Krajowej Administracji Skarbowej²², o Żandarmerii Wojskowej²³ oraz o Służbie Ochrony Państwa²⁴ oraz wznowienia prac nad rozporządzeniem wykonawczym²⁵ do art. 49 ust. 2 Prawa komunikacji elektronicznej. Będę nadto wdzięczny za poinformowanie mnie o stanowisku zajęтым w przedstawionej materii.

Z wyrazami szacunku

Marcin Wiącek

Rzecznik Praw Obywatelskich

/-wydano i podpisano elektronicznie/

¹⁴ Ustawa z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. z 2024 r., poz. 1264 ze zm.)

¹⁵ Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz. U. z 2025 r. poz. 46 z późn. zm.).

¹⁶ Ustawa z dnia 12 lipca 2024 r. - Prawo komunikacji elektronicznej (Dz. U. poz. 1221 z późn. zm.).

¹⁷ Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2025 r. poz. 636 z późn. zm.).

¹⁸ Ustawa z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2025 r. poz. 914 z późn. zm.)

¹⁹ Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2025 r. poz. 902 z późn. zm.).

²⁰ Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2025 r. poz. 712 z późn. zm.).

²¹ Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2026 r. poz. 157).

²² Ustawa z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (Dz. U. z 2025 r. poz. 1131 z późn. zm.).

²³ Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. z 2026 r. poz. 159).

²⁴ Ustawa z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (Dz. U. z 2025 r. poz. 34 z późn. zm.).

²⁵ Na stronach Rządowego Centrum Legislacji znajduje się projekt rozporządzenia dostępny na stronie: <https://legislacja.gov.pl/projekt/12399801/katalog/13142072#13142072>.

Załączniki:

1. Opracowanie pt. „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”;
2. Wystąpienie generalne RPO z dnia 7 sierpnia 2025 r., II.519.109.2015;
3. Opracowanie pt. „Wykonanie wyroku Europejskiego Trybunału Praw Człowieka w sprawie Pietrzak i Bychawska-Siniarska i inni przeciwko Polsce (sprawa nr 72038/17 i 25237/18). Raport w przedmiocie koniecznych zmian w przepisach regulujących pozaprosesową oraz procesową kontrolę i utrwalanie rozmów”.

Do wiadomości:

- Pan Mirosław Wróblewski, Prezes Urzędu Ochrony Danych Osobowych (ePUAP);
- Pan Mariusz Haładyj, Prezes Najwyższej Izby Kontroli (ePUAP);
- Pan Senator Krzysztof Kwiatkowski Przewodniczący Komisji Ustawodawczej Senatu RP (ePUAP);
- Pan Poseł Marek Ast Przewodniczący Komisji Ustawodawczej Sejmu RP (ePUAP).