Minister
Spraw Wewnętrznych
i Administracji

BMP-0790-4-2/2022/MSi

Pan
Marcin Wiącek
Rzecznik Praw Obywatelskich

Szanowny Panie Rzeczniku,

w odpowiedzi na Pana wystąpienia z 13 stycznia 2022 r. (sygn. VII.501.306.2021.KZ) oraz 13 lipca 2022 r. (sygn. VII.501.306.2021.KSZ) *w sprawie zgodności przepisów regulujących zakres czynności operacyjno-rozpoznawczych prowadzonych wobec osób podejrzanych o naruszenie prawa ze standardami określonymi w orzecznictwie Trybunału Konstytucyjnego, Europejskiego Trybunału Praw Człowieka oraz Trybunału Sprawiedliwości Unii Europejskiej*[1], uprzejmie przedstawiam[2], co następuje.

Obowiązujący obecnie model stosowania metod pracy operacyjnej, takich jak kontrola operacyjna czy uzyskiwanie danych telekomunikacyjnych, został wypracowany w wyniku wdrożenia do polskiego porządku prawnego wyroku Trybunału Konstytucyjnego sygn. K 23/11 z dnia 30 lipca 2014 r.[3], która przyjęła formę ustawy z dnia 15 stycznia 2016 r. *o zmianie ustawy o Policji oraz niektórych innych ustaw*[4].

W obecnym stanie prawnym uprawnienia do prowadzenia kontroli operacyjnej w ramach czynności operacyjno-rozpoznawczych przysługują określonej grupie podmiotów[5], którym ustawodawca przypisał obowiązek prowadzenia działań na rzecz szeroko pojętego bezpieczeństwa i porządku publicznego oraz bezpieczeństwa państwa. Uregulowania określające przesłanki, tryb i zasady zarządzania oraz sposób postępowania z materiałami uzyskanymi podczas stosowania kontroli operacyjnej znalazły swoje odzwierciedlenie w ustawach pragmatycznych poszczególnych podmiotów uprawnionych. Kontrolę operacyjną prowadzić mogą zatem:

- Policja, na podstawie art. 19 ustawy z dnia 6 kwietnia 1990 r. *o Policji*[6]*;*
- Straż Graniczna (SG), na podstawie art. 9e ustawy z dnia 12 października 1990 r. *o Straży Granicznej*[7]*;*
- Biuro Nadzoru Wewnętrznego, na podstawie art. 11n ustawy z dnia 21 czerwca 1996 r. *o szczególnych formach sprawowania nadzoru przez ministra właściwego do spraw wewnętrznych*[8]*;*
- Żandarmeria Wojskowa, na podstawie art. 31 ustawy z dnia 24 sierpnia 2001 r. *o Żandarmerii Wojskowej i wojskowych organach porządkowych*[9]*;*
- Agencja Bezpieczeństwa Wewnętrznego (ABW), na podstawie art. 27 ustawy z dnia 24 maja 2002 r. *o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*[10]*;*
- Służba Kontrwywiadu Wojskowego (SKW), na podstawie art. 31 ustawy z dnia 9 czerwca 2006 r. *o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego*[11]*;*
- Centralne Biuro Antykorupcyjne, na podstawie art. 17 ustawy z dnia 9 czerwca 2006 r. *o Centralnym Biurze Antykorupcyjnym*[12]*;*

[1] Przekazane przy pismach Pana Michała Dworczyka, Ministra-Członka Rady Ministrów w Kancelarii Prezesa Rady Ministrów, sygn. BPRM.5090.2.1.2022(2)TI oraz BPRM.5090.2.1.2022(4)TI.
[2] W oparciu m.in. o stanowiska Ministra Obrony Narodowej, Szefa Krajowej Administracji Skarbowej, Prokuratury Krajowej oraz Dyrektora Departamentu Bezpieczeństwa Narodowego w Kancelarii Prezesa Rady Ministrów.
[3] Zwanego dalej: „wyrokiem TK z 2014 r.".
[4] Dz. U. poz. 147.
[5] Zwanych dalej: „podmiotami uprawnionymi".
[6] Dz. U. z 2021 r. poz. 1882, z późn. zm.
[7] Dz. U. z 2022 r. poz. 1061, z późn. zm.
[8] Dz. U. z 2021 r. poz. 2073, z późn. zm.
[9] Dz. U. z 2021 r. poz. 1214, z późn. zm.
[10] Dz. U. z 2022 r. poz. 557.
[11] Dz. U. z 2022 r. poz. 502, z późn. zm.
[12] Dz. U. z 2021 r. poz. 1671, z późn. zm.

ul. Stefana Batorego 5
02-591 Warszawa, Polska
mswia.gov.pl
tel. +48 222 500 112
fax +48 22 601 39 88

- Krajowa Administracja Skarbowa, na podstawie art. 118 ustawy z dnia 16 listopada 2016 r. *o Krajowej Administracji Skarbowej*[13]*;*
- Służba Ochrony Państwa, na podstawie art. 42-55 ustawy z dnia 8 grudnia 2017 r. *o Służbie Ochrony Państwa*[14]*.*

Z kolei sposób dokumentowania prowadzonej kontroli operacyjnej, przechowywania i przekazywania wniosków, zarządzeń i materiałów uzyskanych podczas stosowania tej kontroli, a także przetwarzania i niszczenia tych materiałów został uregulowany w aktach wykonawczych wydanych na postawie powyższych ustaw – odpowiednio w:

- rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 8 lipca 2022 r. *w sprawie kontroli operacyjnej prowadzonej przez Policję*[15]*;*
- rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 25 sierpnia 2011 r. *w sprawie sposobu dokumentowania prowadzonej przez Straż Graniczną kontroli operacyjnej oraz przechowywania i przekazywania wniosków i zarządzeń, a także przechowywania, przekazywania oraz przetwarzania i niszczenia materiałów uzyskanych podczas stosowania tej kontroli*[16]*;*
- rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 14 września 2018 r. *w sprawie sposobu dokumentowania kontroli operacyjnej prowadzonej przez Biuro Nadzoru Wewnętrznego*[17]*;*
- rozporządzeniu Ministra Obrony Narodowej z dnia 23 kwietnia 2018 r. *w sprawie sposobu dokumentowania kontroli operacyjnej przez Żandarmerię Wojskową*[18]*;*
- rozporządzeniu Prezesa Rady Ministrów z dnia 30 lipca 2013 r. *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*[19]*;*
- rozporządzeniu Prezesa Rady Ministrów z dnia 27 września 2006 r. *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*[20]*;*
- rozporządzeniu Prezesa Rady Ministrów z dnia 25 października 2011 r. *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*[21]*;*
- rozporządzeniu Ministra Rozwoju i Finansów z dnia 13 kwietnia 2017 r. *w sprawie dokumentowania kontroli operacyjnej prowadzonej przez Krajową Administrację Skarbową*[22]*;*
- rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 9 października 2018 r. *w sprawie sposobu dokumentowania kontroli operacyjnej prowadzonej przez Służbę Ochrony Państwa*[23]*.*

W dotychczasowym orzecznictwie TK kilkakrotnie wypowiadał się w sprawie konstytucyjności przepisów regulujących czynności operacyjno-rozpoznawcze prowadzące do ingerencji w sferę prywatności jednostek i tajemnicę komunikowania się. Trybunał Konstytucyjny nie podważył dopuszczalności ich stosowania w demokratycznym państwie prawa. Przeciwnie, wyraźnie podkreślił, że niejawne pozyskiwanie przez organy władzy publicznej informacji o obywatelach, w toku kontroli operacyjnej ukierunkowanej na zapobieganie przestępstwom, ich wykrywanie oraz zwalczanie, jest nieodzowne. Jawność tych czynności powodowałaby bowiem ich nieskuteczność, a to z kolei rzutowałoby na poziom bezpieczeństwa państwa i jego obywateli. Ocena ta wynikała z dostrzeżenia specyfiki działalności przestępczej i coraz trudniejszych warunków zapewnienia bezpieczeństwa spowodowanych zagrożeniem terroryzmem, zorganizowaną przestępczością czy wykorzystywaniem przez przestępców nowych technologii w celu komunikowania się.

[13] Dz. U. z 2022 r. poz. 813, z późn. zm., zwanej dalej: „ustawą o KAS".
[14] Dz. U. z 2021 r. poz. 575, z późn. zm.
[15] Dz. U. poz. 1458.
[16] Dz. U. poz. 1190 i z 2018 r. poz. 372.
[17] Dz. U. poz. 1888.
[18] Dz. U. poz. 1035.
[19] Dz. U. poz. 1048, z późn. zm.
[20] Dz. U. z 2019 r. poz. 1768.
[21] Dz. U. Nr 232, poz. 1379.
[22] Dz. U. poz. 828.
[23] Dz. U. poz. 2065.

Prokuratura Krajowa stwierdziła, że co do zasady należy zgodzić się z argumentami przedstawionymi w piśmie Pana Rzecznika dla poparcia tezy, że działalność podmiotów uprawnionych polegająca na niejawnym wykonywaniu czynności operacyjnej, jakkolwiek być może lepszym byłoby użycie sformułowania „czynności wywiadowczych", pozostaje w konflikcie z określonymi w Konstytucji RP gwarancjami obywatelskimi, takimi jak prawo do prywatności, wolność komunikowania się i prawo do zachowania w tajemnicy faktu komunikowania oraz wymienianych treści. Analiza przytoczonych w piśmie Pana Rzecznika argumentów prowadzi jednak do wniosku, że wymogi, jakie zostały określone, aby prawo regulujące zagadnienie czynności operacyjno-rozpoznawczych, a w szczególności kontroli operacyjnej, mogło być uznane za zgodne z Konstytucją RP, zostały w polskim prawodawstwie zrealizowane albo ich zrealizowanie, biorąc pod uwagę cel regulacji, nie jest możliwe.

Dyrektor Departamentu Bezpieczeństwa Narodowego w Kancelarii Prezesa Rady Ministrów (DBN w KPRM) zwrócił uwagę, że nie ma innej czynności operacyjno-rozpoznawczej, której zakres i tryb wykonywania byłby uregulowany tak obszernie, jak w przypadku kontroli operacyjnej, a także która podlegałaby tak ścisłemu i skrupulatnemu nadzorowi ze strony zewnętrznych wobec służb, niezależnych organów. Ma to na celu maksymalizację ochrony praw i wolności obywateli w toku wykonywania tej czynności przez uprawnione do jej stosowania służby państwowe. Kontrola operacyjna jest niewątpliwie szczególną czynnością w pracy operacyjnej, silnie ingerującą w fundamentalne prawa i wolności obywatelskie uregulowane przede wszystkim w art. 47, 49 i 51 Konstytucji RP, stąd właśnie potrzeba jej ustawowego określenia. Ustawowe regulacje w konsekwencji konieczności ww. dostosowania są znaczne rozbudowane; przepisy te w sposób wyczerpujący normują kontrolę operacyjną i najważniejsze kwestie związane z jej stosowaniem.

Dyrektor DBN w KPRM zauważył, że skutkiem ustawy z dnia 15 stycznia 2016 r. *o zmianie ustawy o Policji oraz niektórych innych ustaw* było m.in. rozbudowane i precyzyjne wskazanie na czym polega kontrola operacyjna, *de facto* było to zdefiniowanie tej metody pracy operacyjnej. Przepisy te, stosownie do podniesionych przez TK wymogów konstytucyjnych, precyzują dopuszczalność, warunki i granice niejawnego wkroczenia w sferę prywatności jednostki. Równocześnie kontrola operacyjna w takiej postaci pozwala na uzyskiwanie i utrwalanie szerokiego katalogu informacji, które są w różny sposób przechowywane, przekazywane i wytwarzane – co należy ocenić jako merytorycznie zasadne, mając na uwadze powagę zadań jakie ustawodawca nałożył na służby specjalne. Jest to też wyrazem dostrzeżenia przez ustawodawcę, że w dzisiejszych czasach źródłem informacji istotnych dla rozpoznania, zapobieżenia i wykrywania przestępstw oraz ścigania ich sprawców są nie tylko rozmowy bezpośrednie i telefoniczne prowadzone za pomocą sieci telekomunikacyjnych, ale także inne przekazy danych prowadzone przy wykorzystaniu wielu różnych narzędzi programowych, urządzeń i usług teleinformatycznych.

W opinii Dyrektora DBN w KPRM ustawowy opis kontroli operacyjnej zawarty w ustawach pragmatycznych służb specjalnych czyni zadość wymogom regulacji dotyczącej środka umożliwiającego ingerencję w prawa i wolności konstytucyjne. Wymogi te zostały zdefiniowane w wyroku TK z 2014 r. i przewidują, że ustawa w odniesieniu do kontroli operacyjnej musi określać: 1) kategorie osób, wobec których można stosować kontrolę operacyjną, na podstawie nakazu sądu; 2) rodzaje przestępstw, wobec których można taki nakaz wydać; 3) maksymalną długość czasu kontroli; 4) procedurę informowania o wynikach stosowanego środka; 5) środki gwarantujące przekazanie zapisów w stanie nienaruszonym i w całości umożliwiającym ich skontrolowanie przez sędziego i obronę; 6) określenie przypadków, gdy zapisy mogą lub muszą być zniszczone. Regulacja kontroli operacyjnej zawarta w obowiązujących przepisach spełnia także akcentowany w orzecznictwie TK wymóg subsydiarności, zgodnie z którym kontrola operacyjna jest środkiem o charakterze *ultima ratio* stosowanym tylko, kiedy inne metody okazały się bezskuteczne lub wiadomo, że będą bezskuteczne.

Wśród wielu tez zawartych w uzasadnieniu podnoszonego przez Pana Rzecznika wyroku TK z 2014 r. znalazły się m.in. rozważania wskazujące na potrzebę informowania osoby (jednostki) o podjętych wobec niej działaniach operacyjno-rozpoznawczych. Trybunał Konstytucyjny jednocześnie potwierdził, że w pewnych sytuacjach może być również uzasadnione odstąpienie od wspomnianego obowiązku informacyjnego. Kwestie te pozostawiono jednak do rozstrzygnięcia ustawodawcy.

Ostatecznie kwestia obowiązku informacyjnego nie znalazła się w ustawie z dnia 15 stycznia 2016 r. *o zmianie ustawy o Policji oraz niektórych innych ustaw*. Trzeba bowiem pamiętać, że wprowadzenie takiego obowiązku niesie ze sobą szereg konsekwencji. W szczególności wiązałoby się to z naruszeniem podstawowych zasad, w oparciu o które funkcjonują służby i poważnie mogłoby zaważyć nie tylko na skuteczności ich działań,

ale także mogłoby zagrozić bezpieczeństwu państwa oraz osób, które w sposób niejawny udzielają pomocy służbom. Ponadto wprowadzenie obowiązku informowania pozostawałoby w sprzeczności z ustawowym wymogiem ochrony form i metod czynności operacyjno-rozpoznawczych oraz faktu ich prowadzenia. Należy podkreślić, że argumentacja ta nie traci na ważności także w obliczu wątpliwości podniesionych obecnie przez Pana Rzecznika.

Warto odnotować, że wdrażane przez powyższą nowelizację do polskiego porządku prawnego standardy demokratycznego państwa prawa doprowadziły ostatecznie do takiego ukształtowania przepisów w zakresie kontroli operacyjnej, które stanowi racjonalny kompromis między ochroną prawa do prywatności z jednej strony a zagwarantowaniem narzędzi służących do skutecznego przeciwdziałania i wykrywania przestępczości z drugiej. Egzemplifikacją dokonań w tym zakresie, w obowiązujących obecnie przepisach, spełniających jednocześnie normy konstytucyjne, jest m.in.:

- rygorystyczne określenie przesłanek stosowania kontroli operacyjnej, poprzez wyspecyfikowanie w sposób w miarę możliwości jak najbardziej precyzyjny katalogu przestępstw lub przypadków, kiedy stosowanie takiej kontroli jest dopuszczalne (wcześniejsze uregulowania w tym zakresie pozostawiały szerokie pole do interpretacji);
- określenie rodzajów środków niejawnego pozyskiwania informacji[24];
- przeniesienie z aktów wykonawczych do materii ustawowej regulacji określającej rejestry dokumentacji związanej z jej prowadzeniem[25];
- określenie maksymalnego okresu prowadzenia kontroli operacyjnej (18 miesięcy, z wyjątkiem ABW[26] i SKW[27]);
- określenie zasady postępowania z materiałami, które mogą zawierać informacje objęte tajemnicą zawodową (notarialną, adwokacką, radcy prawnego, doradcy podatkowego, lekarską, dziennikarską)[28] albo są objęte bezwzględnymi zakazami dowodowymi[29].

Dyrektor DBN w KPRM zauważył, że wymóg poinformowania jednostki o podjętych wobec niej działaniach nie wynika wprost z art. 51 Konstytucji RP ani jakiegokolwiek innego przepisu ustawy zasadniczej. Widoczne jest, że TK w swoim rozstrzygnięciu ponad miarę zaostrzył wymogi stawiane w omawianej kwestii przez Europejski Trybunał Praw Człowieka (ETPCz), na orzeczenia którego się powoływał. Trybunał Konstytucyjny w punkcie 2.4.2 wyroku TK z 2014 r. przedstawił standard konwencyjny dotyczący podsłuchów rozmów, a także przechwytywania informacji stanowiących integralny element procesu komunikowania. Wynika z niego, że ETPCz rzeczywiście za jeden z warunków dopuszczalności kontroli rozmów uznaje obowiązek poinformowania osoby, której dane niejawnie pozyskiwano. Równocześnie ETPCz przesądził, czego TK w punkcie 5.2.6. wyroku nie uwzględnia, że poinformowanie jednostki powinno jednak nastąpić w momencie, gdy nie zagrozi to celom kontroli, a nawet zezwala, by w pewnych sytuacjach możliwe było zaniechanie następczego poinformowania.

Według Prokuratury Krajowej nie znajduje uzasadnienia powołanie się Pana Rzecznika na treść art. 51 ust. 3 Konstytucji RP jako podstawy obligującej właściwe organy do powiadomienia obywatela o zastosowaniu wobec niego kontroli operacyjnej czy wręcz prowadzeniu wobec niego czynności operacyjno-rozpoznawczych.

---

[24] Kontrola operacyjna jest prowadzona niejawnie i polega na uzyskiwaniu i utrwalaniu treści: rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą sieci telekomunikacyjnych; obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne; korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej; danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych oraz uzyskiwaniu dostępu i kontroli zawartości przesyłek.

[25] Rejestry postanowień, pisemnych zgód, wniosków i zarządzeń dotyczących kontroli operacyjnej.

[26] Zgodnie z art. 27 ust. 9 ustawy *o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu: w uzasadnionych przypadkach, gdy podczas stosowania kontroli operacyjnej pojawią się nowe okoliczności istotne dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawcy i uzyskania dowodów przestępstwa, sąd, o którym mowa w ust. 2, na pisemny wniosek Szefa ABW, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, może wydawać, również po upływie okresów, o których mowa w ust. 8, kolejne postanowienia o przedłużeniu kontroli operacyjnej na następujące po sobie okresy, z których żaden nie może trwać dłużej niż 12 miesięcy.*

[27] Zgodnie z art. 31 ust. 7 ustawy *o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego: w uzasadnionych przypadkach, gdy podczas stosowania kontroli operacyjnej pojawią się nowe okoliczności istotne dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawcy i uzyskania dowodów przestępstwa, sąd, o którym mowa w ust. 2, na pisemny wniosek Szefa SKW, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, może wydawać, również po upływie okresów, o których mowa w ust. 6, kolejne postanowienia o przedłużeniu kontroli operacyjnej na następujące po sobie okresy, z których żaden nie może trwać dłużej niż 12 miesięcy.*

[28] Wykorzystanie tego rodzaju materiałów jest uzależnione od decyzji sądu.

[29] Podlegają niezwłocznemu zniszczeniu.

Wprawdzie zgodnie z ww. przepisem każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych, to jednak prawo to może zostać ograniczone ustawą. I tak np., stosownie do art. 19 ust. 16 ustawy *o Policji*, osobie, wobec której kontrola operacyjna była stosowana, nie udostępnia się materiałów zgromadzonych podczas trwania tej kontroli.

Prokuratura Krajowa zauważyła, że w swoim wystąpieniu Pan Rzecznik nie wskazał czemu miałby służyć obowiązek informowania osoby objętej kontrolą operacyjną o fakcie jej zastosowania, a jeżeli celem tym miałoby być zbadanie zasadności decyzji sądu wdrażającej kontrolę operacyjną, to nie wskazano jaki miałby być skutek orzeczenia uznającego za niezasadne wdrożenie kontroli. Szukając analogii należy przytoczyć regulacje zawarte np. w art. 246 ustawy z dnia 6 czerwca 1997 r. – *Kodeks postępowania karnego*[30] i rozdziale 58 tej ustawy, uprawniające osobę zatrzymaną do ubiegania się o odszkodowanie i zadośćuczynienie za niewątpliwie niesłuszne zatrzymanie. Trudno w wystąpieniu Pana Rzecznika doszukać się wyjaśnienia tej kwestii. Pan Rzecznik w swoich rozważaniach nie odniósł się także do wpływu ewentualnego kasatoryjnego rozstrzygnięcia sądu odwoławczego na ważność materiałów uzyskanych w toku kontroli operacyjnej, sygnalizując jedynie, że sądy *meriti* nie powinny uwzględniać informacji i dowodów uzyskanych w drodze sprzecznej z prawem Unii Europejskiej (UE) dostępu właściwego organu do danych o ruchu i danych o lokalizacji.

Oprócz wspomnianych wyżej rozwiązań, w obowiązujących obecnie przepisach pragmatycznych dotyczących stosowania kontroli operacyjnej funkcjonują także inne mechanizmy nadzoru i kontroli, które w sposób kompletny i komplementarny zabezpieczają przed nieuprawnionym stosowaniem tej metody uzyskiwania informacji.

W pierwszej kolejności należy wskazać, że wniosek w sprawie zastosowania kontroli operacyjnej wymaga przede wszystkim pisemnej zgody właściwego prokuratora. Przy czym Prokuratura Krajowa podkreśliła, że rolą prokuratora nie jest wyrażanie zgody na zastosowanie kontroli operacyjnej, tylko udzielenie zgody na wystąpienie przez uprawniony organ do sądu z wnioskiem o zarządzenie takiej kontroli. Prokurator dokonuje zatem wstępnej oceny wniosku o zarządzenie kontroli, a w razie braku jego zgody wniosek nie jest kierowany do sądu.

W opinii Prokuratury Krajowej nieporozumieniem jest zgłaszany przez Pana Rzecznika zarzut braku niezależności prokuratury z uwagi na fakt, iż funkcję Prokuratora Generalnego sprawuje Minister Sprawiedliwości. Przypomnieć zatem wypada, że zgodnie z art. 7 § 1 ustawy z dnia 28 stycznia 2016 r. – *Prawo o prokuraturze*[31], prokurator przy wykonywaniu czynności określonych w ustawach jest niezależny. Ograniczenie niezależności prokuratora może nastąpić jedynie na podstawie przepisów tej ustawy.

Umiejscowienie prokuratora w procesie prowadzącym do zarządzenia kontroli operacyjnej nie jest przypadkowe i jest podyktowane w głównej mierze celami, dla których ustawodawca dopuszcza w ogóle stosowanie takiej metody uzyskiwania informacji. Trzeba bowiem pamiętać, że kontrola operacyjna jest podejmowana w celu rozpoznawania, zapobiegania i wykrywania przestępstw oraz uzyskania i utrwalenia dowodów przestępstw określonych odmiennie dla każdego z podmiotów uprawnionych. W efekcie informacje uzyskane podczas stosowania kontroli operacyjnej, o ile będą potwierdzały popełnienie przestępstwa, *de facto* staną się elementem materiału dowodowego w postępowaniu przygotowawczym.

Należy podkreślić, że prokurator – oprócz oceny zasadności wniosku o zarządzenie kontroli operacyjnej – na podstawie art. 57 § 2 ustawy – *Prawo o prokuraturze*, sprawuje także kontrolę nad czynnościami operacyjno-rozpoznawczymi poprzez wgląd w materiały zgromadzone w toku m.in. rzeczonej kontroli operacyjnej. Zakres działań prokuratora w tym zakresie został określony z kolei w § 2 rozporządzenia Ministra Sprawiedliwości z dnia 13 lutego 2017 r. *w sprawie sposobu realizacji czynności prokuratora w ramach kontroli nad czynnościami operacyjno-rozpoznawczymi*[32], zgodnie z którym kontrola prokuratora nad czynnościami operacyjno-rozpoznawczymi określonymi w przepisach, o których mowa w § 1 (w tym nad kontrolą operacyjną), jest sprawowana w szczególności przez badanie faktycznych podstaw tych czynności oraz ich legalności, prawidłowości i efektywności[33].

---

[30] Dz. U. z 2021 r. poz. 534, z późn. zm.

[31] Dz. U. z 2022 r. poz. 1247.

[32] Dz. U. z 2018 r. poz. 626.

[33] W sposób zbliżony kwestia ta była uregulowana w obowiązującym uprzednio rozporządzeniu Ministra Sprawiedliwości z dnia 9 czerwca 2011 r. *w sprawie sposobu realizacji kompetencji prokuratora w zakresie nadzoru nad czynnościami operacyjno-rozpoznawczymi* (Dz. U. Nr 121, poz. 692) – *§ 2. Nadzór prokuratora nad zgodnością z prawem inicjowania i przeprowadzania przez uprawnione organy czynności operacyjno-rozpoznawczych, określonych w przepisach, o których mowa w § 1* [m.in. kontroli

Odnotowania w tym kontekście wymaga, że na podstawie ustawy z dnia 4 lutego 2011 r. *o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw*[34], dla wszystkich podmiotów uprawnionych wprowadzono wymóg przedstawiania wraz z wnioskiem o zastosowanie kontroli operacyjnej także materiałów uzasadniających potrzebę jej zastosowania, co w niebagatelny sposób ułatwia prokuraturze ocenę faktycznych podstaw tych czynności oraz ich legalności, a tym samym gwarantuje, że nie będą one nadużywane. Dodatkowo sam wniosek składa się z ustawowo określonych[35] elementów, wskazujących m.in. na okoliczności uzasadniające potrzebę zastosowania kontroli operacyjnej, w tym stwierdzonej bezskuteczności lub nieprzydatności innych środków.

Powyższy przepis jest skorelowany z odpowiednimi przepisami w ustawach pragmatycznych obligującymi podmioty uprawnione do informowania właściwego prokuratora o wynikach kontroli operacyjnej po jej zakończeniu, a na jego żądanie również o przebiegu tej kontroli.

Dodatkowo należy wskazać, że ustawodawca, co do zasady, przewidział tylko dwie możliwości postępowania z materiałami zgromadzonymi podczas stosowania kontroli operacyjnej:

- przekazanie całości materiałów do prokuratury – w przypadku uzyskania dowodów pozwalających na wszczęcie postępowania karnego lub mających znaczenie dla toczącego się postępowania karnego;
- niezwłoczne, protokolarne, komisyjne zniszczenie – w przypadku gdy nie stanowią one informacji potwierdzających zaistnienie przestępstwa.

Nie można wreszcie zapominać, że z uwagi na przedmiot ingerencji, kontrola operacyjna może być zarządzana w przypadku ograniczonego katalogu przestępstw lub zadań oraz jest zawsze środkiem ostatecznym, stosowanym w sytuacji, gdy inne środki okazały się bezskuteczne albo będą nieprzydatne[36]. Samo zaś zarządzanie kontroli operacyjnej podlega uprzedniej kontroli niezależnego podmiotu, jakim jest sąd, co w połączeniu z uczestnictwem prokuratora w tej procedurze, znacząco podnosi gwarancje legalności działań podejmowanych przez uprawnione podmioty.

Prokuratura Krajowa zwróciła uwagę, że uczestnicy dyskusji, której przedmiotem są działania wywiadowcze uprawnionych organów państwa, ich zakres, tryb prowadzenia, a co najistotniejsze – stopień ingerencji w prawa obywatelskie, zdają się zapominać, że kontrolę operacyjną zarządza sąd, który działa jako organ nadzoru nad Policją i innymi uprawnionymi służbami, a zatem nadzór ten nie ma charakteru następczego. Sąd nie bada zatem czy uprawniony podmiot legalnie i zasadnie prowadził kontrolę, tylko, w oparciu o przedstawione przez wnioskodawcę materiały, decyduje o zastosowaniu kontroli. Rolą sądu jako organu zewnętrznego oraz – co istotne – niezawisłego, nie jest w tym przypadku sprawowanie wymiaru sprawiedliwości, tylko wykonywanie czynności nadzorczych nad działaniami służb, ingerującymi w konstytucyjnie chronione prawa obywatelskie. W takim przypadku nie znajduje zastosowania konstytucyjny standard prawa do zaskarżalności orzeczeń sądowych i dwuinstancyjności, albowiem odnosi się on do postępowań sądowych, a za takie nie sposób uznać procedowanie sądu w przedmiocie zarządzania kontroli operacyjnej.

W tym miejscu należy przytoczyć stanowisko TK wyrażone w wyroku TK z 2014 r., zgodnie z którym *w świetle wyjaśnień otrzymanych od prezesów sądów apelacyjnych liczba sędziów zajmujących się oceną wniosków o zarządzenie kontroli operacyjnej nie wskazuje, by dochodziło do dysfunkcjonalności systemowej co do oceny przedstawionego sądowi materiału. Nie ma tym samym podstaw do stwierdzenia, jakoby nadzór sądowy, w jego obecnej formie był fasadowy i nieefektywny, toteż utrudniał wręcz uniemożliwiał prowadzenie wnikliwej kontroli wniosków o zarządzenie kontroli operacyjnej pod kątem legalności stosowanych środków technicznych i adekwatności środków, o które wnoszono w konkretnej sprawie.*

Istotnym gwarantem przestrzegania procedur w zakresie zarządzania oraz późniejszego wykorzystania materiałów kontroli operacyjnej są przepisy karne – przede wszystkim art. 231 § 1 ustawy z dnia 6 czerwca 1997 r. – *Kodeks karny*[37] sankcjonujący nieprawidłowości w postępowaniu funkcjonariuszy publicznych, polegające na przekroczeniu uprawnień lub niedopełnieniu obowiązków. Oprócz tego wadliwe proceduralnie

operacyjnej]*, realizowany jest w szczególności poprzez merytoryczną i efektywną kontrolę podstaw faktycznych wnioskowanych czynności oraz legalności i prawidłowości ich inicjowania i prowadzenia*.

[34] Dz. U. Nr 53, poz. 273.

[35] W przepisach pragmatycznych podmiotów uprawnionych.

[36] Zgodnie z ustawami pragmatycznymi podmiotów uprawnionych, we wniosku o zarządzenie kontroli operacyjnej muszą być wskazane okoliczności uzasadniające potrzebę zastosowania kontroli operacyjnej, w tym stwierdzonej bezskuteczności lub nieprzydatności innych środków.

[37] Dz. U. z 2022 r. poz. 1138.

działania związane ze stosowaniem kontroli operacyjnej rodzą także odpowiedzialność dyscyplinarną dla funkcjonariuszy podmiotów uprawnionych.

Na uwagę zasługuje również fakt, że funkcjonujące obecnie rozwiązania prawne wychodzą naprzeciw oczekiwaniom TK wyrażonym w uzasadnieniu do wyroku TK z 2014 r., a tym samym są zgodne z intencjami Pana Rzecznika. Otóż podejrzanemu w postępowaniu przygotowawczym przysługuje prawo do końcowego zaznajomienia się z materiałami[38], co w przypadku włączenia do akt materiałów uzyskanych w wyniku stosowania kontroli operacyjnej, w istocie oznacza przekazanie takiej osobie informacji o objęciu jej tym rodzajem czynności operacyjno-rozpoznawczych.

Ze względu na ustawowy obowiązek niezwłocznego niszczenia materiałów z kontroli operacyjnej niezawierających dowodów pozwalających na wszczęcie postępowania karnego lub dowodów mających znaczenie dla toczącego się postępowania karnego, a także obowiązek niezwłocznego niszczenia danych telekomunikacyjnych, pocztowych i internetowych, które nie mają znaczenia dla postępowania karnego, nie jest zasadne i celowe informowanie osób o stosowaniu wobec nich kontroli operacyjnej oraz o uzyskiwaniu dotyczących tych osób danych, w tym danych telekomunikacyjnych, internetowych lub pocztowych. Skoro uzyskane materiały lub dane zostają usunięte i zniszczone, to żadne dane i informacje nie są gromadzone i przechowywane, co oznacza *de facto*, że materiałów i danych nie ma w obrocie prawnym, w posiadaniu żadnego organu władzy, a tym samym nie istnieje w tym przypadku stan naruszenia prawa do ochrony prywatności osoby, wolności i ochrony tajemnicy komunikowania się oraz autonomii informacyjnej.

Należy również mieć na uwadze, że udostępnienie materiałów z kontroli operacyjnej, w tym materiałów związanych z uzyskaniem danych telekomunikacyjnych, internetowych lub pocztowych osobie, wobec której były prowadzone czynności operacyjno-rozpoznawcze, nawet w przypadku gdy materiały z tych czynności okazały się nieprzydatne do celów postępowania karnego, a czynności zostały zakończone, może prowadzić do dekonspiracji czynności służb w innych sprawach, do ujawnienia objętych niejawnością metod i form działania tych formacji w ramach czynności operacyjno-rozpoznawczych, a tym samym zagrażać lub uniemożliwiać realizację ustawowych zadań. Dla osób ze środowisk przestępczych będzie to wyraźny sygnał do zmiany taktyki działania i zwiększenia konspiracji podejmowanych działań przestępczych, a tym samym utrudni w przyszłości ujawnianie i wykrywanie sprawców szkodliwych społecznie zachowań. Ponadto udostępnienie powyższych materiałów może naruszać prawa i wolności innych osób, których dane mogą być zawarte w tych materiałach.

Poza tym specyfika czynności operacyjno-rozpoznawczych sprawia, że w większości przypadków stosowanie kontroli operacyjnej nie jest czynnością samoistną, ale elementem procesu uzyskiwania informacji, w którym krąg osób objętych stosowaniem tej metody jest płynny, zmienia się w zależności od bieżących ustaleń. Kontrola operacyjna nigdy nie jest celem samym w sobie, co czyni zadość zasadzie subsydiarności. Ponadto przy złożonych sprawach o skomplikowanym *modus operandi*, nawet przekazanie do prokuratury materiałów wskazujących na popełnienie przestępstwa nie musi oznaczać zakończenia sprawy. Tym samym trudno wskazać „bezpieczny" moment przekazania informacji o fakcie objęcia kontrolą operacyjną, z punktu widzenia możliwości dalszego, skutecznego prowadzenia tychże czynności.

Trzeba mieć również na względzie orzecznictwo ETPCz. Przykładowo w wyroku Zakharov przeciwko Rosji[39] ETPCz w § 287 stwierdził, że *w praktyce, wymóg informowania może nie być wykonalny w każdej sprawie. Czynność lub zagrożenie, przeciwko którym kierowane są konkretne środki nadzoru, mogą trwać latami, nawet dekadami po zawieszeniu tych środków. Informowanie każdej osoby dotkniętej zawieszonym środkiem, może narazić na szwank długotrwały cel, który oryginalnie przyświecał nadzorowi. Co więcej, informowanie to może skutkować wyjawieniem metod pracy i pól operacji służb wywiadowczych oraz identyfikować ich agentów. Stąd fakt, że osoby, których dotyczą środki tajnego nadzoru nie są informowane od razu po zaprzestaniu przechwytywania, nie może sam w sobie być podstawą do przyjęcia wniosku, że ingerencja nie była „konieczna w demokratycznym społeczeństwie", ponieważ brak wiedzy o stosowanych środkach tajnego nadzoru, zapewnia skuteczność przechwytywania komunikacji. Jak tylko po zakończeniu stosowania środków tajnego nadzoru zaistnieje możliwość poinformowania objętej nimi osoby w sposób niestwarzający zagrożenia dla celu wprowadzonego ograniczenia [prawa do prywatności], odpowiednie informacje powinny zostać jej przekazane (…). Trybunał również bierze pod uwagę Rekomendację Komitetu Ministrów regulującą wykorzystanie danych osobowych w sektorze policji, która stanowi, że jeżeli działania*

[38] Art. 321 § 1 ustawy – *Kodeks postępowania karnego*, przy czym zgodnie z art. 300 § 1, o prawie do końcowego zaznajomienia z materiałami postępowania przygotowawczego podejrzanego poucza się przed pierwszym przesłuchaniem.

[39] Roman Zakharov przeciwko Rosji – wyrok Wielkiej Izby ETPCz z dnia 4 grudnia 2015 r., skarga nr 47143/06.

policji nie są już prowadzone, konkretne osoby, gdy tylko jest to wykonalne, powinny być informowane o tym, że policja przechowuje o nich informacje, ilekroć dane dotyczące jednostek zostały zebrane i przechowywane bez ich wiedzy i jeżeli nie zostały usunięte.

Mając na uwadze orzecznictwo TK oraz wyrok ETPCz należy stwierdzić, że zarówno TK, jak i ETPCz nie formułują wymogu obowiązkowego, każdorazowego informowania przez Policję o stosowanych czynnościach operacyjno-rozpoznawczych, w tym kontroli operacyjnej czy też uzyskiwania danych na jej temat (w tym danych telekomunikacyjnych, pocztowych, internetowych), nie stawiają też wymogu dostępu do informacji, w tym materiałów uzyskanych w toku tych czynności, w każdym przypadku, gdy materiały te nie zostały wykorzystane na potrzeby postępowań karnych (w tym nie zostały przekształcone w materiał procesowy). Ponadto ETPCz wskazuje, że informowanie osób, których dotyczą niejawne działania może nastąpić, w przypadku gdy nie doprowadzi to do zniweczenia lub do stworzenia zagrożenia celowi, dla którego działania były prowadzone, a także gdy nie będzie to skutkować wyjawieniem metod pracy i pól operacji służb wywiadowczych lub gdy nie doprowadzi do zidentyfikowania ich agentów. Europejski Trybunał Praw Człowieka dopuszcza tym samym, że informowanie osób, wobec których były prowadzone niejawne działania (czynności operacyjno-rozpoznawcze, w tym kontrola operacyjna, niejawne uzyskiwanie danych telekomunikacyjnych, pocztowych, internetowych), nawet wiele lat po zakończeniu tych działań może nie być wykonalne z powyższych powodów.

Niezależnie od przytoczonych uwarunkowań związanych z charakterem czynności operacyjno-rozpoznawczych, wprowadzenie obowiązku informacyjnego może powodować również szereg problemów praktycznych. Próby ustalenia tożsamości osób postronnych (np. dzwoniących do osoby objętej kontrolą operacyjną w trakcie jej trwania), z reguły niezwiązanych w żaden sposób z przestępstwem czy okolicznościami jego popełnienia, wiązałyby się z koniecznością gromadzenia dodatkowych danych o tych osobach pozwalających na jednoznaczną identyfikację rozmówcy. Tym samym wprowadzenie prawnego obowiązku informowania o fakcie objęcia kontrolą operacyjną każdej – także postronnej osoby – prowadziłoby w praktyce do konieczności podejmowania przez służbę działań prowadzących do jeszcze dalej idącej ingerencji w sferę prywatności. Warto także zauważyć, że podmiotami „postronnymi" mogą być nie tylko osoby fizyczne, ale również osoby prawne czy organy administracji. Na marginesie trzeba zwrócić uwagę na trudności w realizacji nadzoru nad tak daleko idącym obowiązkiem informacyjnym.

W przypadku uzyskiwania danych telekomunikacyjnych w celu ustalenia sprawców przestępstw, konieczne jest niejednokrotnie uzyskanie informacji o wszystkich logowaniach w danej stacji BTS, w określonym odcinku czasowym. Również w tym 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).

Materia stanowiąca przedmiot wystąpienia Pana Rzecznika została uregulowana również w dyrektywie 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 uchylającej decyzję ramową Rady 2008/977/WSiSW*[40]. Ustanawia ona przepisy o ochronie 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 tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom (art. 1 ust. 1). Artykuł 13 dyrektywy 2016/680 określa zakres prawa do informacji osoby, której dane podlegają przetwarzaniu. Przepis ten w ust. 3 przewiduje, że poinformowanie osoby w konkretnych przypadkach może jednak zostać opóźnione, ograniczone lub wykluczone w takim zakresie i przez taki czas, w jakim odnośny środek jest działaniem koniecznym i proporcjonalnym w społeczeństwie demokratycznym, z należytym uwzględnieniem praw podstawowych i uzasadnionych interesów danej osoby fizycznej, aby m.in. uniemożliwić utrudnianie czynności postępowań urzędowych lub sądowych, postępowań przygotowawczych lub procedur, jak również aby uniemożliwić zakłócanie zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, a także aby chronić bezpieczeństwo publiczne oraz bezpieczeństwo narodowe.

[40] Dz. Urz. UE L 119 z 4.5.2016, s. 89.

Powyższa regulacja została zaimplementowana do polskiego porządku prawnego w postaci art. 26 ust. 1 ustawy z dnia 14 grudnia 2018 r. *o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości*[41], z którego wynika m.in., że nie przekazuje się informacji osobie, której dane dotyczą, jeżeli mogłoby to powodować:

1) ujawnienie informacji uzyskanych w wyniku czynności operacyjno-rozpoznawczych;
2) utrudnienie lub uniemożliwienie rozpoznawania, zapobiegania, wykrywania lub zwalczania czynów zabronionych;
3) utrudnienie prowadzenia postępowania karnego, karnego wykonawczego, karnego skarbowego lub w sprawach o wykroczenia lub wykroczenia skarbowe;
4) zagrożenie życia, zdrowia ludzkiego lub bezpieczeństwa i porządku publicznego;
5) zagrożenie bezpieczeństwa narodowego, w tym obronności lub bezpieczeństwa oraz ekonomicznych podstaw funkcjonowania państwa;
6) istotne naruszenie dóbr osobistych innych osób.

W świetle powyższego, a także wbrew twierdzeniom Pana Rzecznika, nieinformowanie osoby o stosowaniu wobec niej kontroli operacyjnej spełnia standardy prawa europejskiego, w oparciu o które przyjęto analogiczne rozwiązania w prawie krajowym.

Reasumując, w pierwszej kolejności zasygnalizowania wymaga, że zaprezentowana przez Pana Rzecznika idea informowania osób o fakcie objęcia ich kontrolą operacyjną niesie ze sobą wiele ryzyk. Przede wszystkim należy wskazać na zagrożenia, jakie dla skuteczności uprawnionych podmiotów stanowi faktyczna dekonspiracja ich działań, a tym samym negatywnego wpływu na możliwość zapewnienia bezpieczeństwa państwa oraz jego obywateli.

Pan Rzecznik w swoim wystąpieniu zdaje się również nie zauważać funkcjonujących obecnie w przepisach mechanizmów zabezpieczających przed nieprawidłowościami w procesie zarządzania oraz stosowania kontroli operacyjnej, tj. przede wszystkim kontroli prokuratury i sądu. Organy te z jednej strony stanowią gwarancję zgodnego z prawem zarządzenia kontroli operacyjnej, z drugiej zaś – właściwego wykorzystania materiałów zawierających dowód przestępstwa (w postępowaniu przygotowawczym) oraz procedurę postępowania z materiałami, które takich informacji nie zawierają (niezwłoczne zniszczenie).

Ponadto należy podkreślić, że funkcjonujące obecnie rozwiązania prawne dotyczące procedury postępowania przygotowawczego, gwarantujące podejrzanemu prawo do końcowego zaznajomienia się z materiałami sprawiają, że w przypadku włączenia do akt materiałów uzyskanych w wyniku stosowania kontroli operacyjnej (a temu celowi właśnie działania te służą), w istocie oznacza przekazanie takiej osobie również informacji o objęciu jej tym rodzajem czynności operacyjno-rozpoznawczych.

Nie kwestionując niezaprzeczalnej wartości jaką jest ochrona prywatności, nie można nie zauważyć, że sugerowane przez Pana Rzecznika zmiany w przepisach pragmatycznych podmiotów uprawnionych do stosowania kontroli operacyjnej negatywnie wpłyną na możliwość zapewnienia bezpieczeństwa obywatelom, dekonspirując działania podmiotów uprawnionych.

Mając zatem na uwadze procedurę wdrożenia kontroli operacyjnej, cele jakim służy ta metoda uzyskiwania informacji, a także późniejsze wykorzystanie jej efektów w postępowaniu przygotowawczym, skutkujące ujawnieniem faktu jej stosowania, należy ocenić jako niecelowe sugerowane przez Pana Rzecznika zmiany w przepisach w zakresie informowania osób o fakcie objęcia ich kontrolą operacyjną.

Nawiązując do poruszonego w wystąpieniu Pana Rzecznika orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej (TSUE) w zakresie retencji i wykorzystania danych telekomunikacyjnych[42], w tym wyroku z dnia 21 grudnia 2016 r. w połączonych sprawach C-203/15 i C-698/15 *Tele2 Sverige AB i in.* należy stwierdzić, że rozstrzygnięcie to dąży z jednej strony do zaprzestania masowego zatrzymywania danych telekomunikacyjnych przez operatorów, z drugiej zaś do ograniczenia przypadków udostępniania tych danych do walki z „poważną przestępczością" oraz wprowadzenia uprzedniej kontroli ich udostępniania.

Odnosząc się do argumentów Pana Rzecznika w kwestii zatrzymywania przez określony czas przez operatorów tzw. danych lokalizacyjnych, to istotnie obowiązek ten stanowi samoistną ingerencję w prawa chronione konstytucyjnie, w tym prawo do prywatności. Niewątpliwie też stanowi ingerencję w prawo do prywatności możliwość uzyskania dostępu do tych danych przez uprawnione organy krajowe. Celem regulacji obowiązujących w tym zakresie jest jednak zapewnienie dostępności przedmiotowych danych

[41] Dz. U. z 2019 r. poz. 125.

[42] Niestanowiących treści przekazu telekomunikacyjnego.

dla dochodzenia, wykrywania i ścigania poważnych przestępstw, czyli zapewnienie bezpieczeństwa publicznego, a prawo do bezpieczeństwa osobistego ma zdecydowanie wyższą wartość niż prawo do prywatności. W dobie intensywnego rozwoju technologii komunikacyjnych dane pozyskiwane od operatorów telekomunikacyjnych stanowią coraz skuteczniejsze narzędzie do walki z poważną przestępczością, zatem zatrzymywanie tych danych przez operatorów i ich udostępnianie dla celów dochodzeniowo-śledczych służy realizacji zadań państwa w zakresie ochrony bezpieczeństwa obywateli i bezpieczeństwa publicznego.

Należy wyjaśnić, że w polskim prawie funkcjonują odpowiednie uregulowania związane z określeniem zasad zatrzymywania danych, dostępu do nich podmiotów uprawnionych oraz sprawowaniem niezależnej kontroli nad ich uzyskiwaniem. Ograniczenia zawarte w tych przepisach powodują, że Policja i inne podmioty uprawnione nie gromadzą ani nie przechowują masowo danych telekomunikacyjnych, a wyłącznie korzystają z danych zatrzymywanych przez operatorów telekomunikacyjnych, w okolicznościach przewidzianych w ustawach pragmatycznych.

W przepisach wyróżnia się trzy podstawowe kategorie danych, z których mogą korzystać podmioty uprawnione – są to dane telekomunikacyjne, pocztowe i internetowe, o których mowa odpowiednio w:

- art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – *Prawo telekomunikacyjne*[43];
- art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – *Prawo pocztowe*[44];
- art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. *o świadczeniu usług drogą elektroniczną*[45].

Dane te mogą być przetwarzane bez wiedzy i zgody osoby, której dotyczą.

Podmiotami uprawnionymi do uzyskiwania danych telekomunikacyjnych, pocztowych i internetowych są:

- Policja, na podstawie art. 20c ustawy *o Policji;*
- SG, na podstawie art. 10b ustawy *o Straży Granicznej;*
- Biuro Nadzoru Wewnętrznego, na podstawie art. 11w ustawy *o szczególnych formach sprawowania nadzoru przez ministra właściwego do spraw wewnętrznych;*
- Żandarmeria Wojskowa, na podstawie art. 30 ustawy *o Żandarmerii Wojskowej i wojskowych organach porządkowych;*
- ABW, na podstawie art. 28 ustawy *o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu;*
- SKW, na podstawie art. 32 ustawy *o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego;*
- Centralne Biuro Antykorupcyjne, na podstawie art. 18 ustawy *o Centralnym Biurze Antykorupcyjnym;*
- KAS, na podstawie art. 114 ustawy o KAS*;*
- Służba Ochrony Państwa, na podstawie art. 57 ustawy *o Służbie Ochrony Państwa.*

Na gruncie polskiego prawa przepisy regulujące kwestie retencji danych telekomunikacyjnych zostały określone w ustawie – *Prawo telekomunikacyjne* w *Dziale VIII Obowiązki na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego* (art. 180a-180e). Obowiązek zatrzymywania i przechowywania (art. 180a ust. 1 pkt 1) obejmuje okres 12 miesięcy, licząc od dnia połączenia lub nieudanej próby połączenia. Z dniem upływu tego okresu dane są niszczone przez operatora, z wyjątkiem tych, które zostały zabezpieczone, zgodnie z odrębnymi przepisami, w tym wspomnianych ustaw pragmatycznych. Odnotowania w tym miejscu wymaga, że powyższy okres retencji danych jest tożsamy z okresem przechowywania danych o wykonanych usługach telekomunikacyjnych, w zakresie umożliwiającym ustalenie należności za wykonanie tych usług oraz rozpatrzenie reklamacji (art. 168). Dotychczasowe doświadczenia wskazują, że przyjęty w polskim prawie 12-miesięczny okres przechowywania zatrzymanych danych telekomunikacyjnych należy uznać za optymalny z punktu widzenia efektywności działania służb uprawnionych do ich wykorzystywania. Został on zdefiniowany na podstawie ustawy z dnia 16 listopada 2012 r. *o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw*[46], która skróciła okres retencji danych z 24[47]

[43] Dz. U. z 2021 r. poz. 576, z późn. zm.
[44] Dz. U. z 2022 r. poz. 896.
[45] Dz. U. z 2020 r. poz. 344.
[46] Dz. U. poz. 1445, z późn. zm.
[47] Przewidziany jako maksymalny okres zatrzymywania danych w Dyrektywie 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 zmieniającej dyrektywę 2002/58/WE* – art. 6 (Dz. Urz. UE L 105 z 13.04.2006, str. 54) – akt utracił moc.

do 12 miesięcy. Jak wynika z uzasadnienia do treści wyroku TK z 2014 r. podobny termin zatrzymywania danych obowiązuje w większości państw członkowskich UE.

Ponadto, zgodnie z art. 179 ust. 9 ustawy – *Prawo telekomunikacyjne*, przedsiębiorca telekomunikacyjny świadczący publicznie dostępne usługi telekomunikacyjne jest obowiązany prowadzić elektroniczny wykaz abonentów, użytkowników lub zakończeń sieci, uwzględniając w nim dane uzyskiwane przy zawarciu umowy.

Podmioty uprawnione mogą uzyskiwać dane telekomunikacyjne, o których mowa w 180c ustawy – *Prawo telekomunikacyjne*, a także z wykazu, o którym mowa w art. 179 ust. 9, oraz o których mowa w art. 161 tej ustawy, w celu zapobiegania lub wykrywania przestępstw, jak również realizacji określonych ustawowo zadań (np. w przypadku Policji i Żandarmerii Wojskowej – w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych oraz w przypadku Służby Ochrony Państwa – dla zapewnienia bezpieczeństwa ochranianym osobom lub obiektom).

Szef Krajowej Administracji Skarbowej zauważył, że uprawnienie do pozyskiwania danych telekomunikacyjnych, internetowych i pocztowych przysługiwało wywiadowi skarbowemu, analogicznie jak innym służbom, od wielu lat zanim został wydany wyrok TK z 2014 r., w którym wskazano konieczność wprowadzenia kontroli sądowej pozyskiwanych przez te służby ww. danych. Nie można zatem zgodzić się z zarzutem Pana Rzecznika, że uprawnienie to służby uzyskały na podstawie ustawy z dnia 15 stycznia 2016 r. *o zmianie ustawy o Policji oraz niektórych innych ustaw*. Ponadto uprawnienie do pozyskiwania ww. danych nie dotyczy treści przekazów telekomunikacyjnych czy też internetowych. Dostęp do treści tych przekazów jest możliwy wyłącznie w drodze kontroli operacyjnej.

Co istotne, określone w ustawach pragmatycznych uprawnienie służb 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 uprawnionych podmiotów do tych danych ma charakter ukierunkowany, gdyż odbywa się na wniosek w stosunku do indywidulanie określonej osoby, miejsca lub urządzenia. Podkreślenia wymaga, że zapobiegając 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 danych telekomunikacyjnych. Zatem ograniczenie możliwości uzyskiwania takich danych w wielu przypadkach znacząco utrudni wykrycie przestępstw oraz ustalenie ich sprawców. Trzeba mieć na uwadze, że w dobie rozwijającej się bardzo dynamicznie technologii informatycznej większość komunikacji odbywa się drogą elektroniczną. W czasie kiedy kontakty międzyludzkie i procesy związane z konsumpcją oraz funkcjonowaniem podmiotów gospodarczych są oparte na łączności telekomunikacyjnej i elektronicznej, daleko idące ograniczenie możliwości korzystania z danych telekomunikacyjnych w procesie wykrywczym przez organy władzy publicznej lub pozbawienie ich możliwości wykorzystania retencji danych spowodowałoby znaczne zmniejszenie skuteczności ich działań. Należy również wskazać, że Biuro Pana Rzecznika było inicjatorem wielu spotkań związanych z przeciwdziałaniem tzw. „patostrimingu" czy mowy nienawiści, w przypadku których ustalenie sprawcy czynu zabronionego jest możliwe zazwyczaj tylko na skutek uzyskania dostępu do przedmiotowych danych.

Całkowicie nie można zgodzić się z poglądem Pana Rzecznika, że ustawa z dnia 15 stycznia 2016 r. *o zmianie ustawy o Policji oraz niektórych innych ustaw* „nie naprawiła zakwestionowanego przez Trybunał i omówionego wcześniej stanu rzeczy, lecz znacząco poszerzyła możliwości ingerencji Policji i służb specjalnych w sferę prywatności obywateli. Służby uzyskały dostęp do danych internetowych za pomocą stałego łącza. Pobieranie danych obecnie nie musi się zatem wiązać z żadnym toczącym się postępowaniem. Służby nie muszą już od chwili wejścia w życie tej ustawy – tak jak przedtem – składać pisemnych wniosków do dostawców usług internetowych i wykazywać, na potrzeby jakiego postępowania dane są im potrzebne. Oznacza to, że dane te mogą być zbierane nie tylko wówczas, gdy jest to rzeczywiście konieczne do wykrywania lub zapobiegania najpoważniejszym przestępstwom, którym inaczej nie da się przeciwdziałać (jak wskazują standardy wynikające z Konstytucji RP i prawa europejskiego), ale także wtedy, gdy jest to dla służb wygodne". Należy bowiem zauważyć, że tryb udostępniania danych przez przedsiębiorcę telekomunikacyjnego, operatora pocztowego lub usługodawcę świadczącego usługi drogą elektroniczną określa np. art. 20c ust. 2 ustawy

o Policji czy art. 10b ust. 2 ustawy *o Straży Granicznej*. Zgodnie z przytoczonymi przepisami wskazane podmioty udostępniają dane:

1) funkcjonariuszowi wskazanemu w pisemnym wniosku, w przypadku Policji: Komendanta Głównego Policji, Komendanta Centralnego Biura Śledczego Policji, Komendanta Biura Spraw Wewnętrznych Policji, Komendanta Centralnego Biura Zwalczania Cyberprzestępczości, komendanta wojewódzkiego Policji albo osoby przez nich upoważnionej, a w przypadku SG – Komendanta Głównego SG, Komendanta Biura Spraw Wewnętrznych SG lub komendanta oddziału SG albo osoby przez nich upoważnionej;
2) na ustne żądanie funkcjonariusza posiadającego pisemne upoważnienie osób, o których mowa w pkt 1;
3) za pośrednictwem sieci telekomunikacyjnej funkcjonariuszowi posiadającemu pisemne upoważnienie osób, o których mowa w pkt 1.

Ustawy pragmatyczne podmiotów uprawnionych przewidują możliwość uzyskiwania danych telekomunikacyjnych także za pośrednictwem sieci telekomunikacyjnej. Nie oznacza to oczywiście masowego pobierania tego typu danych, bowiem każdorazowo muszą być spełnione ustawowe przesłanki określone w tych przepisach. Przykładowo, przepisy art. 20c ust. 4 ustawy *o Policji* czy art. 10b ust. 4 ustawy *o Straży Granicznej* określają, 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 lub SG albo prowadzonych przez nie czynności. Mechanizm ten zapewnia więc wewnętrzną weryfikowalność przypadków pozyskiwania danych telekomunikacyjnych.

W ramach autokontroli nad wykorzystywaniem powyższych uprawnień, podmioty uprawnione są zobowiązane do prowadzenia rejestru wystąpień o uzyskanie danych telekomunikacyjnych, pocztowych i internetowych zawierające informacje identyfikujące jednostkę organizacyjną i funkcjonariusza uzyskującego te dane, ich rodzaj, cel uzyskania oraz czas, w którym zostały uzyskane. Uzyskane dane, które mają znaczenie dla postępowania karnego, podmioty uprawnione są zobligowane przekazać prokuratorowi, który podejmuje decyzję o zakresie i sposobie ich wykorzystania. Natomiast dane, które nie mają znaczenia dla postępowania karnego albo nie są istotne z punktu widzenia realizowanych zadań, podlegają niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu.

Odnosząc się do zarzutów Pana Rzecznika dotyczących sposobu ukształtowania kontroli nad uzyskiwaniem danych telekomunikacyjnych, pocztowych i internetowych, należy wskazać, że w przepisach pragmatycznych podmiotów uprawnionych ustanowiono następczą kontrolę pozyskiwania powyższych danych, realizowaną przez sąd okręgowy (w przypadku służb wojskowych – wojskowy sąd okręgowy) właściwy dla siedziby podmiotu uprawnionego, na podstawie przekazywanych w okresach półrocznych sprawozdań, obejmujących:

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

W ramach powyższej kontroli sąd może również zapoznać się z materiałami uzasadniającymi udostępnienie podmiotom uprawnionym danych telekomunikacyjnych, pocztowych lub internetowych.

Tak ukształtowane przepisy wpisujące się w zakres dopuszczony wyrokiem TK z 2014 r. pozwalają sądowi, jako niezależnemu organowi wymiaru sprawiedliwości, na swobodne ukształtowanie sposobu przeprowadzania kontroli. To w kompetencji niezawisłego sądu znajduje się decyzja o tym czy lub i w jakim zakresie sprawdzeniu będą podlegać materiały konkretnych spraw oraz jakie będzie kryterium doboru spraw, w których zostanie przeprowadzona pogłębiona kontrola.

Minister Obrony Narodowej zwrócił uwagę, że przedmiotowa kontrola jest tym efektywniejsza, że sprawuje ją sąd wydający zgodę na stosowanie kontroli operacyjnej oraz, że nie jest możliwa sytuacja pobierania danych telekomunikacyjnych bez związku z konkretnym postępowaniem. Możliwość pozyskiwania danych za pomocą stałego łącza ma charakter wyłącznie techniczny, jest konieczna ze względu na postępujący rozwój technologiczny i nie jest okolicznością sprzyjającą nadużyciom. Technologie informatyczne stosowane w związku z pozyskiwaniem danych umożliwiają efektywną kontrolę ich pozyskiwania i wykrycie ewentualnych nadużyć.

Według Prokuratury Krajowej wskazanie przez Pana Rzecznika na brak należytej sądowej kontroli pozyskiwania przez Policję i pozostałe uprawnione podmioty danych telekomunikacyjnych, pocztowych i internetowych stanowi w istocie krytykę nie tyle obowiązującego prawa, tylko praktyki sądowej i stanowi *de facto* zarzut bagatelizowania przez sądy uprawnień kontrolnych wynikających np. z art. 20ca ustawy *o Policji*. W swoim piśmie z 13 stycznia 2022 r. Pan Rzecznik powołał się na orzecznictwo TK i ETPCz dotyczące kontroli operacyjnej oraz orzecznictwo TSUE dotyczące retencji danych telekomunikacyjnych, w żaden sposób nie różnicując tych dwóch sfer. Na podstawie tez orzeczeń ETPCz i TSUE, Pan Rzecznik przedstawił postulaty, aby:

- obywatel był informowany o zakończonej kontroli operacyjnej – przy czym nie wskazano czy celowe byłoby wprowadzenie wyjątków od tej reguły, a jeśli tak, w jakich sytuacjach;
- obywatel miał dostęp do materiałów z kontroli operacyjnej;
- obywatel miał prawo złożenia zażalenia na decyzję sądu o przeprowadzeniu tej kontroli, przy czym nie ograniczono zakresu tego zażalenia ani przedmiotowo (np. do kwestii zgodności z prawem) ani podmiotowo (poprzez wskazanie kręgu osób uprawnionych spośród wszystkich osób, których prywatność, chociażby incydentalnie, została naruszona w toku kontroli).

Pan Rzecznik nie przedstawił natomiast postulatów własnych w zakresie retencji danych, ograniczając się tutaj jedynie do wskazania orzecznictwa TSUE. Odnosząc się do przedstawionego przez Pana Rzecznika zagadnienia trzeba wskazać na to, że kontrola operacyjna i retencja danych są zupełnie odmiennymi instytucjami, służącymi innym celom i w różny sposób ingerującymi w prawa i wolności obywatelskie. Należy wreszcie podnieść, że stanowisko TK nie jest bynajmniej podzielane przez organy konstytucyjne i najwyższe organy sądowe wszystkich państw – członków UE. Kompleksowe raporty Agencji Praw Podstawowych Unii Europejskiej (FRA), ustanowionej przez rozporządzenie Rady (WE) nr 168/2007 z dnia 15 lutego 2007 r., wskazują, że w większości państw unijnych nie obowiązują regulacje postulowane przez Pana Rzecznika. Praktycznie w każdym państwie unijnym prawo osoby objętej tego rodzaju działaniami służb do informacji i dostępu do danych jest ograniczone albo wyłączone. Na przykład, z raportu FRA opublikowanego w 2017 r. wynika, że tylko Niemcy i Szwecja przewidują powiadomienie jednostki, której dane uzyskano w ramach ogólnego pozyskiwania danych, z tym, że powiadomienie nie jest wymagane, jeśli decyzja o uzyskaniu danych nie odnosiła się bezpośrednio do tej jednostki (Szwecja) lub jeśli dane zostały niezwłocznie zniszczone (Niemcy). W niektórych krajach (Irlandia, Hiszpania, Szwecja) obowiązek informacyjny jest ograniczany przez przepisy o ochronie informacji niejawnych, w innych (Dania, Finlandia) może być wyłączony na mocy postanowienia sądu lub organu nadzorczego (Niemcy), w jeszcze innych (np. Dania, Finlandia, Holandia) obowiązek ten może być wykonany dopiero wtedy, jeśli jego wykonanie nie zagrozi bezpieczeństwu narodowemu. Prawo dostępu do informacji jest wykonywane pośrednio, tj. za pośrednictwem organu uprawnionego do dostępu do informacji niejawnych czy też najwyższego organu ochrony danych osobowych. W trzech państwach unijnych (Francja, Niemcy, Irlandia) istnieją sądy lub sędziowie wyspecjalizowani w sprawach kontroli operacyjnej, rozpoznający skargi obywateli; w innych państwach skargi rozpoznają specjalne komisje czy organy parlamentarne. Z raportu nie wynika, aby w jakimkolwiek państwie unijnym istniał system spełniający postulaty Pana Rzecznika, a więc przewidujący nieograniczone prawo do informacji, nieograniczone prawo dostępu do zgromadzonych przez uprawnione organy danych i nieograniczone prawo kontroli sądowej.

Należy także przypomnieć, że w przytaczanym przez Pana Rzecznika wyroku TK z 2014 r. TK uznał co prawda, że obywatel powinien mieć prawo do informacji po zakończeniu kontroli, lecz nie uznał tego prawa za bezwzględne, przyznając, że ustawodawca w określonych sytuacjach może je wyłączyć. Trybunał Konstytucyjny podkreślił również, że *brak wyposażenia służb policyjnych oraz służb ochrony państwa w możliwość korzystania ze zdobyczy nowoczesnej techniki, a nawet wyposażenie ich w taką możliwość, lecz w niewystarczającym zakresie, może oznaczać niewywiązanie się państwa z jego konstytucyjnego zadania strzeżenia niepodległości i nienaruszalności terytorium Rzeczypospolitej Polskiej, a także zapewnienia bezpieczeństwa obywateli (art. 5 Konstytucji), czy naruszać zasadę sprawności działania instytucji publicznych (wstęp do Konstytucji). Niekiedy może powodować naruszenie obowiązków wiążących Polskę umów międzynarodowych zobowiązujących do współdziałania w walce z międzynarodową przestępczością i terroryzmem. (…) Naruszenie prawa do ochrony prywatności zagwarantowanego w art. 47 Konstytucji może bowiem nastąpić nie tylko przez bezpośrednie działanie polskich organów państwa, pozyskujących informacje o jednostkach w sposób niejawny. Nastąpi to również w sytuacji braku dostatecznej ochrony obywateli przez państwo przed ingerencją w tę wolność, spowodowaną działaniami innych podmiotów.*

Prokuratura Krajowa zwróciła uwagę, że wyrok TK z 2014 r. został wydany w zupełnie innej sytuacji międzynarodowej, kiedy Polska nie była bezpośrednio zagrożona przez działania militarne lub inną formę międzynarodowej agresji, a co za tym idzie, nie istniała tak istotna potrzeba podejmowania jak najskuteczniejszych działań kontrwywiadowczych. Informowanie agentów wywiadu potencjalnie agresywnego państwa, że stosowano wobec nich kontrolę operacyjną, byłoby działaniem szkodliwym zarówno dla Państwa, jak i – docelowo – dla polskich konstytucyjnych standardów, bowiem w razie wybuchu na terytorium Polski działań wojennych zabraknie instytucji, które mają te standardy chronić. Innymi słowy, w niczym nie negując wzniosłości tych standardów, należy wskazać, że istnienie suwerennego, demokratycznego Państwa Polskiego stanowi wartość nadrzędną, której owe standardy powinny być podporządkowane.

Prokuratura Krajowa zauważyła, że w odniesieniu do retencji danych, system prawny w państwach unijnych nie jest bynajmniej jednolity, pomimo wyroków TSUE i odpowiadających im wyroków sądów krajowych. W niektórych państwach stan prawny ulega obecnie zmianie w kierunku wskazanym przez TSUE, w innych natomiast najwyższe organy sądowe uznały dotychczasowy stan prawny za generalnie zgodny z wymogami unijnymi – można tu wskazać wyrok czeskiego trybunału konstytucyjnego z 15 maja 2019 r., wyrok francuskiego sądu administracyjnego z 21 kwietnia 2021 r. czy też wyrok hiszpańskiego trybunału konstytucyjnego z 23 marca 2021 r.

Rozważania nad potrzebą i kierunkiem zmiany prawa są obecnie o tyle bezprzedmiotowe, że prawo unijne dotyczące omawianego zagadnienia w dalszym ciągu się kształtuje. Powoływane przez Pana Rzecznika orzeczenia TSUE odnosiły się do dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. *dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywy o prywatności i łączności elektronicznej)*[48], która w ciągu najbliższych kilku lat ma zostać uchylona i zastąpiona przez rozporządzenie w sprawie e-prywatności (*regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC*), co do którego trwają obecnie uzgodnienia trójstronne między organami unijnymi. Dokonywanie zmian prawnych w chwili obecnej jest więc bezprzedmiotowe, ponieważ ich kształt musiałby uwzględniać treść aktu prawnego będącego obecnie dopiero przedmiotem prac.

Prokuratura Krajowa uznała za nieodpowiednie posłużenie się przez Pana Rzecznika, w ocenie obowiązujących w Polsce przepisów dotyczących czynności operacyjno-rozpoznawczych, zatrzymywania danych retencyjnych oraz ich wykorzystywania przez uprawnione organy państwa, argumentacją ETPCz zawartą w wyroku z dnia 4 grudnia 2015 r. odnoszącą się do prawa rosyjskiego.

Ustawa z dnia 15 stycznia 2016 r. *o zmianie ustawy o Policji oraz niektórych innych ustaw* wprowadziła dodatkowy mechanizm niezależnej kontroli nad pozyskiwaniem danych przez służby poprzez obowiązek corocznego przekazywania zagregowanej informacji w tym zakresie przez Ministra Sprawiedliwości do Sejmu RP i Senatu RP (art. 175b § 2 ustawy z dnia z dnia 27 lipca 2001 r. – *Prawo o ustroju sądów powszechnych*[49]).

Opisane powyżej mechanizmy kontrolne wydają się być nie tylko racjonalne z punktu widzenia prawidłowej realizacji ustawowych zadań Policji oraz innych podmiotów uprawnionych, ale przede wszystkim skuteczne i wystarczające w kontekście przestrzegania praw człowieka. Spełniają również postulat stosowania niezależnej kontroli zewnętrznej dla tego typu uprawnień, ingerujących w prywatność. Należy przy tym zaznaczyć, że ingerencja ta jest daleko mniej idąca w porównaniu chociażby z kontrolą operacyjną, bowiem nie dochodzi do rejestracji treści korespondencji, a jedynie danych użytkowników końcowych.

Dodatkowo należy wskazać, że mimo, iż wyrok TK z 2014 r. odnosił się wyłącznie do danych telekomunikacyjnych – jak wynika z uzasadnienia do projektu ustawy *o zmianie ustawy o Policji oraz niektórych innych ustaw*[50] *– z uwagi na konieczność opracowania kompleksowego ujęcia materii, obok danych telekomunikacyjnych, kontrolą sądową objęto również proces udostępniania uprawnionym służbom danych pocztowych, określonych na podstawie ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. z 2012 r. poz. 1529) oraz tzw. danych internetowych, określonych w art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422). Pomimo, że pkt 5 wyroku Trybunału o sygn. K 23/11 nie obejmuje swoim zakresem danych uzyskiwanych na podstawie prawa pocztowego oraz danych uzyskiwanych na podstawie ustawy o świadczeniu usług drogą elektroniczną, powyższe rozszerzenie zakresu przedmiotowego kontroli znajduje uzasadnienie w tym, że działalność służb w tych obszarach*

[48] Dz. Urz. UE L 201 z 31.07.2002, str. 37, z późn. zm.

[49] Dz. U. z 2020 r. poz. 2072, z późn. zm.

[50] druk sejmowy nr 154 (VIII kadencja Sejmu RP).

w podobnym stopniu ingeruje w prawa i wolności obywatelskie jak proces pozyskiwania danych telekomunikacyjnych. Projekt przewiduje również takie same przesłanki udostępniania, procedury weryfikacji oraz niszczenia udostępnianych służbom danych pocztowych oraz danych o których mowa w ustawie o świadczeniu usług drogą elektroniczną, zbędnych dla prowadzonego postępowania. Skorelowanie regulacji prawnych w stosunku do wszystkich obszarów danych dotyczących sfery komunikacji między osobami stanowi rozwiązanie systemowe służące pogłębieniu zaufania obywateli do organów państwowych.

Nie bez znaczenia dla oceny rozwiązań przyjętych w poszczególnych państwach członkowskich UE w analizowanym zakresie pozostaje specyfika procesu wykrywczego w tych krajach, która determinuje konieczność zapewnienia adekwatnych środków w zakresie sposobu sprawowania nadzoru nad uzyskiwaniem przez uprawnione podmioty danych telekomunikacyjnych. W Polsce ciężar procesu wykrywczego koncentruje się na etapie czynności operacyjno-rozpoznawczych, a nie na etapie procesu karnego, jak ma to miejsce w części państw Europy Zachodniej.

Co istotne, odnosząc się do przytoczonego przez Pana Rzecznika orzecznictwa[51] TSUE, za uprawnione należy uznać stwierdzenie, w oparciu o toczącą się na forum europejskim dyskusję w analizowanym obszarze, że sposób wdrożenia rozwiązań wynikających z treści wyroków Trybunału budzi szereg kontrowersji w wielu państwach członkowskich UE, z uwagi na konieczność zachowania równowagi pomiędzy skutecznością działania służb w obszarze zapewnienia bezpieczeństwa i porządku publicznego a poszanowaniem prawa do prywatności.

Powyższe kryterium zostało również uwzględnione podczas oceny rozwiązań przyjętych w ustawie z dnia 15 stycznia 2016 r. *o zmianie ustawy o Policji oraz niektórych innych ustaw* przez Komisję Wenecką. W opinii z dnia 13 lutego 2016 r.[52] Komisja wskazała, że z zadowoleniem przyjmuje starania polskiego ustawodawcy o wykonanie wyroku TK z 2014 r. Podniesiono, że wiele państw stoi obecnie w obliczu bardzo realnych zagrożeń ze strony terroryzmu i przestępczości zorganizowanej. Zgodnie z Konwencją o ochronie praw człowieka i podstawowych wolności[53], zwaną Europejską Konwencją Praw Człowieka, państwa mają margines swobody przy podejmowaniu decyzji, w jaki sposób zachować równowagę między bezpieczeństwem a wolnością. Polski ustawodawca nie jest bynajmniej jedynym, który spotkał się z krytyką dotyczącą sposobu, w jaki ta równowaga została osiągnięta.

W kontekście wyroku TSUE w połączonych sprawach C-203/15 i C-698/15 *Tele2 Sverige AB i in.* wątpliwości dotyczą również interpretacji określenia „poważnej przestępczości". Należy jednak odnotować, że w polskim prawie ustawodawca dokonał rozróżnienia czynów karalnych na przestępstwa i wykroczenia kierując się m.in. oceną szkodliwości społecznej czynów, co w konsekwencji przekłada się na zróżnicowanie dotkliwości sankcji za przestępstwa i wykroczenia. Można więc domniemywać, że wprowadzając to rozróżnienie ustawodawca dokonał także podziału czynów zabronionych na te, które mają charakter poważny (przestępstwa) oraz pozostałe (wykroczenia). Wskazane powyżej przepisy pragmatyczne podmiotów uprawnionych dotyczące pozyskiwania danych telekomunikacyjnych bazują na opisywanym podziale czynów zabronionych i dopuszczają dostęp do nich w celu zapobiegania lub wykrywania przestępstw. Wątpliwości budzi pogląd, że na gruncie polskiego ustawodawstwa pojęcie „poważnej przestępczości" można odnieść do katalogu przestępstw, w odniesieniu do których jest możliwe prowadzenie kontroli operacyjnej, bowiem tego rodzaju przeniesienie rozwiązań na grunt pozyskiwania danych telekomunikacyjnych mogłoby spowodować realny brak możliwości ścigania sprawców niektórych przestępstw, które wprawdzie są zagrożone niższą sankcją, ale ich specyfika uniemożliwia prowadzenie ich w inny sposób, np. niektóre formy stalkingu.

Warto podkreślić, że TK, wydając wyrok z 2014 r., nie wypowiedział się kategorycznie czy niezależna kontrola uzyskiwania danych telekomunikacyjnych powinna mieć charakter uprzedni czy też następczy, pozostawiając tę kwestię do wyważenia ustawodawcy. W związku z powyższym w toku prac nad dostosowaniem obowiązujących wówczas przepisów do tego rozstrzygnięcia wypracowano wariant stanowiący optymalny kompromis między zapewnieniem skuteczności realizacji ustawowych zadań podmiotów uprawnionych do uzyskiwania tego typu danych, a zapewnieniem faktycznej kontroli nad ich uzyskiwaniem. Przyjęty w polskim systemie prawnym model następczej kontroli sądowej jest rozwiązaniem

[51] m.in. w sprawach C-293/12 i C-594/12 (Digital Rights Ireland Ltd), C-203/15 i C-698/15 (Tele2 Sverige AB i in.), C-511/18, C-512/18 i C-520/18 (La Quadrature du Net i in.).

[52] nr 839/2016.

[53] sporządzoną w Rzymie dnia 4 listopada 1950 r., zmienioną następnie Protokołami nr 3, 5 i 8 oraz uzupełnioną Protokołem nr 2 (Dz. U. z 1993 r. Nr 61, poz. 284, z późn. zm.).

optymalnym także z punktu widzenia szybkości działania Policji w przypadku ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych, a w przypadku Służby Ochrony Państwa – dla zapewnienia bezpieczeństwa ochranianym osobom lub obiektom.

W opinii resortu spraw wewnętrznych i administracji, rozważania na temat wprowadzenia uprzedniej kontroli sądowej udostępniania danych telekomunikacyjnych, pocztowych i internetowych wydają się być w obecnych uwarunkowaniach trudne do zrealizowania, w szczególności w kontekście sprawności i szybkości działania podmiotów uprawnionych. Co więcej, wydaje się, że kontrola następcza może być, co do zasady, bardziej dogłębna, a przez to także skuteczniejsza, w stosunku do kontroli uprzedniej. O ile bowiem kontrola uprzednia, w kontekście skali wystąpień o uzyskanie danych, sprowadzałaby się niemal wyłącznie do formalnej kontroli poprawności wypełnienia wniosku, to w przypadku kontroli następczej (prowadzonej wprawdzie nie w odniesieniu do wszystkich spraw, ale odpowiednio dobranych – w oparciu o kryteria określone przez niezależne sądy) jest możliwe szczegółowe sprawdzenie całości okoliczności sprawy, z sięgnięciem do jej materiałów włącznie. Ponadto sprawowanie przez sądy uprzedniej kontroli w stosunku do wszystkich wniosków o udostępnienie danych telekomunikacyjnych może rodzić poważne obawy w kontekście sprawności i skuteczności ścigania przestępstw.

Przepisy polskiego prawa wprawdzie nie przewidują obowiązku informowania osób, wobec których stosowano uprawnienie pozyskiwania danych telekomunikacyjnych, o tym fakcie, jednak należy zauważyć, że funkcjonujące obecnie rozwiązania prawne częściowo spełniają powyższy wymóg informacyjny, bowiem – jak już wyżej wspomniano – podejrzanemu w postępowaniu przygotowawczym przysługuje prawo do końcowego zaznajomienia się z materiałami, co w przypadku włączenia do akt postępowania przygotowawczego materiałów uzyskanych w wyniku dostępu do danych telekomunikacyjnych, w istocie oznacza przekazanie takiej osobie informacji o objęciu jej tym rodzajem czynności.

Opisane powyżej rozwiązania w zakresie uzyskiwania przez podmioty uprawnione dostępu do danych telekomunikacyjnych, a także ich późniejszego wykorzystania bądź zniszczenia, w powiązaniu z zasadami zatrzymywania i niszczenia danych telekomunikacyjnych, określonymi w art. 180a ust. 1 pkt 1 ustawy – *Prawo telekomunikacyjne*, a także obowiązkami w zakresie ich ochrony wynikającymi z art. 180a ust. 1 pkt 3 tej ustawy, stanowią z jednej strony gwarancję ich dostępności wyłącznie dla podmiotów uprawnionych, z drugiej zaś zapobiegają ich nieuprawnionemu wykorzystaniu po przekazaniu przez operatora.

Podkreślenia wymaga, że dane telekomunikacyjne są częstokroć jedynym sposobem uzyskiwania dowodów w przypadku uciążliwych i szkodliwych społecznie przestępstw takich jak np. uporczywe nękanie (stalking), oszustwa internetowe, rozpowszechnianie pornografii dziecięcej czy innych przestępstw popełnianych za pomocą sieci telekomunikacyjnych. Tego rodzaju środek pozwala również na szybką reakcję służb w wypadkach wielu innych dolegliwych przestępstw, jak chociażby kradzieże telefonów.

Wydaje się przy tym niemożliwe wypracowanie jakichkolwiek racjonalnych mechanizmów pozwalających na inne niż masowe zatrzymywanie danych telekomunikacyjnych przez operatorów. Należy bowiem wyjaśnić, że w zdecydowanej większości przypadków punktem wyjścia do podjęcia działań przez Policję jest zdarzenie kryminalne (przestępstwo), a kluczowym elementem tych działań, w szczególności na ich początkowym etapie, jest analiza danych telekomunikacyjnych, pozwalająca na wytypowanie osób, które mogły mieć związek z tymi zdarzeniami. Badanie *ex post* jest więc podstawową formą prowadzenia analizy kryminalnej. Tym samym próby wprowadzenia jakiekolwiek reglamentacji w tym zakresie w znacznym stopniu ograniczą skuteczność działań na rzecz bezpieczeństwa i porządku publicznego.

Warto również podkreślić, że niewątpliwie problematyka kontroli operacyjnej czy retencji danych jest istotna z punktu widzenia ochrony porządku publicznego i bezpieczeństwa państwa. Pozyskiwanie danych przez służby służy zwalczaniu przestępczości, ochronie życia i zdrowia ludzkiego, co nabiera szczególnego znaczenia w kontekście zagrożenia terrorystycznego. Wprowadzenie ewentualnych ograniczeń w zakresie zatrzymywania oraz dostępu do danych telekomunikacyjnych może zatem negatywnie wpłynąć na możliwość pełnego wykorzystania rozwiązań przyjętych w ustawie z dnia 10 czerwca 2016 r. *o działaniach antyterrorystycznych*[54].

Dyrektor DBN w KPRM podkreślił potrzebę funkcjonowania szczególnej postaci kontroli operacyjnej, tzw. czynności przewidzianych do rozpoznawania, zapobiegania i zwalczania przestępstw terrorystycznych. Jest to niewątpliwie szczególna instytucja prawna, której istotą i uzasadnieniem jest jak najszybsze wdrożenie tych czynności w celu zapobiegania aktom terrorystycznym. Jej stosowanie jest przewidziane do wyjątkowych

[54] Dz. U. z 2021 r. poz. 2234, z późn. zm.

sytuacji, kiedy nawet niewielkie opóźnienie mogłoby negatywnie wpłynąć na skuteczność działania mającego na celu zapobieżenie popełnienia przestępstw o charakterze terrorystycznym, odznaczających się bardzo wysokim stopniem społecznej szkodliwości i stanowiącym ogromne zagrożenie zarówno dla życia i zdrowia obywateli, jak i państwa.

Jednocześnie Dyrektor DBN w KPRM wskazał, że w kontekście kompleksowej regulacji instytucji ww. czynności jako zasadna jawi się modyfikacja art. 9 ust. 7 ustawy *o działaniach antyterrorystycznych* i wprowadzenie rozwiązań, w świetle których do Prokuratora Generalnego będą przekazywane wszystkie materiały zgromadzone podczas stosowania czynności tylko w przypadku uzyskania dowodów pozwalających na wszczęcie postępowania karnego lub mających znaczenie dla toczącego się postępowania karnego. W pozostałych przypadkach, tj. w sytuacji zgromadzenia podczas stosowania ww. czynności materiałów, które nie są istotne dla bezpieczeństwa państwa lub nie stanowią informacji potwierdzających zaistnienie przestępstwa, uzyskane materiały powinny podlegać niezwłocznemu, protokolarnemu, komisyjnemu zniszczeniu zarządzanemu przez Szefa ABW.

Kontrola operacyjna i ww. czynności mogą polegać również na uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych. Uwzględniając fakt, że współczesne aparaty telefonii komórkowej, w szczególności typu smartfon, zawierają informatyczne nośniki danych jako swoje części integralne, nie budzi wątpliwości, że obecne uregulowania ustawowe jednoznacznie pozwalają na uzyskiwanie i utrwalanie danych w nich zawartych. Uprawnienie to niewątpliwie umożliwia ingerencję w konstytucyjne prawa i wolności, dlatego też art. 31 ust. 3 Konstytucji RP wymaga unormowania go na poziomie ustawowym, co też zostało wykonane w ustawach pragmatycznych służb specjalnych. Równocześnie uregulowania konstytucyjne, jak trafnie zauważył TK w wyroku TK z 2014 r., nie wymagają, aby ustawa określała w sposób wyczerpujący metody lub środki (a więc również oprogramowanie), dzięki którym jest możliwe skuteczne przeprowadzenie danej, dopuszczalnej prawem postaci kontroli operacyjnej. W tej kwestii TK stwierdził[55], że *niezbędne jest sprecyzowanie sposobu niejawnego wkroczenia w sferę prywatności jednostki. Nie jest przy tym konieczne wskazanie w przepisach prawa konkretnych środków techniki operacyjnej ani tym bardziej zdefiniowanie ich parametrów.* Uzasadniając to stanowisko, TK dostrzegł niezwykle dynamiczny rozwój sposobów komunikowania się, który jest związany z wykorzystywaniem coraz to nowych kanałów i narzędzi komunikacyjnych: *w dobie rozwoju technologicznego, wielości form popełniania przestępstw i kanałów komunikowania się przestępców nie wydaje się realne stworzenie zamkniętego katalogu środków technicznych, które mogą być stosowane w celu uzasadnionego konstytucyjnie niejawnego pozyskiwania informacji, bez uszczerbku dla efektywnej walki z zagrożeniami czy dekonspiracji działalności operacyjnej.*

W oparciu o przywołane fragmenty wyroku TK z 2014 r. należy potwierdzić, że uprawnione służby państwowe mają uprawnienie m.in. do uzyskiwania danych zawartych w informatycznych nośnikach danych. Równocześnie TK nie zobowiązał tych służb do wskazywania konkretnych metod, środków, narzędzi, programów itd. jakie są wykorzystywane przez nie do realizacji opisanej wyżej kompetencji. W związku z tym, z punktu widzenia standardów konstytucyjnych, których respektowanie warunkuje legalność kontroli operacyjnej, stosowanie konkretnego programu lub narzędzia informatycznego, w celu przeprowadzenia prawnie dopuszczalnej postaci kontroli operacyjnej, jest indyferentne.

Równocześnie, bazując na doświadczeniach związanych z przedłużaniem stosowanych kontroli operacyjnych (co jest powiązane z zapoznawaniem się i analizą materiału uzyskanego w wyniku kontroli), należy podkreślić, że umożliwienie uzyskiwania i utrwalania danych zawartych w informatycznych nośnikach danych w dobie obecnego rozwoju technologicznego jest rozwiązaniem nie tylko merytorycznie zasadnym, ale nawet koniecznym. Zaobserwować można, że osoby podejrzewane o zachowania wyczerpujące znamiona czynów zabronionych do komunikacji używają zaawansowanych środków technicznych wykraczających poza tradycyjne prowadzenie rozmów głosowych przy użyciu sieci telekomunikacyjnych. W ostatnich latach zwiększa się częstotliwość używania szyfrowanych komunikatorów internetowych, a istotne z punktu widzenia bezpieczeństwa państwa i jego obywateli dane rutynowo zaczynają być gromadzone i przechowywane w tzw. chmurach internetowych. Uwzględniając to, że jednym z fundamentalnych obowiązków państwa, wynikającym wprost z art. 5 Konstytucji RP, jest zapewnienie bezpieczeństwa obywateli, ustawodawca jest zobowiązany wyposażyć właściwe organy państwa w narzędzia umożliwiające realne i efektywne zwalczanie przestępczości. Spełnienie tego wymogu zapewnia kontrola operacyjna możliwa

[55] Pkt 5.1.3.2 wyroku TK z 2014 r.

do przeprowadzenia w różnych postaciach i za pomocą różnych środków, a w efekcie pozwalająca na pozyskiwanie szerokiego katalogu informacji.

Publicznie podniesione zagadnienie możliwości kontroli operacyjnej aparatów telefonii komórkowej (mobilnej), które są telekomunikacyjnymi urządzeniami końcowymi, w kontekście wątpliwości wyrażanych w wystąpieniu Pana Rzecznika (w tym przywołanej w nim literatury), wymaga stwierdzenia, że formy tej kontroli są enumeratywnie i szczegółowo opisane w ustawach regulujących funkcjonowanie podmiotów uprawnionych do prowadzenia kontroli operacyjnej. W każdej z tych ustaw jest mowa o tym, że niejawnie prowadzona kontrola operacyjna może polegać m.in. na uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych.

„Uzyskiwanie" oznacza otrzymywanie czegoś, co było przedmiotem starań, a „utrwalanie" polega na zarejestrowaniu jakiejś treści w pamięci komputera w celu jej późniejszego odtworzenia[56]. Pozostałe części składowe opisujące tę formę kontroli operacyjnej zdefiniowano w Konwencji Rady Europy *o cyberprzestępczości,* sporządzonej w Budapeszcie dnia 23 listopada 2001 r.[57], ustawie – *Prawo telekomunikacyjne* oraz ustawie z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne*[58].

Zgodnie z art. 1 lit. b) ww. konwencji „dane informatyczne" oznaczają dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny. Z kolei „system informatyczny", w myśl art. 1 lit. a) ww. konwencji, oznacza każde urządzenie lub grupę wzajemnie połączonych lub związanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, wykonuje automatyczne przetwarzanie danych, zaś „system teleinformatyczny", zgodnie z art. 3 pkt 3 ustawy *o informatyzacji działalności podmiotów realizujących zadania publiczne*, to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy – *Prawo telekomunikacyjne*. Mamy zatem do czynienia z zapisem określonej informacji przechowywanej na dysku lub na innym nośniku informacji, np. w smartfonie lub laptopie. Dane są składowane i przetwarzane w informatycznych nośnikach danych, a więc urządzeniach służących do zapisywania, przechowywania i odczytywania obiektów w postaci cyfrowej. Z kolei telekomunikacyjne urządzenia końcowe są podłączone do zakończeń sieci, co umożliwia abonentowi korzystanie poprzez odpowiednie łącza (przewodowe lub bezprzewodowe) z przekazów telekomunikacyjnych.

Z powyższego wynika, że jedna z dopuszczalnych form pracy operacyjnej może obejmować zdalne uzyskiwanie i rejestrację informacji zawartych w różnego rodzaju elektronicznych urządzeniach końcowych (np. smartfonach) użytkowanych przez osobę pozostającą w zainteresowaniu służb, w celu późniejszego ich odtworzenia i analizy.

Forma kontroli operacyjnej ukierunkowanej na „urządzenie końcowe" została wprowadzona *expressis verbis* wspomnianą już ustawą z dnia 15 stycznia 2016 r. *o zmianie ustawy o Policji oraz niektórych innych ustaw* i realizowała orzeczenie TK z 2014 r. Warto przy tym zauważyć, że postulaty jej dopuszczenia pojawiły się już wcześniej m.in. propozycję definicji kontroli operacyjnej obejmującej „urządzenie końcowe" przedstawił np. zespół ds. zmian legislacyjnych wynikających z wyroku Trybunału Konstytucyjnego K 23/11 z dnia 30 lipca 2014 r., powołany decyzją przewodniczącego Kolegium do Spraw Służb Specjalnych z dnia 8 października 2014 r.

Kontrola operacyjna urządzenia końcowego nie jest środkiem nadzwyczajnym wśród czynności operacyjnych stosowanych przez służby państwowe na całym świecie i wynika z dostosowywania form pracy operacyjnej do realiów „cyfrowego świata". Przepisy obowiązujące w Niemczech przyznają np. służbom prawo wykorzystywania oprogramowania do przełamywania zabezpieczeń telefonów i komputerów oraz odczytywania zawartości urządzeń użytkowanych przez osoby, którym oficjalnie nie postawiono zarzutów, ale są podejrzewane o popełnienie przestępstwa. Narzędzia takie są nazywane „*Staatstrojanern*", czyli „trojanami państwowymi" i stosowane do szerszej grupy przestępstw, aniżeli tylko terrorystyczne.

W aktach konkretnych spraw dotyczących wyrażania przez sąd zgód na prowadzenie kontroli w formie uzyskiwania i utrwalania danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych

[56] Zob. np. internetowy słownik języka polskiego PWN.

[57] Dz. U. z 2015 r. poz. 728.

[58] Dz. U. z 2021 r. poz. 2070, z późn. zm.

urządzeniach końcowych, systemach informatycznych i teleinformatycznych, sędzia, wraz z wnioskiem o zarządzenie albo przedłużenie kontroli operacyjnej, otrzymuje szczegółowe materiały uzasadniające potrzebę zastosowania kontroli. We wniosku o zarządzenie kontroli podaje się natomiast m.in. dane osobowe, ustawowy opis formy kontroli i podstawę prawną stosowania kontroli. Ponadto, we wnioskach o przedłużenie stosowania kontroli operacyjnej przytacza się wprost lub opisuje informacje uzyskane z urządzenia końcowego, zatem sąd rozpatrujący wniosek ma świadomość, skąd pochodzą informacje oraz jak zostały uzyskane. Wobec tego sugestie, jakoby sędzia zarządzający lub przedłużający kontrolę nie wiedział jakiej formy ona dotyczy, godzą w powagę urzędu sędziowskiego, tym bardziej, że sędzia ma ustawowy obowiązek zapoznania się z materiałami zgromadzonymi w toku prowadzonej kontroli.

Natomiast podmioty uprawnione, wnioskujące o prowadzenie kontroli operacyjnej, mają obowiązek chronić środki, formy i metody realizowanych zadań. Dlatego szczegółowe kwestie techniczne związane z wdrożeniem kontroli operacyjnej nie są i nie mogą być przedmiotem wniosku o jej zarządzenie. Wprawdzie przepisy nakładają na określone podmioty obowiązek zapewnienia „warunków technicznych i organizacyjnych" umożliwiających prowadzenie kontroli operacyjnej, ale skorzystanie z nich jest fakultatywne i służby mają prawo realizować kontrolę własnymi środkami techniczno-logistycznymi[59].

W swoim wystąpieniu Pan Rzecznik odwołał się również do wyroku TK z dnia 12 grudnia 2005 r.[60] przywołując elementy, jakie powinna zawierać ustawowa regulacja kontroli operacyjnej, tak aby były spełnione standardy konstytucyjne. Analiza obowiązujących ustaw prowadzi do wniosku, że wymogi te są spełnione: przywołane przepisy określają warunki oraz tryb zarządzenia i przedłużania kontroli operacyjnej, przewidując w nim udział i kontrolę ze strony Prokuratora Generalnego i rozstrzygają jednocześnie, że podmiotem decydującym o zastosowaniu tej metody jest niezawisły sąd. Regulacja kontroli operacyjnej, ujęta w ustawach pragmatycznych służb wyznacza także katalog przestępstw, celem ścigania których jest dopuszczalne stosowanie kontroli, okresy jej stosowania, oraz sposób postępowania z materiałami uzyskanymi w wyniku jej stosowania (np. obowiązek przekazania całości materiałów w przypadku uzyskania dowodów pozwalających na wszczęcie postępowania lub mających znaczenie dla toczącego się postępowania karnego). Zrealizowano również *gros* wskazań TK wyrażonych w wyroku TK z 2014 r., przewidując precyzyjną regulację w zakresie postępowania z materiałami uzyskanymi w wyniku kontroli, zawierającymi informacje związane z wykonywaniem zawodu lub funkcji. Przywołane przepisy odsyłają do rozwiązań zawartych w ustawie – *Kodeks postępowania karnego* i w sposób wystarczający i wyważony chronią ww. tajemnice. Przepisy te wprost także uzależniają zastosowanie kontroli operacyjnej od spełnienia warunku subsydiarności, co powoduje, że analizowana metoda pracy operacyjnej ma charakter *ultima ratio*. Równocześnie stosowanie czynności z art. 9 ustawy *o działaniach antyterrorystycznych* jest dopuszczalne tylko w sytuacjach nadzwyczajnych, wymagających wręcz natychmiastowej reakcji; pozwala to przyjąć, że także ta forma kontroli odznacza się charakterem *ultima ratio*.

Odnosząc wymogi sformułowane przez ETPCz do czynów zabronionych, co do których rozpoznawania, zapobiegania i zwalczania właściwe są służby specjalne, Dyrektor DBN w KPRM wskazał, że wiele z tych czynów jest realizowanych w ramach zorganizowanych grup przestępczych, organizacji terrorystycznych lub przez albo przy współudziale obcych służb specjalnych. Działania te są więc prowadzone w warunkach szczególnej konspiracji oraz (zwłaszcza w odniesieniu do przestępstwa szpiegostwa oraz przestępstw o charakterze terrorystycznym) przez dłuższy czas. W takich sytuacjach nierzadko kontrola operacyjna nie jest prowadzona w sposób ciągły, lecz, w zależności od potrzeb operacyjnych, po przerwaniu jest wznawiana. Poinformowanie osób o fakcie stosowania wobec nich kontroli operacyjnej uczyniłoby późniejsze wznowienie zupełnie nieskutecznym, co niewątpliwie negatywnie odbiłoby się na możliwości osiągnięcia celów prowadzonych procedur operacyjnych, a w konsekwencji ochronie dóbr, której ma służyć prowadzona w ich ramach praca operacyjna. Fakt informowania o kontroli operacyjnej nie przyczyni się do przerwania działalności przestępczej lub zagrażającej bezpieczeństwu państwa, a jedynie do jej większego zakonspirowania. Powyższe okoliczności powodują, że ujawnienie informacji o prowadzonych czynnościach operacyjnych jest rozwiązaniem nieproporcjonalnym i jawi się jako wyraz nadmiernej i nieuzasadnionej preferencji prawa do prywatności ze szkodą dla innych praw i wolności oraz obowiązków, które państwo musi wyważyć. W tym kontekście należy podnieść, że ETPCz wielokrotnie orzekał, że pozytywne obowiązki państwa wynikające z art. 3 i 8 Europejskiej Konwencji Praw Człowieka (zakaz tortur i prawo do prywatności), którym odpowiadają gwarancje zawarte

[59] Paweł Opitek. *Kontrola telefonu za pomocą Pegasusa,* „Rzeczpospolita". 21 stycznia 2022 r.
[60] sygn. akt K 32/04.

w art. 4 i 7 Karty Praw Podstawowych Unii Europejskiej[61], oznaczają w szczególności przyjęcie przepisów materialnych i proceduralnych oraz środków praktycznych pozwalających na skuteczne zwalczanie przestępstw przeciwko osobom w drodze dochodzenia i skutecznego ścigania. Do przywołanej linii orzeczniczej nawiązał również TSUE we wskazanym przez Pana Rzecznika wyroku C-511/18, *La Quadrature du Net i in. przeciwko Premier ministre i in*.

Dyrektor DBN w KPRM zauważył, że pozyskiwanie tzw. danych telekomunikacyjnych, pocztowych i internetowych to instytucja prawna stanowiąca podstawowy i nieodzowny element pracy operacyjnej, niemniej diametralnie odmienna od kontroli operacyjnej. Tymczasem można odnieść wrażenie, że Pan Rzecznik je utożsamia, sugerując odwoływanie się do wyroku ETPCz w sprawie *Zakharov przeciwko Rosji*. Ta tendencja daje się także zauważyć w orzecznictwie TSUE[62], co prowadzi do bezzasadnego rozszerzenia standardów dotyczących kontroli operacyjnej na pozyskiwanie ww. danych. Warto odnotować, że osoba, która chce korzystać z określonych usług, dobrowolnie godzi się na podanie szeregu danych niezbędnych usługodawcy do realizacji świadczenia, dodatkowo samo korzystanie z zamówionych usług generuje kolejne informacje, które również automatycznie są gromadzone przez usługodawcę. Zbieranie tych danych przez usługodawcę wynikające z dobrowolnej decyzji osoby i istoty świadczonych usług nie budzi, co do zasady, wątpliwości zainteresowanych, którzy zapewne traktują je jako konieczną cenę korzystania z nowoczesnych rozwiązań komunikacyjnych. Również Pan Rzecznik w swoim wystąpieniu nie zgłosił do opisanej praktyki żadnych uwag i to mimo faktu, że nierzadko podmioty świadczące usługi internetowe to podmioty zagraniczne, o niejasnej strukturze kapitałowej, wykorzystujące do świadczenia usług serwery w zagranicznych, często egzotycznych lokalizacjach nieobjętych specjalnymi rygorami ochrony danych osobowych, co powoduje, że bardzo często osoba, która przekazuje swoje dane, nie ma żadnej wiedzy i wpływu, jak i gdzie są one przetwarzane i wykorzystywane. W tym kontekście podnoszenie tak istotnych zastrzeżeń co do faktu korzystania z ww. danych przez uprawnione instytucje państwowe, w oparciu o ustawowo opisane procedury i w celu realizacji ustawowych zadań ukierunkowanych wyłącznie na realizację art. 5 Konstytucji RP stanowiącego, że RP zapewnia bezpieczeństwo swoich obywateli, a w konsekwencji domaganie się, by na korzystanie z ww. danych były nałożone rygory analogiczne jak przy kontroli operacyjnej, według Dyrektora DBN w KPRM jawi się jako nieuzasadnione i aksjologicznie niespójne.

Analiza wyroku C-511/18, *La Quadrature du Net i in. przeciwko Premier ministre i in.* prowadzi do wniosku, że TSUE dopuszcza przepisy, które zezwalają właściwym organom państwa na nakazanie dostawcom usług łączności elektronicznej zatrzymywania danych o ruchu i danych o lokalizacji wszystkich użytkowników środków łączności elektronicznej w ograniczonym okresie, o ile występują wystarczająco konkretne okoliczności, które pozwalają na uznanie, że w danym państwie członkowskim istnieje poważne zagrożenie dla bezpieczeństwa narodowego, które jest rzeczywiste i aktualne lub przewidywalne. Regulacje zezwalające na zatrzymanie, gromadzenie i przetwarzanie danych telekomunikacyjnych, pocztowych i internetowych muszą oczywiście spełnić wymóg proporcjonalności, tj. muszą istnieć jasne i precyzyjne przepisy regulujące zakres i sposób stosowania rozpatrywanego środka oraz ustanawiające minimalne wymogi służące temu, aby osoby, o których dane osobowe chodzi, miały wystarczające gwarancje pozwalające na skuteczną ochronę tych danych przed ryzykiem nadużyć.

Należy także przypomnieć, że na gruncie postępowania karnego art. 218 ustawy – *Kodeks postępowania karnego,* regulujący dostęp do bilingów w toku postępowania przygotowawczego, został umieszczony w rozdziale 25 tej ustawy, mówiącym o przeszukaniu i zatrzymaniu rzeczy, a nie w rozdziale 26 dotyczącym kontroli i utrwalania rozmów. Nie ulega wątpliwości, że przepisy rozdziału 25 stawiają znacznie niższe wymagania proceduralne odnośnie uzyskiwania dowodów niż przepisy rozdziału 26. Zgodnie z art. 218 ww. ustawy, dane telekomunikacyjne wydaje się na żądanie prokuratora, podczas gdy, stosownie do art. 237, na zarządzenie kontroli rozmów telefonicznych prokurator potrzebuje zgody sądu.

Według Dyrektora DBN w KPRM ponownie wymaga zaakcentowania, że uzyskiwanie danych telekomunikacyjnych, pocztowych i internetowych stanowi, w przeciwieństwie do kontroli operacyjnej, podstawowy i konieczny element w pracy operacyjnej, a uzyskana w ten sposób wiedza służy np. do weryfikacji potrzeby stosowania kontroli operacyjnej, a także jest wykorzystywana w uzasadnieniu wniosków o tę kontrolę. Pozyskiwanie ww. danych jest niezbędne do rozpoznania szeregu przestępstw, szczególnie tych popełnianych w ramach zorganizowanych grup przestępczych i terrorystycznych oraz szpiegostwa. Z tych

[61] Dz. Urz. UE C 303 z 14.12.2007, str. 1, z późn. zm.

[62] Wyrok TSUE z dnia 8 kwietnia 2014 r. w sprawach połączonych: Digital Rights Ireland Ltd (C-293/12) oraz Karntner Landesregierung i in. (C-594/12) przeciwko Minister for Communications i in.

powodów uzyskiwanie wspomnianych danych, w przeciwieństwie do kontroli operacyjnej, nie jest i nie może być uzależnione od spełnienia przesłanki subsydiarności, tym bardziej, że warunek taki nie wypływa z Konstytucji RP. Wprowadzenie wymogu, jak tego domaga się Pan Rzecznik, by uzyskanie danych telekomunikacyjnych, pocztowych i internetowych było uzależnione od uprzedniej decyzji sądu, doprowadziłoby do paraliżu pracy operacyjnej i bardzo negatywnie wpłynęłoby na skuteczność i efektywność realizowanych operacji[63]. To ostatnie ryzyko w sytuacji pogarszającej się sytuacji międzynarodowej, która skutkuje m.in. istotnym zintensyfikowaniem aktywności w RP wrogich służb specjalnych, jak i znacznym zwiększeniem zagrożenia terrorystycznego, będącego pochodną napływu uchodźców z kolejnych zdestabilizowanych państw, jest szczególnie groźne.

Wobec powyższego, oceniając regulacje dotyczące służb specjalnych w kontekście znaczenia realizacji przez nie zadań ustawowych dla urzeczywistnienia konstytucyjnego zadania ochrony bezpieczeństwa państwa oraz bezpieczeństwa obywateli, należy uznać, że pobieranie przez te służby danych telekomunikacyjnych, pocztowych i internetowych oraz warunkujący tę czynność obowiązek retencji ww. danych, spełniają tzw. test proporcjonalności zawarty w art. 31 ust. 3 Konstytucji RP. Trzeba przy tym zaznaczyć brak uzasadnienia dla konieczności obwarowania pozyskiwania danych telekomunikacyjnych, pocztowych i internetowych dodatkowymi obowiązkami w postaci uprzedniej zgody sądu oraz informowania osoby, której dane pobrano, o tym fakcie.

Wprowadzanie arbitralnych ograniczeń w zakresie stosowania określonych metod pracy operacyjnej, wyłącznie w oparciu o teoretyczne rozważania na temat potencjalnych możliwości naruszenia praw obywateli przez organy państwowe, wydaje się nierozważne i nie bierze pod uwagę innych dostępnych metod gwarantowania legalizmu ich wykorzystywania. Może to skutkować zamknięciem służbom i instytucjom odpowiedzialnym za ochronę porządku publicznego i bezpieczeństwa państwa dostępu do określonych informacji, które mogą okazać się niezbędne do prawidłowej realizacji ich zadań, a w konsekwencji prowadzić do zagrożenia zdrowia i życia obywateli (np. w odniesieniu do zagrożeń natury terrorystycznej).

W rozważaniach nad poziomem ingerencji w prawo do prywatności, w kontekście wykorzystywania analizowanych metod pracy operacyjnej, należy w pierwszej kolejności brać pod uwagę wartości, których ochrona jest celem stosowania wspomnianych czynności. Ograniczenie stosowania wspomnianych metod pracy operacyjnej do rozpoznawania, zapobiegania i zwalczania tzw. poważnych przestępstw, w szczególności godzących w bezpieczeństwo wewnętrzne państwa oraz zdrowie i życie jego obywateli, wydaje się dostatecznym uzasadnieniem dla ich wykorzystywania i zabezpiecza obywateli przed nadmierną ingerencją w ich prawa i wolności. Natomiast sukcesywnie rozbudowywane mechanizmy kontroli i nadzoru prowadzenia czynności operacyjno-rozpoznawczych (zarówno przewidziane w przepisach powszechnie obowiązujących, jak i w wewnętrznych regulacjach poszczególnych służb) w dostatecznym stopniu gwarantują legalizm i rozliczalność stosowania analizowanych metod pracy operacyjnej, zapewniając zarówno wymóg autoryzacji pozyskiwania danych telekomunikacyjnych, pocztowych i internetowych, jak i określenie odpowiedzialnych w przypadku wystąpienia nadużyć w tym względzie. Wprowadzenie rozwiązań postulowanych przez Pana Rzecznika w postaci ograniczenia dostępu służb do danych telekomunikacyjnych, pocztowych i internetowych, wdrożenia obowiązku notyfikacji (powiadamiania obywatela o fakcie pozyskania przez służbę jego danych) czy też ograniczenia instrumentów służących realizacji zadań (np. zakazu wykorzystywania określonego oprogramowania) w sposób negatywny wpłynęłoby na skuteczność prowadzonych przez uprawnione służby działań operacyjnych.

Szef KAS wskazał, że przepisy ustawy o KAS w zakresie kontroli operacyjnej zostały przeniesione i dostosowane z ustawy z 28 września 1991 r. *o kontroli skarbowej*[64], uchylonej ustawą z 16 listopada 2016 r. – *Przepisy wprowadzające ustawę o Krajowej Administracji Skarbowej*[65]. Artykuł 36c ustawy *o kontroli skarbowej* (dotyczący kontroli operacyjnej stosowanej przez wywiad skarbowy) był przedmiotem badania przez TK, który w wyroku z dnia 20 czerwca 2005 r. w sprawie sygn. K 4/04, nie zakwestionował jego konstytucyjności. Trybunał Konstytucyjny uznał, że ustawa *o kontroli skarbowej* ściśle określa sytuacje, które uzasadniają przeprowadzenie kontroli operacyjnej, *a ich charakter wskazuje na istnienie konieczności zastosowania tego rodzaju ograniczeń. Skoro bowiem ustawodawca nakłada na organy kontroli skarbowej zadania polegające na rozpoznaniu i ujawnieniu przestępstw i wykroczeń w niej określonych oraz zapobieganiu*

[63] Dla przykładu, aby przeciwdziałać zagrożeniom ze strony osób o inklinacjach terrorystycznych, należy wcześniej pozyskać wiedzę o ich planach, kontaktach, powiązaniach.

[64] Dz. U. z 2016 r. poz. 720, z późn. zm. – akt utracił moc.

[65] Dz. U. poz. 1948, z późn. zm.

im (art. 3 ust. 4 i 5 ustawy), to organy te muszą być wyposażone w instrumenty prawne pozwalające na wykonanie tych zadań. Ustawa szczegółowo reguluje procedurę związaną z przeprowadzeniem kontroli operacyjnej, dopuszczalny czas jej trwania i sposób postępowania z materiałami uzyskanymi w jej wyniku. Kontrola operacyjna zarządzana jest przy tym przez sąd, a to oznacza istnienie gwarancji ochrony praw człowieka. Warto zwrócić uwagę, że Generalny Inspektor Kontroli Skarbowej przedstawia corocznie Sejmowi i Senatowi informację o działalności określonej w art. 36-36d ustawy o kontroli skarbowej (art. 36l ustawy). Jednocześnie w ww. wyroku Trybunał uznał, że przyjęte przez ustawodawcę rozwiązania odpowiadają wymogom formalnym zdefiniowanym w art. 8 ust. 2 Europejskiej Konwencji Praw Człowieka. Jak zauważył ETPCz w wyroku z dnia 4 maja 2000 r. w sprawie Rotaru przeciwko Rumunii, skarga nr 28341/95: *Aby systemy niejawnej inwigilacji były zgodne z art. 8 Konwencji, muszą one zawierać gwarancje prawne stosowane do kontroli działań właściwych służb. Procedury kontrolne muszą odpowiadać wartościom demokratycznego społeczeństwa tak wiernie, jak to możliwe, a w szczególności zasadzie praworządności, która jest w sposób wyraźny przywołana w preambule do Konwencji. Zasada rządów prawa zakłada, między innymi, iż ingerencja ze strony organów władzy wykonawczej w prawa jednostki powinna być przedmiotem skutecznej kontroli, która w normalnych warunkach powinna być przeprowadzona przynajmniej przez organy sądowe, jako że kontrola sądowa zapewnia najlepszą gwarancję niezależności, bezstronności oraz stosowania właściwej procedury.* Wszystkie te kryteria wypełnia, zdaniem TK, art. 36c ustawy *o kontroli skarbowej*. Ponadto Generalny Inspektor Kontroli Skarbowej informuje Prokuratora Generalnego o wynikach kontroli operacyjnej po jej zakończeniu, a na jego żądanie również o przebiegu tej kontroli, przedstawiając zebrane w jej toku materiały. Obecnie wszystkie te uregulowania zostały przeniesione do ustawy o KAS, w związku z powyższym nie ma podstaw prawnych, aby je ponownie analizować a tym bardziej kwestionować, w związku z tym stanowisko TK wskazane wyżej pozostaje aktualne na gruncie przepisów ustawy o KAS.

Wprowadzenie omawianych regulacji do ustawy o KAS miało służyć i służy przede wszystkim zwalczaniu oszustw podatkowych i celnych, przynoszących ogromne straty dla budżetu państwa, takich jak wyłudzanie nienależnego zwrotu podatku VAT (karuzele podatkowe) oraz związanych z obrotem towarowym z zagranicą dotyczących uszczuplania należności celnych i podatkowych. Wspomniane zjawiska przestępczości skarbowej i celnej (zwłaszcza wyłudzenia podatku VAT na ogromną skalę), ale również przestępczości korupcyjnej, bez wątpienia stanowią istotne zagrożenie dla bezpieczeństwa finansowego państwa oraz porządku publicznego. Z tego też powodu wykonywane przez funkcjonariuszy Służby Celno-Skarbowej czynności operacyjno-rozpoznawcze należy uznać, w świetle wspomnianych norm konstytucyjnych, za środki proporcjonalne służące zwalczaniu tego rodzaju przestępczości, a obowiązujące w tym zakresie przepisy ustawy o KAS za zgodne z Konstytucją RP.

Szef KAS wskazał, że obowiązujące przepisy ustawy o KAS precyzyjnie określają warunki ingerencji władzy państwowej w prawa obywatelskie, ponieważ w zadawalającym stopniu regulują katalog przestępstw, co do których jest dopuszczalne zarządzenie kontroli operacyjnej, a w związku z tym jednoznacznie określają katalog osób, w stosunku do których może być zarządzona kontrola operacyjna, określają czas jej trwania, wskazują organy kontrolujące zarządzenie i przebieg kontroli, zasady przekazywania i niszczenia materiałów. Dają więc obywatelom odpowiednie wskazówki co do wymogów, warunków i okoliczności, w których władze publiczne są uprawnione do korzystania z czynności operacyjnych, co oznacza, że przepisy ustawy o KAS odpowiadają gwarancjom wskazywanym przez TK, ETPCz i TSUE. Analogicznie jest w przypadku pozyskiwania danych telekomunikacyjnych (w tym internetowych), gdzie określono podstawy prawne wystąpienia o te dane, ich rodzaj, sposoby udostępniania oraz nałożono na podmiot występujący obowiązek prowadzenia rejestru, w którym szczegółowo wskazuje się kto, kiedy, po co i jakie dane pozyskał. Kontrolę w tym zakresie powierzono z kolei sądowi okręgowemu, który może ją przeprowadzić w każdym czasie i nie polega jedynie na analizie sprawozdań, lecz ma szerszy charakter.

Z powyższych względów wniosek Pana Rzecznika, zawarty we wspomnianym na wstępie piśmie z 13 stycznia 2022 r., dotyczący podjęcia pilnych działań mających na celu dostosowanie obowiązujących przepisów regulujących zakres czynności operacyjno-rozpoznawczych do standardów konstytucyjnych oraz europejskich wydaje się być nieuzasadniony.

Obowiązujące w Polsce uregulowania prawne w zakresie czynności operacyjno-rozpoznawczych, w tym stosowania kontroli operacyjnej oraz uzyskiwania danych telekomunikacyjnych, nie wymagają zmiany w kontekście wątpliwości podniesionych w ww. wystąpieniu Pana Rzecznika.

Z kolei odnosząc się do zagadnień poruszonych w piśmie Pana Rzecznika z 13 lipca 2022 r., w ocenie resortu spraw wewnętrznych i administracji zaproponowane rozwiązania w ramach art. 47 i art. 49 projektu

ustawy – *Prawo komunikacji elektronicznej*[66] są właściwe i uzasadnione z punktu widzenia służb odpowiedzialnych za rozpoznawanie, zapobieganie i wykrywanie przestępstw. Wejście w życie tych regulacji umożliwi skuteczną realizację ustawowych zadań nałożonych na poszczególne służby. Będzie stanowić również swego rodzaju przeciwwagę dla przestępczości wykorzystującej coraz częściej zdobycze nowoczesnej technologii. Ponadto stosowanie różnego rodzaju mechanizmów anonimizujących działalność przestępczą wymaga wprowadzenia rozwiązań prawnych, które w realny sposób pozwolą na identyfikację i ściganie sprawców. Rozszerzenie zakresu danych objętych obowiązkiem retencji, o których mowa w art. 49 ust. 1 pkt 2 projektu PKE, będzie zatem stanowić istotne narzędzie w walce z przestępczością występującą w cyberprzestrzeni.

Należy także zaznaczyć, że uzyskiwanie i wykorzystanie przez podmioty uprawnione danych, o których mowa w art. 47 i art. 49 projektu PKE, będzie podlegać rygorom wynikającym z ustaw pragmatycznych. Fakt uzyskania tych danych będzie miał swoje odzwierciedlenie w rejestrze wystąpień o uzyskanie danych telekomunikacyjnych, pocztowych i internetowych, zawierającym informacje identyfikujące jednostkę organizacyjną i funkcjonariusza uzyskującego te dane, ich rodzaj, cel uzyskania oraz czas, w którym zostały uzyskane. Nadal ich wykorzystanie będzie również podlegać ustawowo określonym trybom postępowania, w zależności od znaczenia tych danych dla postępowania karnego (będą przekazywane prokuratorowi albo niezwłocznie, komisyjnie i protokolarnie niszczone). Co istotne, uzyskiwanie tego rodzaju danych w dalszym ciągu będzie podlegać kontroli sądowej.

W opinii resortu spraw wewnętrznych i administracji nie zachodzi potrzeba wprowadzania w projekcie PKE postulatów podniesionych przez Pana Rzecznika. Zasady działania służb nie ulegną zmianie i będzie obowiązywał podobny model postępowania przy uzyskiwaniu danych telekomunikacyjnych, internetowych i pocztowych. Natomiast wejście w życie art. 47 i art. 49 projektu PKE pozwoli na skuteczniejszą reakcję na przestępczość związaną z funkcjonowaniem sieci Internet.

W kwestii poruszonego przez Pana Rzecznika wyroku TSUE z dnia 5 kwietnia 2022 r. w sprawie C-140/20, należy podkreślić, że wykorzystanie danych telekomunikacyjnych stanowi dla organów ścigania jedno z podstawowych narzędzi utrzymania wysokiego poziomu bezpieczeństwa. Dane te są również częstokroć jedynym sposobem uzyskiwania dowodów w przypadku uciążliwych i szkodliwych społecznie przestępstw takich jak na przykład uporczywe nękanie (stalking), oszustwa internetowe, rozpowszechnianie pornografii dziecięcej czy innych przestępstw popełnianych za pomocą sieci telekomunikacyjnych. Tego rodzaju środek pozwala również na szybką reakcję służb w wypadkach wielu innych dolegliwych przestępstw, jak chociażby kradzieże telefonów. Ze względu na dominujący model analizy kryminalnej oparty na analizie danych *ex post*, w zdecydowanej większości przypadków podstawową przyczyną sięgania przez uprawnione podmioty po dane telekomunikacyjne jest zaistnienie zdarzenia kryminalnego lub aktu terroru. Co istotne, służby nie posiadają uprawnień do pozyskiwania tzw. metadanych w sprawach o wykroczenia.

Zmiany w ustawach pragmatycznych Policji, Straży Granicznej i Służby Ochrony Państwa w analizowanym obszarze, wynikające z projektu ustawy *Przepisy wprowadzające ustawę – Prawo komunikacji elektronicznej*, będą miały wyłącznie dostosowawczy charakter.

Z poważaniem

z up. Maciej Wąsik
Sekretarz Stanu
Ministerstwo Spraw Wewnętrznych i Administracji
/podpisano kwalifikowanym podpisem elektronicznym/

Do wiadomości:
Kancelaria Prezesa Rady Ministrów.

[66] Zwanego dalej: „projektem PKE".