Minister Spraw Wewnętrznych i Administracji

BMP.0790.3.5.2026(13)

Pan
Marcin Wiącek
Rzecznik Praw Obywatelskich

Szanowny Panie Rzeczniku,

odpowiadając na wystąpienie Pana Rzecznika[1] w przedmiocie wykonania wyroku Europejskiego Trybunału Praw Człowieka w sprawie Pietrzak i Bychawska-Siniarska i inni przeciwko Polsce (sprawa nr 72038/17 i 25237/18), uprzejmie przedstawiam stanowisko w odniesieniu do służb podległych ministrowi właściwemu do spraw wewnętrznych.

Ponownie należy podkreślić, że Ministerstwo Spraw Wewnętrznych i Administracji (MSWiA) dostrzega potrzebę wprowadzenia zmian w zakresie sposobu ukształtowania nadzoru sądu nad stosowaniem przez uprawnione służby kontroli operacyjnej. Z tego względu działania MSWiA koncentrują się obecnie na prowadzonych w Sejmie RP pracach legislacyjnych nad rządowym projektem ustawy o zmianie niektórych ustaw w celu wzmocnienia nadzoru sądowego nad kontrolą operacyjną (druk sejmowy nr 2411).

Natomiast w odniesieniu do podnoszonych przez Pana Rzecznika postulatów dotyczących obowiązującego modelu retencji metadanych, tj. danych telekomunikacyjnych, pocztowych i internetowych, należy w pierwszej kolejności wskazać, że określone w ustawach pragmatycznych służb podległych ministrowi właściwemu do spraw wewnętrznych uprawnienie nie pozwala na zobowiązanie dostawców usług telekomunikacyjnych do nieograniczonego i masowego przekazywania zatrzymywanych danych. Nie ma również możliwości i podstaw do dowolnego przeszukiwania przez służby baz danych przedsiębiorców telekomunikacyjnych oraz usługodawców świadczących usługi drogą elektroniczną. Dostęp funkcjonariuszy uprawnionych służb do tych danych ma charakter ukierunkowany, gdyż odbywa się na wniosek w stosunku do indywidualnie określonej osoby, miejsca lub urządzenia. Zgodnie z przepisami art. 20c ust. 1 ustawy z dnia 6 kwietnia 1990 r. *o Policji*[2] oraz art. 10b ustawy z dnia 12 października 1990 r. *o Straży Granicznej*[3] odpowiednio Policja i Straż Graniczna jest uprawniona do uzyskiwania metadanych w celu zapobiegania lub wykrywania przestępstw oraz przestępstw skarbowych, a Policja dodatkowo również w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych. Zauważyć przy tym należy, że dane te, co do zasady, mogą być pozyskiwane wyłącznie w zakresie niezbędnym do realizacji zadań związanych

[1] Pismo o sygn. II.519.1068.2022.DC.

[2] Dz.U. z 2025 r. poz. 636, z późn. zm.

[3] Dz.U. z 2026 r. poz. 367.

ul. Stefana Batorego 5
02-591 Warszawa, Polska

z zapobieganiem i wykrywaniem przestępczości, przy czym w odniesieniu do Straży Granicznej katalog czynów zabronionych, do których rozpoznawania, zapobiegania i wykrywania Straż Graniczna została upoważniona, określa art. 1 ust. 2 pkt 4 oraz ust. 2a ustawy *o Straży Granicznej*. Natomiast w odniesieniu do Służby Ochrony Państwa dane te można pozyskiwać wyłącznie w celu rozpoznania, zapobiegania i wykrywania przestępstw, o których mowa w art. 42 ust. 1 ustawy z dnia 8 grudnia 2017 r. *o Służbie Ochrony Państwa*[4] (art. 57 ust. 1 tejże ustawy).

W celu zapobiegania przestępstwom służby są zobligowane do podejmowania szybkich i zdecydowanych działań, które przełożą się na ich skuteczność. W takich sytuacjach często jedynym skutecznym rozwiązaniem, które już na samym początku procesu wykrywczego dostarczy licznych informacji niezbędnych do podjęcia dalszych działań, w tym pozwalających na ustalenie kręgu osób zaangażowanych w popełnienie przestępstwa, będzie uzyskanie metadanych. W tym kontekście należy zwrócić uwagę na zmieniający się obraz przestępczości. Aktualnie nawet takie czyny zabronione jak oszustwa czy uporczywe nękanie mają swój nieodzowny komponent technologiczny. Sprawcy wykorzystują zaawansowane narzędzia komunikacyjne, wiele kart SIM czy numery techniczne, aby zatrzeć ślady swojej działalności. Ich skuteczne ściganie wymaga więc ustalenia przez organy ścigania skomplikowanych łańcuchów powiązań. Powyższe wymusza analizę licznych sesji transmisji danych i logowań w celu zidentyfikowania użytkownika końcowego, co powoduje wzrost liczby zapytań o metadane. Wzrost ten warunkowany jest również ewaluacją infrastruktury telekomunikacyjnej. Przejście z technologii 3G na standardy 4G, a obecnie 5G wiąże się z ogromnym zagęszczeniem nadajników i częstotliwością przełączania się urządzeń. Urządzenia typu smartfon, tablet w sposób ciągły, zautomatyzowany komunikują się z siecią, co implikuje logowania do stacji bazowych (BTS), także w ramach odświeżania aplikacji w tle czy synchronizacji poczty, bez aktywności użytkownika. W celu odtworzenia przebiegu zdarzenia tylko w jednym postępowaniu niezbędne jest przeanalizowanie nieporównywalnie większego zbioru metadanych, co może być odczytywane jako wzrost zapytań, mimo utrzymującej się na podobnym poziomie liczby postępowań przygotowawczych.

Tryb udostępniania przez przedsiębiorcę telekomunikacyjnego, operatora pocztowego lub usługodawcę świadczącego usługi drogą elektroniczną danych określa art. 20c ust. 2 ustawy *o Policji*. Zgodnie z przytoczonym przepisem prawa wskazane podmioty udostępniają dane:

- funkcjonariuszowi wskazanemu w pisemnym wniosku Komendanta Głównego Policji, Komendanta Centralnego Biura Śledczego Policji (CBŚP), Komendanta Biura Spraw Wewnętrznych Policji (BSWP), Komendanta Centralnego Biura Zwalczania Cyberprzestępczości (CBZC), komendanta wojewódzkiego Policji albo osoby przez nich upoważnionej;
- na ustne żądanie funkcjonariusza posiadającego pisemne upoważnienie osób, o których mowa w pkt 1;

[4] Dz.U. z 2025 r. poz. 34, z późn. zm.

- za pośrednictwem sieci telekomunikacyjnej funkcjonariuszowi posiadającemu pisemne upoważnienie osób, o których mowa w pkt 1.

Doprecyzowanie przytoczonych regulacji stanowią przepisy art. 20c ust. 4 ustawy *o Policji* określające, że udostępnienie danych telekomunikacyjnych może nastąpić za pośrednictwem sieci telekomunikacyjnej wyłącznie jeżeli wykorzystywane sieci telekomunikacyjne zapewniają możliwość ustalenia osoby uzyskującej dane, ich rodzaj oraz czas, w którym zostały uzyskane, a także zabezpieczenie techniczne i organizacyjne uniemożliwiające osobie nieuprawnionej dostęp do danych. Ponadto taka forma udostępniania danych może mieć miejsce jedynie, jeżeli jest to uzasadnione specyfiką lub zakresem zadań wykonywanych przez jednostki organizacyjne Policji albo prowadzonych przez nie czynności. Analogiczne rozwiązania wynikają z art. 10b ust. 2 i 4 ustawy *o Straży Granicznej* oraz art. 57 ust. 2 i 4 ustawy *o Służbie Ochrony Państwa*. Mechanizm ten zapewnia więc wewnętrzną weryfikowalność przypadków pozyskiwania danych telekomunikacyjnych. Celowi temu służą również przepisy zobowiązujące uprawnione podmioty (Komendanta Głównego Policji, Komendanta CBŚP, Komendanta BSWP, Komendanta CBZC i komendanta wojewódzkiego Policji, Komendanta Głównego Straży Granicznej, Komendanta Biura Spraw Wewnętrznych Straży Granicznej i komendanta oddziału Straży Granicznej oraz Komendanta Służby Ochrony Państwa) do prowadzenia rejestrów wystąpień o uzyskanie danych telekomunikacyjnych, pocztowych i internetowych zawierających informacje identyfikujące jednostkę organizacyjną i funkcjonariusza uzyskującego te dane, ich rodzaj, cel uzyskania oraz czas, w którym zostały uzyskane.

Ustawy pragmatyczne służb podległych ministrowi właściwemu do spraw wewnętrznych różnicują dwie kategorie uzyskiwania danych: dane określone w art. 20c i dane, o których mowa w art. 20cb ustawy *o Policji*, oraz odpowiednio w art. 10b i art. 10bb ustawy *o Straży Granicznej*, a także w art. 57 i art. 59 ustawy *o Służbie Ochrony Państwa*. Podstawą rozróżnienia sposobu ukształtowania nadzoru nad tymi kategoriami danych stanowi zakres ingerencji w prawa i wolności jednostki. Kontroli sądowej nie przewidziano jedynie w odniesieniu do danych osobowych abonentów (art. 20cb ustawy *o Policji*, art. 10bb ustawy *o Straży Granicznej* oraz art. 59 ustawy *o Służbie Ochrony Państwa*). Dane te podlegają jednak obowiązkowi wprowadzenia do rejestru (co zapewnia ich rozliczalność), jak również pozostałym rygorom związanym z procedurą ich uzyskiwania, wykorzystania i niszczenia, analogicznie jak w odniesieniu do metadanych. Tym samym pozyskane w tym trybie dane, które mają znaczenie dla toczącego się postępowania karnego są przekazywane przez uprawniony organ właściwemu miejscowo lub rzeczowo prokuratorowi. To prokurator podejmuje decyzję o zakresie i sposobie wykorzystania tych danych, sprawując tym samym kontrolę nad ich uzyskiwaniem.

W kontekście postulowanego przez Rzecznika Praw Obywatelskich wprowadzenia obowiązku informowania jednostki o tym, że jej dane zostały pozyskane przez uprawnione służby należy zasygnalizować, że może to powodować szereg

problemów praktycznych. W celu ustalenia sprawców przestępstw, konieczne jest niejednokrotnie uzyskanie informacji o wszystkich logowaniach w danej stacji BTS, w określonym odcinku czasowym. W powyższym przypadku ustalenie danych osób w celu ich poinformowania wymagałoby pobrania kolejnych danych telekomunikacyjnych. Ustalenia takie mogą być szczególnie skomplikowane np. w przypadku, gdy z danego numeru korzysta inna osoba niż strona umowy o świadczenie usługi telekomunikacyjnej (np. członek rodziny – żona, dziecko).

Biorąc pod uwagę specyfikę uzyskiwania metadanych należy również wskazać na trudności we wdrożeniu postulatu dotyczącego wprowadzenia rozwiązań, które miałyby zapobiegać uzyskaniu informacji objętych tajemnicami zawodowymi, w tym tajemnicą dziennikarską i obrończą. Podkreślenia wymaga bowiem, że dopiero uzyskanie pierwotnych danych, takich jak dane abonenta, może pozwolić na uzyskanie informacji, czy dany przypadek pozyskania metadanych może dotyczyć osoby związanej tajemnicą. Natomiast zasadniczym problemem będzie ustalenie, czy w konkretnym przypadku, bez dostępu do treści komunikatu, będzie można określić, że dane pozyskane w trybie art. 20c i art. 20cb ustawy *o Policji*, art. 10b i art. 10bb ustawy *o Straży Granicznej* oraz art. 57 i art. 59 ustawy *o Służbie Ochrony Państwa* są objęte tajemnicą. Sam kontakt z określoną osobą nie jest bowiem równoznaczny z pozyskaniem materiałów zawierających tajemnice prawnie chronione.

Z informacji przekazanych przez podległe służby wynika, że rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1543 z dnia 12 lipca 2023 r. *w sprawie europejskich nakazów wydawania i europejskich nakazów zabezpieczania dowodów elektronicznych w postępowaniu karnym oraz w postępowaniu karnym wykonawczym w związku z wykonaniem kar pobawienia wolności*[5] nie będzie wywierało wpływu na obowiązujący model retencji metadanych.

Niezależnie od powyższego uprzejmie informuję, że po zakończeniu prac nad projektem ustawy o zmianie niektórych ustaw w celu wzmocnienia nadzoru sądowego nad kontrolą operacyjną w MSWiA, we współpracy z podległymi służbami, zostaną podjęte prace koncepcyjne nad kierunkami ewentualnych zmian w ustawach pragmatycznych w zakresie pozyskiwania danych telekomunikacyjnych, pocztowych i internetowych w sposób gwarantujący ochronę praw podstawowych jednostki, przy jednoczesnym zapewnieniu służbom narzędzi niezbędnych do skutecznego zapobiegania i zwalczania przestępczości.

Z poważaniem

z up. Czesław Mroczek
Sekretarz Stanu
Ministerstwo Spraw Wewnętrznych i Administracji
(podpisano kwalifikowanym podpisem elektronicznym)

[5] Dz. Urz. UE. L Nr 191, str. 118.