



Minister – Członek Rady Ministrów Koordynator Służb Specjalnych

Tomasz Siemoniak

DKSS.WP.416.1.2026

Warszawa, 07 lipca 2026 r.

Pan
Marcin Wiącek
Rzecznik Praw Obywatelskich

Szanowny Panie Rzeczniku,

odpowiadając na pismo z dnia 7 kwietnia 2026 r. o sygn. II.519.1068.2022.DC zawierające, zgodnie z art. 16 ust. 2 pkt 1 ustawy z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich, prośbę o dokonanie analizy wskazanych w przekazanym piśmie problemów i rozważenie zainicjowania w związku z tym zmian legislacyjnych w Kodeksie postępowania karnego oraz w następujących ustawach: Prawo komunikacji elektronicznej, o Policji, o Straży Granicznej, o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu, o Centralnym Biurze Antykorupcyjnym, o Służbie Wywiadu Wojskowego i Służbie Kontrwywiadu Wojskowego, o Krajowej Administracji Skarbowej, o Żandarmerii Wojskowej oraz o Służbie Ochrony Państwa, przekazuję następujące stanowisko.

W ślad za pismem z dnia 6 października 2025 r. o sygn. DBN.WP.414.96.2025, pragnę podkreślić, że działania mające na celu zmianę funkcjonowania służb specjalnych w obszarach działań jakimi są kontrola operacyjna oraz wykorzystywanie danych niestanowiących treści komunikatu elektronicznego, podlegają permanentnej ocenie prawnej, w tym w zakresie ich zgodności z тезami Europejskiego Trybunału Praw Człowieka (dalej „ETPCz”) wyrażonymi w wyroku ws. *Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce* (skargi 72038/17 i 25237/18). Skutkiem przeprowadzania tej oceny są zaś systematycznie realizowane działania zmierzające do zmiany reżimu prawnego w omawianym zakresie.

W tym miejscu należy zaznaczyć, że przedmiotowa problematyka obejmująca obszary wskazane w przywołanym orzeczeniu ETPCz, dotycząca wprowadzenia zmian w obszarze dokumentowania kontroli operacyjnej realizowanej przez służby specjalne, w szczególności wzory wniosków do właściwego sądu o zarządzenie kontroli operacyjnej, została już uregulowana w rozporządzeniach Prezesa Rady Ministrów:

- z dnia 12 grudnia 2024 r. zmieniającym rozporządzenie w sprawie sposobu dokumentowania prowadzonej przez Agencję Bezpieczeństwa Wewnętrznego kontroli operacyjnej oraz przechowywania i przekazywania wniosków i zarządzeń, a także przechowywania, przekazywania, przetwarzania i niszczenia materiałów uzyskanych podczas stosowania tej kontroli (Dz.U. 2024 r. poz. 1845),
- z dnia 12 grudnia 2024 r. zmieniającym rozporządzenie w sprawie sposobu dokumentowania prowadzonej przez Centralne Biuro Antykorupcyjne kontroli operacyjnej, przechowywania i przekazywania wniosków, postanowień i zarządzeń oraz przechowywania, przekazywania, przetwarzania i niszczenia materiałów uzyskanych podczas stosowania tej kontroli (Dz.U. 2024 r. poz. 1850),
- z dnia 12 grudnia 2024 r. zmieniającym rozporządzenie w sprawie sposobu dokumentowania kontroli operacyjnej prowadzonej przez Służbę Kontrwywiadu Wojskowego oraz

przechowywania i przekazywania wniosków i zarządzeń, przechowywania, przekazywania oraz przetwarzania i niszczenia materiałów uzyskanych podczas prowadzenia tej kontroli, a także wzorów druków i rejestrów (Dz.U. 2024 r. poz. 1843).

Istota zmian, wpisująca się kwestie będące przedmiotem analizy ETPCz, wynikająca z ww. aktów prawnych została omówiona we wspomnianym piśmie z dnia 6 października 2025 r.

Jednocześnie pragnę wskazać, że zainicjowane przez Ministra Koordynatora Służb Specjalnych zostały zmiany ustawowe, obejmujące szereg ustaw pragmatycznych służb państwowych uprawnionych do stosowania kontroli operacyjną, skonsolidowane w rządowym projekcie ustawy *o zmianie niektórych ustaw w celu wzmocnienia nadzoru sądowego nad kontrolą operacyjną* (druk nr 2411); projekt jest obecnie rozpatrywany przez Sejm Rzeczypospolitej Polskiej. Wyjaśnienie istoty proponowanych zmian, a w szczególności ich wpływu na wzmocnienie nadzoru sądowego nad kontrolą operacyjną i realizację standardów ochrony praw człowieka, oraz przedstawienie obowiązujących ram prawnych w tym zakresie, zostało dokonane we wcześniejszej korespondencji.

Jak wynika z powyższego, zagadnienia poruszone przez ETPCz w wyroku *Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce* (skargi 72038/17 i 25237/18) są elementem permanentnej analizy, która musi uwzględniać zachowanie prawidłowej równowagi pomiędzy prawem do prywatności jednostki a bezpieczeństwem narodowym bezpośrednio wpływającym na bezpieczeństwo, życie i zdrowie obywateli Rzeczypospolitej Polskiej.

Jednocześnie odnosząc się do pisma Ministra Sprawiedliwości z dnia 13 kwietnia 2026 r. o sygn. DPK-I.053.10.2026, pragnę potwierdzić fakt pozostawania w kontakcie z Ministrem Sprawiedliwości oraz Ministrem Spraw Wewnętrznych i Administracji, w celu opracowania koniecznych zmian w obowiązujących aktach prawnych.

Jednocześnie ponownie wskazuję, że prowadzone prace muszą odpowiadać realiom współczesnych zagrożeń. Opracowywane zmiany, szanując prawa i swobody obywatelskie, powinny umożliwiać państwu skuteczne przeciwdziałanie i reakcję, także na zagrożenia o większej skali i intensywności. Jest to zagadnienie merytoryczne o wysokim stopniu skomplikowania i wymaga prowadzenia prac we współpracy ze wszystkimi zainteresowanym stronami oraz w tempie właściwym dla charakteru i wagi analizowanego zagadnienia, które nabiera nowego wymiaru w aktualnie istniejącej sytuacji geopolitycznej, podlegającej istotnym zmianom rodzącym poważne zagrożenia, w tym zagrożenia o charakterze międzynarodowym, które mogą bezpośrednio jak i pośrednio wpływać na bezpieczeństwo narodowe Rzeczypospolitej Polskiej.

Jednocześnie pragnę wskazać, że w myśl art. 4 ust. 2 Traktatu o Unii Europejskiej do wyłącznej kompetencji każdego z państw członkowskich należy kwestia bezpieczeństwa narodowego. Istotnym uzupełnieniem powyższego wyłączenia jest zasada kompetencji wyrażona w art. 5 Traktatu stanowiąca, że kompetencje nieprzyznane Unii należą do państw członkowskich.

Z uwagi zatem na wyłączenie bezpieczeństwa narodowego spod bezpośredniej regulacji prawa wspólnotowego należy stwierdzić, że przepisy wprowadzające w życie postanowienia wyroku ETPC powinny uwzględniać fakt, iż spektrum działania służb, którego ten wyrok dotyczy, jest bardzo zróżnicowane. Wprowadzane zatem regulacje nie mogą być absolutnie jednolite i powinny uwzględniać realizację przez niektóre z uprawnionych służb zadań o szczególnie istotnym znaczeniu dla bezpieczeństwa i obronności państwa.

Wzmocnieniem prezentowanego stanowiska jest także art. 8 ust. 2 Europejskiej

Konwencji Praw Człowieka, który umożliwia ingerencję organów władzy w prawo do prywatności, pod pewnymi wszakże warunkami. Wśród przesłanek wymienionych w tym przepisie jest działanie na podstawie prawa oraz wymóg osiągnięcia publicznego (nadrzędnego) celu jakim jest bezpieczeństwo narodowe, porządek publiczny lub ochrona praw innych osób.

Zatem postanowienia art. 4 ust. 2 Traktatu o Unii oraz 8 ust. 2 Europejskiej Konwencji Praw Człowieka dają podstawę do opracowania przepisów krajowych wyłączających służby specjalne lub przynajmniej ograniczających zakres zmian wprowadzanych w wyniku implementacji wyroku ETPCz.

Należy z całą stanowczością stwierdzić, że zadania realizowane przez służby specjalne należą do obszaru ochrony bezpieczeństwa narodowego. Wprawdzie w prawie wspólnotowym jak i krajowym nie ma legalnej definicji terminu bezpieczeństwa narodowego, jednakże realizacja zadań polegających na zapewnieniu bezpieczeństwa narodowego, a także zwalczaniu zagrożeń godzących w porządek konstytucyjny państwa, jego suwerenność, niepodległość i nienaruszalność terytorium, przesądza o tym, że można je zaliczyć do tej kategorii spraw. W tym miejscu należy wskazać, że zwalczanie działalności godzącej w interesy ekonomiczne państwa służy zapewnieniu bezpieczeństwa narodowego, w szczególności w aspekcie ochrony ekonomicznej. Centralne Biuro Antykorupcyjne realizujące ww. obowiązek stanowi wyspecjalizowaną służbę specjalną dedykowaną do przeciwdziałania przestępczości negatywnie wpływającej na bezpieczeństwo ekonomiczne Polski, które jest integralną częścią systemu bezpieczeństwa narodowego. Przestępczość godząca w interesy ekonomiczne państwa prowadzi do zachwiania stabilności systemu gospodarczego, a w konsekwencji do destabilizacji kraju i zwiększenia jego podatności na wpływy zewnętrzne, co wprost zagraża suwerenności państwa. Oznacza to, że działalność CBA mieści się w zakresie pojęcia *bezpieczeństwa narodowego*, które należy rozumieć szeroko, poprzez uwzględnianie w nim w szczególności bezpieczeństwa ekonomicznego państwa, będącego bazą zachowania przez nie zdolności obronnych.

W dalszej kolejności należy wskazać na rolę służb specjalnych w państwie. Dostęp do danych retencyjnych przez wyspecjalizowane organy rządowe, jakimi są służby specjalne, stanowi fundamentalne narzędzie umożliwiające skuteczną realizację naczelných zadań, takich jak rozpoznawanie, zapobieganie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny, a także bezpieczeństwo obywateli.

Realizacja ww. celów przez służby specjalne uwzględnia m. in. konieczność pozyskiwania danych retencyjnych w toku ściśle określonych prawnie procedur, których przestrzeganie podlega nadzorowi.

Przepis art. 47 ustawy - *Prawo komunikacji elektronicznej* (dalej „PKE”) nakłada na przedsiębiorcę telekomunikacyjnego obowiązek zatrzymywania i przechowywania określonych danych generowanych w publicznej sieci telekomunikacyjnej lub przez niego przetwarzanych na terytorium Rzeczypospolitej Polskiej. Retencja danych służy w szczególności wykrywaniu przestępstw skierowanych przeciwko obronności, bezpieczeństwu państwa, bezpieczeństwu i porządkowi publicznemu oraz przestępstw skarbowych. Przepis art. 49 ust. 1 PKE wymienia dane, które powinny być zatrzymywane i przechowywane przez okres 12 miesięcy, przy czym okres ten liczy się od dnia połączenia lub nieudanej próby połączenia. Następnie dane te należy zniszczyć z dniem upływu tego okresu,

z wyjątkiem tych, które zostały zabezpieczone zgodnie z przepisami odrębnymi¹.

Dane, o których mowa w art. 49 ust. 1 PKE, są udostępniane podmiotom uprawnionym, w trybie określonym w poszczególnych pragmatykach służbowych, tzn. na podstawie przepisów o randze ustawy.

Dopuszczalność występowania o udostępnienie danych telekomunikacyjnych wymaga łącznego spełnienia dwóch przesłanek:

1. dane muszą wiązać się z zadaniami ustawowymi służb specjalnych, realizowanymi w zakresie ich właściwości oraz
2. muszą mieć charakter niezbędny.

Decyzja o ich pozyskaniu powinna być podejmowana z zachowaniem wymogu konieczności, a w konsekwencji także zasady proporcjonalności i subsydiarności². Ponadto ustawodawca przewidział kontrolę nad uzyskiwaniem przez służby specjalne danych retencyjnych, którą sprawuje niezależny i niezawisły sąd. W ramach przedmiotowej kontroli szef właściwej służby specjalnej przekazuje w okresach półrocznych, z zachowaniem przepisów o ochronie informacji niejawnych, ww. sądowi sprawozdanie obejmujące:

1. liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych, pocztowych lub internetowych,
2. rodzaj tych danych oraz
3. kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne, pocztowe lub internetowe.

Co więcej, ww. sąd może zapoznać się z materiałami uzasadniającymi udostępnienie służbom specjalnym tych danych. W efekcie obowiązujące krajowe przepisy prawa dotyczące korzystania przez służby specjalne z danych retencyjnych zawierają liczne normy o charakterze gwarancyjnym, mające na celu zapobieżenie ewentualnym nadużyciom władzy. Zatem ww. uregulowania krajowe przewidują materialne i proceduralne warunki regulujące dostęp odpowiednich organów władz państwowych do przechowywanych danych, które jest oparte na obiektywnych kryteriach umożliwiających określenie okoliczności i warunków przyznania dostępu właściwym organom władz krajowych do danych abonentów lub zarejestrowanych użytkowników. W tym względzie, biorąc pod uwagę cel polegający m.in. na zwalczaniu poważnej przestępczości, dostęp ten jest przyznany w odniesieniu do danych dotyczących osób już podejrzewanych o planowanie, popełnianie lub popełnienie poważnego przestępstwa bądź zaangażowanych w inny sposób w takie przestępstwo. Ponadto został spełniony obowiązek zachowania kryterium proporcjonalności, w szczególności w odniesieniu do kategorii danych i okresu ich zatrzymywania przy ich wykorzystywaniu wyłącznie do zwalczania najpoważniejszej przestępczości zgodnie z ustawowo określonym katalogiem. Jednocześnie służby specjalne uzyskują dane retencyjne tylko za okres niezbędny i przydatny do oceny dowodowej danego przestępstwa.

Wskutek powyższego, w przypadku retencji danych, o której mowa w art. 47 PKE, w polskim ustawodawstwie zachowane są zasady konieczności i proporcjonalności także w odniesieniu do zatrzymywania danych o ruchu oraz danych o lokalizacji. Wskazuje na to ustawowa regulacja wprowadzona w tym zakresie w ustawach kompetencyjnych

¹ M. Rogalski [w:] K. Kawałek, W. Krupa, M. Wach, M. Rogalski, *Prawo komunikacji elektronicznej. Komentarz*, Warszawa 2025, art. 47.

² Wyrok Sądu Apelacyjnego w Warszawie z dnia 6 kwietnia 2013 r., sygn. I ACa 1002/12.

uprawnionych podmiotów. Należy zauważyć, że obowiązek zatrzymywania danych, o którym mowa w art. 47 PKE, następuje w sposób prewencyjny, uogólniony i nieodróżniony, ale tylko w celu zapewnienia ochrony bezpieczeństwa narodowego, zwalczania przestępczości i ochrony bezpieczeństwa publicznego. Omawiany przepis powinien być więc odczytywany zawsze przez pryzmat przepisów kompetencyjnych organów uprawnionych do uzyskiwania danych retencyjnych. Retencja danych ma na celu zabezpieczenie samej możliwości przyszłego pozyskania danych na potrzeby zwalczania najpoważniejszej przestępczości. W momencie powstania obowiązku retencji danych przez przedsiębiorcę telekomunikacyjnego organy ścigania nie mają możliwości jednoznacznego ustalenia danych użytkownika, który właśnie popełnia przestępstwo; tym samym logicznym jest, że nie ma możliwości ograniczenia retencji danych wyłącznie do osób w odniesieniu do których trwa, przykładowo, postępowanie karne. Ustawodawca przewidział przy tym jednolity, dwunastomiesięczny okres retencji danych, ustawowo określając maksymalny (nieprzekraczalny) okres ewentualnego ograniczenia prawa do prywatności jednostki, co jest kolejną gwarancją ochrony jej praw.

Jednocześnie należy wskazać, że korelacja między możliwością uzyskiwania danych retencyjnych, a określonym zagrożeniem karą lub szkodliwością czynu pomija funkcję, jaką ma spełniać udostępnienie takich danych. Należy wskazać, że na etapie przedprocesowym podmioty uprawnione nie są powołane do pełnej prawnokarnej oceny czynu zabronionego, lecz przede wszystkim dokonują ustaleń faktycznych oraz gromadzą materiał dowodowy. Ostateczna ocena szkodliwości społecznej czynu oraz jego kwalifikacja prawna, od której uzależnione jest zagrożenie karą, uwidaczniane są co najmniej na etapie postanawiania o wszczęciu postępowania przygotowawczego oraz na dalszych etapach procesu karnego (postanawianie o przedstawieniu zarzutów, akt oskarżenia, wyrok), które znajdują się poza kompetencjami podmiotów uprawnionych do korzystania retencji danych. W tym miejscu warto zaznaczyć, że cechą charakterystyczną przestępczości korupcyjnej lub mającej na celu zakłócenie przetargu jest ścisła solidarność między sprawcami, w wyniku której wykrycie czynu zabronionego innymi środkami jest często niemożliwe, tym bardziej że tego rodzaju czyny nie manifestują swoich cech w zewnętrznym odbiorze, tak jak ma to miejsce np. przy przestępczości przeciwko zdrowiu lub życiu. Powyższe utrudnia uzyskanie wiedzy na temat samego przestępstwa, w tym także od innych osób.

Tym samym postulowany przez Pana Rzecznika kazuistyczny charakter regulacji dotyczących pozyskiwania danych retencyjnych może budzić wątpliwości co do jego adekwatności względem rzeczywistej ingerencyjności tej metody. Należy mieć na uwadze, że na etapie działań operacyjnych proponowane regulacje mogą doprowadzić do trudności związanych z subsumpcją, tj. zakwalifikowaniem rozpoznawanego zagrożenia i w konsekwencji zidentyfikowania odpowiednich przepisów w zakresie ochrony danych, które będą miały zastosowanie. Jednocześnie wejście w życie postulowanych zmian w fazie procesu karnego doprowadzi do nadmiernego sformalizowania już rozbudowanej regulacyjnie procedury karnej. Co więcej, przedstawione propozycje Pana Rzecznika nie uwzględniają potrzeby wprowadzenia rozwiązań organizacyjnych związanych ze zwiększeniem obsady kadrowej zarówno w służbach policyjnych i specjalnych, jak też w sądach w związku z pozyskiwanymi danymi retencyjnymi, co będzie skutkowało utrudnieniami w wykonywaniu ustawowych czynności służb, a także sądownictwa.

Krytycznie należy ustosunkować się także do propozycji usunięcia z ustaw policyjnych oraz kompetencyjnych służb specjalnych przepisów dotyczących możliwości

uzyskiwania danych retencyjnych bez zgody sądu. Takie działanie byłoby nadinterpretacją wyroków TSUE w tej materii. Należy zasygnalizować, że wskazanie przez TSUE na wprowadzenie tych samych gwarancji w zakresie retencji danych, jakie przepisy krajowe przewidują dla kontroli operacyjnej, nie oznacza jednak całkowitego pozbawienia podmiotów uprawnionych możliwości uzyskiwania tych danych lub konieczności uzyskiwania każdorazowej zgody sądu, co *de facto* przerzuciłoby na sąd ciężar podejmowania decyzji w tym obszarze, poprzedzonej wcześniejszym zbadaniem podstaw prawnych i faktycznych. Propozycja ta tym samym pomija kwestię ekonomiki procesowej oraz zdarzeń, w których wymagana jest od podmiotów uprawnionych dynamika oraz sprawność prowadzonych czynności.

Należy uznać za niezasadną propozycję zwiększenia ochrony tajemnic prawnie chronionych w obszarze retencji danych. Retencja danych, w tym danych o lokalizacji, nie ujawnia podmiotom uprawnionym treści komunikatów elektronicznych, a wyłącznie położenie urządzenia końcowego abonenta; ponadto dysponenti tajemnic nie są wyłączeni spod możliwości stosowania wobec nich uprawnień nadanych w ustawach kompetencyjnych podmiotom uprawnionym. Warto zasygnalizować, że nie każda aktywność osób wykonujących określony zawód, na podstawie ustawy przewidującej określoną tajemnicę zawodową, determinuje jej powstanie, a co więcej, potencjalna działalność przestępcza danego dysponenta tajemnicy może w ogóle nie wiązać się z wykonywaniem przez niego określonego zawodu. W konsekwencji należy podkreślić, że kolejne ograniczenia w zakresie ochrony tajemnic prawnie chronionych uniemożliwią uzyskiwanie danych retencyjnych wyłącznie z istnienia samego faktu, że abonent może być dysponentem tajemnicy prawnie chronionej, co w efekcie nada tej grupie osób *quasi* immunitet przed stosowaniem przewidzianych w ustawie uprawnień podmiotów uprawnionych.

W zakresie propozycji informowania osoby o uzyskiwaniu danych retencyjnych przez podmioty uprawnione należy wskazać, że sama informacja nie wprowadza dla tej osoby wymiernych uprawnień, tzn. nie stwarza możliwości dostępu do źródłowych materiałów, np. materiałów pracy operacyjnej stanowiących podstawę faktyczną do uzyskiwania takich danych. Informowanie osób o uzyskiwaniu danych retencyjnych jest również sprzeczne ze wspomnianą funkcją wykrywczą, np. czynności operacyjno-rozpoznawczych. Należy zauważyć, że przekazanie takiej informacji może doprowadzić do ujawnienia samego faktu prowadzenia czynności przez służby specjalne, np. wśród określonych zorganizowanych środowisk przestępczych lub o charakterze terrorystycznym czy też szpiegowskim. Jest to wprost sprzeczne z niejawnym charakterem czynności operacyjno-rozpoznawczych oraz koniecznością ich maskowania, mogąc prowadzić do dekonspiracji realizowanych działań, ale przede wszystkim generując zagrożenia dla życia i zdrowia nie tylko funkcjonariuszy, ale także osób udzielających im pomocy przy realizacji czynności operacyjno-rozpoznawczych oraz potencjalnie osób trzecich.

Konkludując należy zaznaczyć, że fundamentalne kwestionowanie zasadności pozyskiwania i przechowywania danych retencyjnych, z uwagi na rosnące zagrożenie w obszarze granic Rzeczypospolitej Polskiej z Federacją Rosyjską i Republiką Białorusi oraz uwzględniając obecną sytuację geopolityczną na Bliskim Wschodzie, której przejawem jest intensyfikacja działań dywersyjno-sabotażowych, będzie wiązało się z ograniczeniem działalności służb specjalnych, w tym w zakresie pozyskiwania i przetwarzania danych retencyjnych, co może stanowić istotne zagrożenia dla bezpieczeństwa państwa.

Wspomniana bezprecedensowa eskalacja działań obcych służb specjalnych ma również wpływ na stan przestępczości w Polsce, co wynika z dużego napływu w ostatnich latach obywateli byłych republik radzieckich, z których wielu powiązanych jest z funkcjonującymi na ww. obszarach strukturami przestępczości zorganizowanej. W związku z tym aktualna sytuacja geopolityczna wymaga radykalnego wzmocnienia i usprawniania pracy polskich służb specjalnych i policyjnych, a nie znaczącego ograniczania możliwości ich skutecznego działania.

Z wyrazami szacunku

Tomasz Siemoniak
Minister - Członek Rady Ministrów,
Koordynator Służb Specjalnych
/dokument podpisany elektronicznie/