Minister
Spraw Wewnętrznych
i Administracji

BMP-0790-6-1/2021/JS

Pan
Marcin Wiącek
Rzecznik Praw Obywatelskich

Szanowny Panie Rzeczniku,

w odpowiedzi na wystąpienie[1] dotyczące *wykorzystywania danych telekomunikacyjnych przez Policję i służby specjalne* uprzejmie przedstawiam, co następuje.

Na wstępie należy wskazać, że ustawa z dnia 15 stycznia 2016 r. *o zmianie ustawy o Policji oraz niektórych innych ustaw*[2], zwana dalej *„ustawą nowelizującą"*, miała na celu realizację wyroku Trybunału Konstytucyjnego (TK) z dnia 30 lipca 2014 r., sygn. K 23/11, dotyczącego prowadzenia przez służby mundurowe, służby specjalne i właściwe organy kontroli operacyjnej oraz uzyskiwania i przetwarzania przez wskazane podmioty danych telekomunikacyjnych.

W treści ww. wyroku TK stwierdził, że art. 20c ust. 1 ustawy z dnia 6 kwietnia 1990 r. *o Policji*[3] oraz art. 10b ust. 1 ustawy z dnia 12 października 1990 r. *o Straży Granicznej*[4] przez to, że nie przewidują niezależnej kontroli udostępnienia danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. *Prawo telekomunikacyjne*[5] są niezgodne z art. 47 i art. 49 w związku z art. 31 ust. 3 *Konstytucji RP*.

W ocenie TK jednym z wymagań, jakie powinny spełniać przepisy ustawowe upoważniające do pozyskiwania danych telekomunikacyjnych, jest wykreowanie mechanizmu niezależnej kontroli. TK nie wskazuje jednak, jak ma wyglądać procedura dostępu do danych telekomunikacyjnych, w szczególności, czy konieczne ma być w odniesieniu do każdego rodzaju zatrzymywanych danych uzyskanie zgody na ich udostępnienie. Nie wszystkie informacje powodują taką samą intensywność ingerencji w wolności i prawa człowieka. Zdaniem TK, nie jest wobec tego wykluczone, w odniesieniu do udostępniania danych telekomunikacyjnych w toku czynności operacyjno-rozpoznawczych wprowadzenie, jako zasady, kontroli następczej.

Zgodnie ze znowelizowanymi przepisami art. 20c ust. 1 ustawy *o Policji* oraz art. 10b ust. 1 ustawy *o Straży Granicznej* służby te są uprawnione do uzyskiwania tzw. metadanych w celu zapobiegania lub wykrywania przestępstw oraz przestępstw skarbowych, Policja dodatkowo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych. Zauważyć przy tym należy, że dane te mogą być pozyskiwane wyłącznie w zakresie niezbędnym do realizacji zadań ustawowych wskazanych formacji, przy czym w odniesieniu do Straży Granicznej katalog czynów zabronionych, do których rozpoznawania, zapobiegania i wykrywania Straż Graniczna została upoważniona, określa art. 1 ust. 2 pkt 4 oraz ust. 2a ustawy *o Straży Granicznej*.

Natomiast odnosząc się do przytoczonego w wystąpieniu Pana Rzecznika wyroku Trybunału Sprawiedliwości Unii Europejskiej (TSUE) z dnia 2 marca 2021 r. w sprawie C-746/18 (sprawa *Prokuratuur*) oraz zastrzeżenia dotyczącego użycia przez ustawodawcę w ustawie *o Policji* oraz ustawie *o Straży Granicznej* ogólnego określenia przestępstwa należy zauważyć, że zgodnie z ww. orzeczeniem TSUE dostęp organów władzy publicznej do zbioru danych o ruchu lub danych o lokalizacji, które mogą dostarczyć

[1] Przekazane przy piśmie Pana Michała Dworczyka Ministra – Członka Rady Ministrów w Kancelarii Prezesa Rady Ministrów (znak: BPRM.5237.10.1.2021.TI).
[2] Dz. U. poz. 147.
[3] Dz. U. z 2020 r. poz. 360, z późn. zm.
[4] Dz. U. z 2020 r. poz. 305, z późn. zm.
[5] Dz. U. z 2021 r. poz. 576.

informacji o połączeniach wykonywanych przez użytkownika lub o lokalizacji używanego przez niego urządzenia oraz umożliwić wyciągnięcie precyzyjnych wniosków na temat jego życia prywatnego, do celów zapobiegania, dochodzenia, wykrywania i karania przestępstw, powinien być ograniczony do postępowań mających na celu zwalczanie poważnej przestępczości lub zapobieganie poważnym zagrożeniom bezpieczeństwa publicznego. Należy wskazać, że TSUE nie określił enumeratywnego katalogu przestępstw, do zapobiegania i wykrywania których instytucje państwowe mogą uzyskiwać dane telekomunikacyjne. Nie zostało również zdefiniowane samo pojęcie poważnej przestępczości.

W polskim systemie prawnym został przyjęty podział czynów zabronionych na te, które mają charakter poważny (przestępstwa) oraz pozostałe (wykroczenia). Wskazane rozróżnienie wiąże się również m.in. z oceną szkodliwości danej kategorii czynów i ich powszechności, co w konsekwencji przekłada się na zróżnicowanie rodzaju sankcji przewidzianych za przestępstwa i wykroczenia oraz ich dotkliwość. Z treści przepisów ustaw pragmatycznych służb w sposób jednoznaczny wynika, że nie posiadają one uprawnień do uzyskiwania tzw. metadanych na potrzeby prowadzenia postępowań w sprawie o wykroczenie. Powyższe wydaje się więc uzasadniać stwierdzenie, że wprowadzając podział czynów zabronionych na przestępstwa i wykroczenia ustawodawca określił, które z nich mają charakter poważny, a które nie należą do tej kategorii.

W rezultacie można stwierdzić, że zarówno art. 20c ustawy *o Policji*, jak i art. 10b ustawy *o Straży Granicznej* nie naruszają w analizowanym zakresie wymogu proporcjonalności ingerencji w prawo do prywatności, wolności komunikowania się oraz prawo do autonomii informacyjnej.

Jednocześnie pragnę zaznaczyć, że brak zdecydowanej i skutecznej reakcji organów władzy publicznej na czyny przestępcze może powodować poczucie bezkarności ich sprawców. Ponadto, rozważając ewentualne zawężenie katalogu przestępstw, w przypadku których możliwe byłoby uzyskiwanie danych telekomunikacyjnych, należy mieć na uwadze, że ze względu na powszechność narzędzia komunikowania się, jakim jest telefon komórkowy, ograniczenie dla służb dostępu do danych telekomunikacyjnych bez wątpienia wpłynie na znaczne utrudnienie wykrywania sprawców przestępstw. W szczególności w sytuacji, gdy dany czyn zabroniony będzie popełniony przy użyciu środków komunikacji elektronicznej.

Należy również wyjaśnić, że określone w ustawach pragmatycznych uprawnienie służb podległych ministrowi właściwemu do spraw wewnętrznych nie zobowiązuje dostawców usług telekomunikacyjnych do nieograniczonego i masowego przekazywania 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. 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.

Tryb udostępniania przez przedsiębiorcę telekomunikacyjnego, operatora pocztowego lub usługodawcę świadczącego usługi drogą elektroniczną danych określa art. 20c ust. 2 ustawy *o Policji* oraz art. 10b ust. 2 ustawy *o Straży Granicznej*. Zgodnie z przytoczonymi przepisami wskazane podmioty udostępniają dane:

1) funkcjonariuszowi wskazanemu w pisemnym wniosku odpowiednio w przypadku Policji: Komendanta Głównego Policji, Komendanta CBŚP, Komendanta BSWP, komendanta wojewódzkiego Policji albo osoby przez nich upoważnionej, a w przypadku Straży Granicznej - Komendanta Głównego Straży Granicznej, Komendanta BSWSG lub komendanta oddziału Straży Granicznej 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.

Doprecyzowaniem przytoczonych regulacji są przepisy art. 20c ust. 4 ustawy *o Policji* oraz art. 10b ust. 4 ustawy *o Straży Granicznej* określające, że udostępnienie danych może nastąpić za pośrednictwem sieci telekomunikacyjnej wyłącznie jeżeli zapewnia ona możliwość ustalenia osoby uzyskującej te dane, ich rodzaju oraz czasu, w którym zostały uzyskane, a także zabezpieczenie techniczne i organizacyjne uniemożliwiające dostęp osobie nieuprawnionej. Mechanizm ten zapewnia wewnętrzną weryfikowalność przypadków pozyskiwania danych telekomunikacyjnych. Celowi temu służą również przepisy zobowiązujące uprawnione podmioty (Komendanta Głównego Policji, Komendanta CBŚP, Komendanta BSWP i komendanta wojewódzkiego Policji oraz Komendanta Głównego Straży Granicznej, Komendanta BSWSG i komendanta oddziału Straży Granicznej) do prowadzenia rejestrów wystąpień o uzyskanie danych telekomunikacyjnych, pocztowych i internetowych.

W kwestii sposobu ukształtowania kontroli nad uzyskiwaniem przez Policję i Straż Graniczną metadanych należy wskazać, że obowiązujące rozwiązania przewidują mechanizmy pozwalające na skuteczne realizowanie funkcji kontrolnej przez sąd okręgowy właściwy dla siedziby składającego wniosek organu Policji lub Straży Granicznej (art. 20ca ustawy *o Policji* oraz art. 10ba ustawy *o Straży Granicznej*). Właściwy organ, który wystąpił z wnioskiem, przekazuje, z zachowaniem przepisów o ochronie informacji niejawnych, sądowi okręgowemu, w okresach półrocznych, sprawozdanie obejmujące:

- 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.

Sąd okręgowy może zapoznać się z materiałami uzasadniającymi udostępnienie przedmiotowych danych. Tak ukształtowane przepisy, wpisujące się w zakres dopuszczony orzeczeniem TK o sygn. K 23/11, pozwalają sądowi, jako niezależnemu organowi wymiaru sprawiedliwości, na swobodne ukształtowanie sposobu przeprowadzania kontroli. W kompetencji sądu znajduje się decyzja o tym czy i w jakim zakresie sprawdzeniu podlegać będą konkretne materiały oraz jakie będzie kryterium doboru spraw, w których przeprowadzona zostanie pogłębiona kontrola.

Ponadto, dodatkowym elementem weryfikacji uzyskiwania danych telekomunikacyjnych przez Policję i Straż Graniczną jest procedura określona w art. 20c ust. 6 i 7 ustawy *o Policji* oraz art. 10b ust. 6 i 7 ustawy *o Straży Granicznej*. Zgodnie z przytoczonymi przepisami te dane, które mają znaczenie dla postępowania karnego uprawniony organ przekazuje prokuratorowi właściwemu miejscowo lub rzeczowo, który podejmuje decyzję o zakresie i sposobie wykorzystania przekazanych informacji. Natomiast dane telekomunikacyjne, które nie mają znaczenia dla postępowania karnego podlegają niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu.

Odnosząc się do kwestii 12 miesięcznego okresu przechowywania danych należy go 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*[6] , która skróciła okres retencji danych z 24 do 12 miesięcy. Jak wynika z uzasadnienia do treści wyroku TSUE w sprawie Prokuratuur podobny termin zatrzymywania danych obowiązuje w większości państw członkowskich UE.

Nie bez znaczenia dla oceny rozwiązań przyjętych w poszczególnych państwach członkowskich UE w analizowanym zakresie pozostaje specyfika procesu wykrywczego, 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

[6] Dz. U. poz. 1445, z późn. zm.

na etapie czynności operacyjno-rozpoznawczych, a nie na etapie procesu karnego, jak ma to miejsce w wielu państwach Europy Zachodniej.

Odnosząc się z kolei do podnoszonych przez Pana Rzecznika wątpliwości dotyczących art. 168a ustawy z dnia 6 czerwca 1997 r. *Kodeks postępowania karnego*[7] należy wskazać, że jest to przepis o charakterze generalnym, który wyznacza zasady w zakresie dopuszczalności dowodów na gruncie postępowania karnego we wszystkich rodzajach spraw. Tym samym ww. regulacja nie dotyczy tylko dowodów uzyskanych w drodze zatrzymania danych o ruchu i danych o lokalizacji. Toteż analiza odnośnie zasadności postulowanej zmiany ww. generalnego przepisu z obszaru procedury karnej wiąże się z zakresem właściwości Ministra Sprawiedliwości[8].

Z poważaniem
MINISTER
SPRAW WEWNĘTRZNYCH i ADMINISTRACJI
z up. Maciej Wąsik
Sekretarz Stanu
- podpisano kwalifikowanym podpisem elektronicznym -

Otrzymuje:
Pan Michał Dworczyk Minister – Członek Rady Ministrów w Kancelarii Prezesa Rady Ministrów.

[7] Dz. U. z 2021 r. poz. 534.
[8] art. 24 ust. 1 i 2 ustawy z dnia 4 września 1997 r. *o działach administracji rządowej* (Dz. U. z 2020 r. poz. 1220, z późn. zm.).