RZECZNIK PRAW OBYWATELSKICH

Adam Bodnar

Warszawa, 31-03-2021 r.

II.519.109.2015.MM

Pan
Mateusz Morawiecki
Prezes Rady Ministrów

ePUAP

Szanowny Panie Premierze,

w moim zainteresowaniu pozostaje kwestia zbierania i wykorzystywania danych telekomunikacyjnych dotyczących lokalizacji telefonów komórkowych przez Policję i służby specjalne, a także nadzór nad powyższymi działaniami prowadzony przez sąd. Jak wielokrotnie podkreślałem, wymogi bezpieczeństwa państwa nie oznaczają, że prowadzenie inwigilacji nie ma podlegać ograniczeniom wynikającym z konstytucyjnych praw i wolności. Powinny być one wynikiem odpowiedniego wyważania pomiędzy potrzebą ochrony bezpieczeństwa obywateli oraz ich prawa do prywatności. Należy wskazać, że w tym zakresie jednostka ma bardzo ograniczone środki bezpośredniej ochrony prawnej. Nie bez znaczenia w tym aspekcie jest najnowszy wyrok Trybunału Sprawiedliwości Unii Europejskiej (dalej „TSUE") z dnia 2 marca 2021 r. wydany w sprawie C-746/18 *Prokuratuur*[1].

W wyroku tym TSUE wskazał, że art. 15 ust. 1 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)[2], zmienionej dyrektywą Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r.[3], w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej należy interpretować w ten sposób, że

[1] ECLI:EU:C: 2021:152.
[2] Dz. Urz. UE z dnia 21 lipca 2002 r., Seria L, Nr 201, str. 37.
[3] Dz. Urz. UE z dnia 18 grudnia 2009 r., Seria L, Nr 337, str. 11.

sprzeciwia się on przepisom krajowym umożliwiającym dostęp organów władzy publicznej do zbioru danych o ruchu lub danych o lokalizacji, które mogą dostarczyć informacji o połączeniach wykonywanych przez użytkownika środka łączności elektronicznej lub o lokalizacji używanego przez niego urządzenia końcowego oraz umożliwić wyciągnięcie precyzyjnych wniosków na temat jego życia prywatnego, do celów zapobiegania, dochodzenia, wykrywania i karania przestępstw, bez ograniczania takiego dostępu do postępowań mających na celu zwalczanie poważnej przestępczości lub zapobieganie poważnym zagrożeniom bezpieczeństwa publicznego, niezależnie od długości okresu, na jaki wniesiono o dostęp do takich danych, oraz ilości i rodzaju danych dostępnych przez taki okres.

Trybunał przypomniał, że art. 15 ust. 1 dyrektywy o prywatności i łączności elektronicznej w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 KPP stoi na przeszkodzie środkom ustawodawczym przewidującym w tych celach prewencyjne uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych o lokalizacji[4]. Jedynie walka z poważną przestępczością i zapobieganie poważnym zagrożeniom bezpieczeństwa publicznego mogą uzasadniać poważne ingerencje w prawo do poszanowania życia prywatnego i rodzinnego oraz prawo do ochrony danych osobowych, takie jak te związane z zatrzymywaniem danych o ruchu i danych o lokalizacji, które mogą dostarczyć informacji o połączeniach wykonywanych przez użytkownika środka łączności elektronicznej lub o lokalizacji używanych przez niego urządzeń końcowych i umożliwiają wyciągnięcie precyzyjnych wniosków na temat życia prywatnego osób, których dotyczą[5]. Ingerencja w te prawa ma w każdym wypadku poważny charakter, niezależnie od długości okresu na jaki się wnosi o dostęp do wspomnianych danych[6]. W każdym wypadku powinno dojść do spełnienia wymogu proporcjonalności a odstępstwa od poszanowania prywatności czy danych osobowych powinny być ograniczone do tego, co jest ściśle niezbędne do celów danego dochodzenia[7].

W tym aspekcie konieczne jest wskazanie, że polskie prawo nie spełnia wymogów wynikających z prawa Unii Europejskiej, które znalazły odzwierciedlenie w

[4] Pkt 30 uzasadnienia wyroku.
[5] Ibidem, pkt 33-35.
[6] Ibidem, pkt 39.
[7] Ibidem, pkt 38.

przedmiotowym rozstrzygnięciu. Uchwalona w dniu 15 stycznia 2016 r. ustawa o zmianie ustawy o Policji[8] dokonała zmian m.in. w art. 20c ust. 1 ustawy o Policji[9], art. 10b ust. 1 ustawy o Straży Granicznej[10], art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych[11], art. 28 ust. 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu[12], art. 32 ust. 1 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego[13], art. 18 ust. 1 ustawy o Centralnym Biurze Antykorupcyjnym[14]. W brzmieniu obowiązującym po nowelizacji ustawy o Policji, na podstawie art. 20c ust. 1 ustawodawca przyznał Policji prawo do uzyskiwania danych niestanowiących treści odpowiednio, przekazu telekomunikacyjnego, przesyłki pocztowej albo przekazu w ramach usługi świadczonej drogą elektroniczną, a także do przetwarzania tych danych bez wiedzy i zgody osoby, której dotyczą. Prawo to przyznane zostało w celu zapobiegania lub wykrywania przestępstw albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych. Dane, do których uzyskiwania i przetwarzania zyskała dostęp Policja określone są odpowiednio w:

- art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243 ze zm., dalej jako: Prawo telekomunikacyjne) – tzw. „dane telekomunikacyjne”,
- art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529 oraz z 2015 r. poz. 1830, dalej jako: Prawo pocztowe) – tzw. „dane pocztowe”,
- art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422 orz z 2015 r. poz. 1844, dalej jako: uśude) – tzw. „dane internetowe”.

Analogiczne uprawnienia do uzyskiwania i przetwarzania danych uzyskały pozostałe służby:

- Straż Graniczna – w celu zapobiegania lub wykrywania przestępstw (art. 10b ust. 1 ustawy o Straży Granicznej),

[8] Dz.U. z 2016 r., poz. 147.
[9] Dz.U. z 2020 r., poz. 360 - t.j.
[10] Dz.U. z 2020 r., poz. 305 - t.j.
[11] Dz.U. z 2020 r., poz. 431 - t.j.
[12] Dz.U. z 2020 r., poz. 27 - t.j.
[13] Dz.U. z 2019 r., poz. 687 - t.j.
[14] Dz.U. z 2019 r., poz. 1921 - t.j.

- Żandarmeria Wojskowa – w celu zapobiegania lub wykrywania przestępstw, w tym przestępstw skarbowych, popełnionych przez osoby, o których mowa w art. 3 ust. 2 pkt 1, 3, 4, 5 i 6 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych (art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych),
- Agencja Bezpieczeństwa Wewnętrznego – do realizacji zadań ustawowych (art. 28 ust. 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu),
- Służba Kontrwywiadu Wojskowego – do realizacji zadań ustawowych (art. 32 ust. 1 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego),
- Centralne Biuro Antykorupcyjne – do realizacji zadań ustawowych (art. 18 ust. 1 ustawy o Centralnym Biurze Antykorupcyjnym).

Analizując wskazane przepisy ustaw należy rozpocząć od stwierdzenia, że w art. 20c ust. 1 o Policji (oraz analogicznie w pozostałych przepisach wskazanych ustaw) nie są spełnione kryteria uzasadniające ograniczenie praw i wolności obywatelskich, wynikających z Konstytucji, co poddaje w wątpliwość zgodność art. 20c ust. 1 ustawy o Policji oraz pozostałych wskazanych przepisów z art. 2, 30, 47, 49, 51 ust. 2 Konstytucji w zw. z art. 31 ust. 3 oraz art. 8 EKPC i art. 7 i 8 w zw. z art. 52 ust. 1 KPP UE.

Jak wskazano wyżej, ustawa o Policji przewiduje dopuszczalność uzyskiwania danych telekomunikacyjnych, danych pocztowych i danych internetowych do celów określonych w omawianych przepisach. Tym samym celom ma służyć pozyskiwanie danych, określonych w art. 20cb ust. 1 ustawy o Policji. Analizując katalog przestępstw, w przypadku których dopuszczalne jest uzyskiwanie i przetwarzanie tych danych w odniesieniu do poszczególnych służb wyraźnie widać, że jest on nadmiernie szeroki, co wskazuje na przekroczenie granic, o których mowa w art. 31 ust. 3 Konstytucji, art. 8 ust. 2 EKPC oraz art. 52 ust. 1 KPP UE. W art. 20c ust. 1 ustawy o Policji nie wskazano poszczególnych typów czynów zabronionych pod groźbą kary, które uzasadniałyby sięgnięcie po tego typu dane o obywatelach, lecz użyto ogólnego określenia „przestępstwa". Oznacza to możliwość uzyskiwania przez Policję danych w odniesieniu do wszystkich czynów zabronionych spełniających znamiona jakiegokolwiek przestępstwa, w tym ściganego na wniosek lub z

oskarżenia prywatnego. Tym samym stanowić to będzie nadmierną ingerencję w prawo do prywatności i w prawo do ochrony danych osobowych, a także naruszenie zasady autonomii informacyjnej, wyrażone w art. 47, 49 oraz 51 ust. 2 Konstytucji, przez co naruszona jest również zasada godności człowieka, określona w art. 30 Konstytucji.

Użyte w tych przepisach pojęcia nie spełniają wskazanego kryterium jasności przepisów. Tak ujęty cel gromadzenia i przetwarzania danych może bowiem oznaczać w istocie brak selektywności już na etapie rozpoczęcia pozyskiwania danych internetowych, czyli możliwości uzyskiwania przez służby danych w postępowaniach w sprawie bliżej nieokreślonych czynów zabronionych, bez względu na ich szkodliwość społeczną. Oznacza ponadto, że nie zagwarantowano, by gromadzenie i przetwarzanie danych internetowych było subsydiarnym środkiem pozyskiwania informacji lub dowodów o osobach fizycznych. Brak subsydiarności przepisów otwiera możliwość wykorzystywania danych telekomunikacyjnych, pocztowych i internetowych nie tylko wówczas, gdy jest to rzeczywiście konieczne do wykrywania lub zapobiegania przestępstwom, ale także wtedy, gdy jest to po prostu najprostsze i najwygodniejsze[15]. Do tej kwestii odniósł się również Trybunał Konstytucyjny w wyroku z dnia 30 lipca 2014 r. w sprawie K 23/11 wskazując, że „niejawne pozyskiwanie informacji o jednostkach w toku czynności operacyjno-rozpoznawczych musi być środkiem subsydiarnym, czyli stosowanym wówczas, gdy inne rozwiązania są nieprzydatne lub nieskuteczne".

Na konieczność precyzyjnego uregulowania zakresu przestępstw, w przypadku których dopuszczalne jest sięganie po dane, wskazywały również trybunały ponadnarodowe: Europejski Trybunał Praw Człowieka (ETPC) i Trybunał Sprawiedliwości Unii Europejskiej (TSUE), interpretując przepisy odpowiednio EKPC i KPP UE. W sprawie Zakharov przeciwko Rosji[16] ETPC wskazał, że przesłanką uzasadniającą stwierdzenie naruszenia art. 8 EKPC jest m.in. brak sprecyzowania jakichkolwiek okoliczności, w których organy mogą prowadzić inwigilację obywateli. Z kolei w sprawie C-293/12 i C-594/12 Digital Rights Ireland Ltd[17] TSUE, stwierdzając nieważność dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie

[15] Zob. wyroki Trybunału Konstytucyjnego: z 12.12.2005 r. w sprawie K 32/04, OTK-A 2005/11/132; z 23.06.2009 r. w sprawie K 54/07, OTK-A 2009/6/86.
[16] Wyrok ETPC z 4.12.2015 r., w sprawie Roman Zakharov v. Rosja, skarga nr 47143/06.
[17] Wyrok TSUE z 8.04.2014 r., C-293/12 i C-594/12, Digital Rights Ireland Ltd, ECLI:EU:C:2014:238.

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[18] w związku z naruszeniem wymogu proporcjonalności przy ingerencji w prawo do prywatności i prawo do ochrony danych osobowych uznał, że nie wystarczy samo odniesienie się do „poważnych przestępstw" by uznać przesłanki wskazane w art. 52 ust. 1 KPP UE za spełnione i uzasadniające ingerencję w określone wyżej prawa. Wskazane przepisy ustaw są zatem niezgodne z art. 30, 47, 49, 51 ust. 2 w zw. z art. 31 ust. 3 Konstytucji, a także z art. 8 EKPC oraz 7 i 8 w zw. z art. 52 ust. 2 KPP UE. Ponadto, wskazane przepisy ustaw naruszają również art. 30, 47, 49, 51 ust. 2 Konstytucji w zw. z art. 2 Konstytucji statuującym zasadą ochrony zaufania do państwa i stanowionego przez nie prawa, a także zasadę określoności przepisów prawa poprzez odwołanie się do definicji pojęcia „dane internetowe", które nie jest jasne i precyzyjne, a tym samym normy te naruszają wymóg przewidywalności przepisów ograniczających prawo do prywatności, prawo do ochrony danych osobowych oraz zasadę autonomii informacyjnej jednostki.

Wskazać należy w szczególności, że pojęcie „danych internetowych" definiowane jest poprzez odwołanie do art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[19]. Pojęcie to obejmuje zatem: 1) dane osobowe usługobiorcy niezbędne do nawiązania, ukształtowania treści, zmiany lub rozwiązania stosunku prawnego, między innymi nazwisko i imiona usługobiorcy, numer ewidencyjny PESEL, lub – gdy numer ten nie został nadany – numer paszportu, dowodu osobistego lub innego dokumentu potwierdzającego tożsamość, adres zameldowania na pobyt stały, adres do korespondencji, dane służące do weryfikacji podpisu elektronicznego usługobiorcy, adresy elektroniczne usługobiorcy; 2) inne dane niezbędne ze względu na właściwość świadczonej usługi lub sposób jej rozliczenia; 3) inne dane dotyczące usługobiorcy, które nie są niezbędne do świadczenia usługi drogą elektroniczną, przekazane za zgodą usługobiorcy; 4) tzw. dane eksploatacyjne, charakteryzujące sposób korzystania z usługi świadczonej drogą elektroniczną, w tym oznaczenia identyfikujące usługobiorcę, oznaczenia identyfikujące zakończenie sieci telekomunikacyjnej lub system teleinformatyczny, z którego korzystał

[18] Dz. Urz. UE z dnia 31 lipca 2002 r., seria L, Nr 105, str. 54.
[19] Dz. U. z 2013 r., poz. 1422 ze zm.

usługobiorca, informacje o rozpoczęciu, zakończeniu oraz zakresie każdorazowego korzystania z usługi świadczonej drogą elektroniczną, informacje o skorzystaniu przez usługobiorcę z usług świadczonych drogą elektroniczną. Pragnę podkreślić, że wymienione w tym przepisie kategorie danych są określone bardzo ogólnie, co może powodować niejasności i prowadzić do zbyt szerokiego pojmowania tych pojęć, a w efekcie do nadmiernej ingerencji w prawa podstawowe. Przypomnieć należy, że prawo określające granice ingerencji państwa w prawa człowieka i obywatela musi spełniać wymogi jakościowe, być dostępne oraz przewidywalne dla jednostek – z prawa muszą wynikać okoliczności i warunki, w których władze publiczne będą sięgać po określone dane. Precyzja regulacji prawnej ma zapobiegać ryzyku arbitralności działań, z natury rzeczy pozostających poza zasięgiem kontroli publicznej. Niejasności związane z zakresem danych internetowych, które mogą być gromadzone przez służby, powoduje, że nie można uznać, by spełniony był wymóg precyzyjności prawa. Trzeba również podkreślić, że wskazany szeroki zakres informacji, do których mają dostęp służby, pozwala na szerokie i precyzyjne odtworzenie różnych aspektów życia prywatnego. Może również prowadzić do budowania profilu osobowego osób uczestniczących w procesie komunikacji, a co za tym idzie – do ustalenia ich trybu życia, przynależności do organizacji społecznych czy politycznych, osobistych upodobań czy skłonności osób poddanych obserwacji. Uzyskiwanie i przetwarzanie danych internetowych nie musi mieć też związku z żadnym konkretnym toczącym się postępowaniem.

Powyższą konstatację potwierdzają wyniki z kontroli planowej nr P/12/191 Najwyższej Izby Kontroli – „Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180c i d ustawy Prawo telekomunikacyjne". W podsumowaniu wyników kontroli stwierdzono, że: „[w] ocenie NIK, obowiązujące przepisy w zakresie pozyskiwania przez uprawnione podmioty danych telekomunikacyjnych nie chronią w stopniu wystarczającym praw i wolności obywatelskich przed nadmierną ingerencją ze strony państwa. Niejednolitość i ogólnikowość przepisów uprawniających do pozyskiwania danych telekomunikacyjnych, może nasuwać wątpliwości, co do współmierności stosowanych ograniczeń praw i wolności obywatelskich w sferze wolności komunikacji z zasadami określonymi w Konstytucji RP. Należy ponadto zauważyć, iż obowiązujący system zbierania informacji o zakresie

wykorzystania przez organy państwa danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180c i d ustawy Prawo telekomunikacyjne, nie pozwala na określenie rzeczywistej liczby dokonywanych sprawdzeń. Brak jest również mechanizmów kontroli o charakterze zewnętrznym, które pozwoliłyby na weryfikację zakresu wykorzystywania danych telekomunikacyjnych przez uprawnione podmioty, a w szczególności zasadności ich pozyskiwania i przetwarzania”[20].

W tym kontekście pragnę przypomnieć, że Rzecznik zainicjował postępowanie przed Trybunałem Konstytucyjnym w sprawie K 23/11, w której, w wyroku wydanym 30 lipca 2014 r., Trybunał stwierdził niekonstytucyjność części zaskarżonych przepisów, co miało doprowadzić do stworzenia systemu przetwarzania danych opartego o konstytucyjny standard ochrony prywatności. Należy jednak stwierdzić, że ustawodawca nie spełnił niestety pokładanych w nim w tym zakresie nadziei. Mająca wykonywać wyrok, wspomniana już ustawa z dnia 5 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw, nowelizując relewantne przepisy, znacząco poszerzyła możliwości ingerencji formacji i służb specjalnych w sferę prywatności obywateli.

Znowelizowane przepisy nie tylko nie realizują wyroku TK z 2014 r., ale w poważnym zakresie naruszają konstytucyjne prawa i wolności człowieka oraz standardy wyznaczone w prawie międzynarodowym. W wyniku zmiany przepisów służby uzyskały dostęp do danych internetowych za pomocą stałego łącza. Pobieranie danych nie musi się wiązać z żadnym toczącym się postępowaniem. Służby nie muszą już - 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 i prawa europejskiego), ale także wtedy, gdy jest to dla służb po prostu wygodne. Taki dowolny dostęp do danych oznacza ryzyko poważnych nadużyć. Służby mogą na tej podstawie np. precyzyjnie odtwarzać różne aspekty życia prywatnego obywatela, zbierać dane o trybie życia, poglądach, upodobaniach czy skłonnościach. Kolejnym zarzutem wobec znowelizowanych przepisów był nieproporcjonalnie długi czasu trwania kontroli operacyjnej - do 18 miesięcy. Ponadto

[20] https://www.nik.gov.pl/kontrole/wyniki-kontroli-nik/pobierz,nik-p-12-191-billingi,typ,kk.pdf

znowelizowane przepisy ograniczyły chronioną prawem tajemnicę zawodów zaufania publicznego, m.in. adwokatów, radców prawnych, lekarzy i dziennikarzy. Zdobyte podczas inwigilacji tajemnice mogą bowiem być wykorzystane w postępowaniu karnym, gdy „jest to niezbędne ze względu na dobro wymiaru sprawiedliwości, a okoliczność ta nie może być ustalona na podstawie innego dowodu".

W czerwcu 2016 r. Komisja Wenecka uznała, że nowelizacja ustawy o Policji nadaje służbom zbyt szerokie kompetencje, które mogą uderzać bezpośrednio w prawo do prywatności obywateli. Oceniła m.in., że dostęp służb do najbardziej wrażliwych danych telekomunikacyjnych i internetowych powinien wymagać uprzedniej zgody sądu; nadzór nad zbieraniem mniej wrażliwych danych powinien sprawować niezależny organ, a jednostka powinna być informowana o ich pobraniu; system składania sądom ogólnych sprawozdań przez służby będzie nieskuteczny. Komisja Wenecka zalecała m.in. by pozyskiwanie najważniejszych danych telekomunikacyjnych i internetowych ograniczyć do najgroźniejszych sytuacji; by skrócić czas przechowywania danych oraz zadbać o nienaruszanie tajemnicy adwokackiej[21].

Rozwiązania polskie są również niezgodne z powołanym na wstępie wyrokiem TSUE, który podkreślił, że dyrektywa o prywatności i łączności elektronicznej stoi na przeszkodzie środkom ustawodawczym nakładającym na dostawców usług łączności elektronicznej obowiązek prewencyjnego, uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji. Są one też niezgodne z tą dyrektywą w zakresie w jakim pozwalają na korzystanie z tego typu danych w każdym postępowaniu, a nie jedynie w postępowaniu zmierzającym do zwalczania poważnej przestępczości lub zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego. Tylko bowiem to ostatnie może uzasadniać dostęp organów władzy publicznej do zbioru danych o ruchu lub danych o lokalizacji, które umożliwiają wyciągnięcie precyzyjnych wniosków na temat życia prywatnego osób, których dane dotyczą. Jednocześnie, inne czynniki związane z proporcjonalnością wniosku o udzielenie dostępu, takie jak długość okresu, na jaki wniesiono o dostęp, nie mogą skutkować tym, aby uzasadnienie wniosku sprowadzało się do wskazania celu polegającego na dochodzeniu, wykrywaniu i karaniu ogółu przestępstw lub zapobieganiu im.

[21] https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD%282016%29012-e

Ustawa o zmianie ustawy o Policji dodała również przepisy, regulujące zasady sprawowania przez sąd okręgowy kontroli nad uzyskiwaniem przez Policję i inne służby danych telekomunikacyjnych, pocztowych lub internetowych. Są to – odpowiednio: art. 20ca ustawy o Policji, art. 10ba ustawy o Straży Granicznej, art. 30b ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28a ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 32a ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego oraz art. 18a ustawy o Centralnym Biurze Antykorupcyjnym. Zgodnie z tymi przepisami, kontrolę nad uzyskiwaniem przez daną służbę danych telekomunikacyjnych, pocztowych lub internetowych sprawować ma sąd okręgowy właściwy dla siedziby organu Policji (i odpowiednio innych służb, z wyjątkiem Żandarmerii Wojskowej, w przypadku której kontrolę sprawuje wojskowy sąd okręgowy właściwy ze względu na siedzibę organu Żandarmerii Wojskowej oraz Agencji Bezpieczeństwa Wewnętrznego i Centralnego Biura Antykorupcyjnego w przypadku których sądem właściwym jest Sąd Okręgowy w Warszawie, a także Służby Kontrwywiadu Wojskowego w przypadku której sądem właściwym jest Wojskowy Sąd Okręgowy w Warszawie), któremu udostępniono te dane. Właściwy organ Policji (i odpowiednio innych służb) ma obowiązek przekazywać, z zachowaniem przepisów o ochronie informacji niejawnych, właściwemu sądowi, w okresach półrocznych, sprawozdanie obejmujące: 1) liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych, pocztowych lub internetowych oraz rodzaj tych danych, 2) 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 kontroli sąd okręgowy może zapoznać się z materiałami uzasadniającymi udostępnienie Policji (i odpowiednio pozostałym służbom) danych telekomunikacyjnych, pocztowych lub internetowych. Sąd okręgowy informuje organ Policji (i odpowiednio pozostałych służb) o wyniku kontroli w terminie 30 dni od jej zakończenia. Dodatkowo przepisy określają przypadek, kiedy uzyskiwanie danych nie podlega kontroli sądu (dane zbierane na podstawie art. 20cb ustawy o Policji i odpowiednio przepisów pozostałych ustaw). Wskazane w ustawach procedury kontrolne budzą jednak poważne wątpliwości.

Kwestia zapewnienia realnej uprzedniej kontroli sądowej była już wcześniej przedmiotem rozważań Trybunału Sprawiedliwości UE w połączonych sprawach C-293/12 i C-594/12[22], gdzie TSUE stwierdził wyraźnie – analizując przepisy dyrektywy 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 – że nie przewidziała ona uprzedniej kontroli sądu lub niezależnego organu administracyjnego, który pilnowałby, aby udostępnianie i wykorzystywanie danych ograniczało się do przypadków, gdy jest to ściśle konieczne do realizacji zamierzonego celu oraz orzekały lub decydowały wyłącznie na uzasadniony wniosek przedstawiony w kontekście postępowań mających na celu zapobieganie, wykrywanie lub ściganie przestępstw. Brak uprzedniej kontroli sądu lub niezależnego organu TSUE uznał za nieuzasadnioną ingerencję w prawa podstawowe ustanowione w art. 7 i 8 KPP UE. Z kolei Trybunał Konstytucyjny, orzekając w sprawie K 23/11 w odniesieniu do danych telekomunikacyjnych stwierdził wyraźnie, że ogólny standard konstytucyjny nie przesądza, jak dokładnie ma wyglądać procedura dostępu do danych telekomunikacyjnych, a w szczególności czy konieczne ma być w odniesieniu do każdego rodzaju zatrzymywanych danych, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego, uzyskanie zgody na ich udostępnienie. Nie wszystkie dane tego rodzaju powodują taką samą intensywność ingerencji w wolności i prawa człowieka. Zdaniem Trybunału, „nie jest wobec tego wykluczone – w odniesieniu do udostępniania danych telekomunikacyjnych w toku czynności operacyjno-rozpoznawczych – wprowadzenie, jako zasady, kontroli następczej. Regulując ten mechanizm, ustawodawca powinien uwzględnić m.in. specyfikę działania i ustawowy zakres zadań poszczególnych służb, sytuacje niecierpiące zwłoki, w których szybkie pozyskanie danych telekomunikacyjnych może być niezbędne do zapobieżenia popełnieniu przestępstwa lub jego wykrycia. Zgodnie z konstytucyjną zasadą sprawności działania instytucji publicznych (wstęp do Konstytucji) należy wykreować mechanizm, który umożliwiłby służbom odpowiedzialnym za bezpieczeństwo państwa i porządek publiczny efektywną walkę z zagrożeniami. Trybunał dostrzega jednak argumenty za wprowadzeniem kontroli uprzedniej

[22] Wyrok TSUE z 8.04.2014 r., Digital Rights Ireland Ltd, ECLI:EU:C:2014:238.

w pewnych wypadkach. W szczególności chodzić może o dostęp do danych telekomunikacyjnych osób wykonujących zawody zaufania publicznego lub jeśli nie ma koniecznego pilnego działania służb. Kwestie te musi jednak odpowiednio wyważyć ustawodawca". W przepisach dotyczących poszczególnych służb wskazuje się na właściwość sądu okręgowego (lub odpowiednio innych sądów) w tzw. trybie następczym. Kontrola ta ma polegać na analizie półrocznych sprawozdań przedkładanych sądom przez służby. Należy podkreślić, że w przypadku zakwestionowanych ustaw regulujących dostęp do omawianych danych ustawodawca nie podjął się żadnego wyważenia potrzeby wprowadzenia uprzedniej kontroli, a ponadto – w odniesieniu do kontroli następczej – skonstruował ją w ten sposób, że w praktyce ma ona charakter iluzoryczny. Sprawozdania służb kierowane co pół roku do właściwego sądu w oparciu o przepisy o ochronie informacji niejawnych nie stanowią informacji publicznej, chociaż zawierają informacje dotyczące liczby przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych, pocztowych lub internetowych oraz rodzaj tych danych, a także kwalifikacji prawnej czynów, w związku z zaistnieniem których wystąpiono o dane. Przeprowadzenie czynności kontrolnych przez sąd ma charakter fakultatywny, a nie obligatoryjny. Ponadto, sąd po przeprowadzeniu kontroli może jedynie poinformować kontrolowaną służbę o wynikach kontroli, ale nie może zarządzić zniszczenia zgromadzonych danych. Wydaje się, że przy dużej skali pozyskiwanych danych oraz stosunkowo dużym odstępie czasowym, kontrola ta może mieć w istocie charakter iluzoryczny i nie spełniać wymogów wynikających z Konstytucji RP, a także z powołanych wcześniej umów międzynarodowych. Obecna forma kontroli jest zatem niewystarczająca. Kontrola następcza nie powinna być stosowana domyślnie, lecz może być dopuszczalna jedynie wyjątkowo, w sytuacjach, w których zachodzi potrzeba natychmiastowego działania służb. Omawiane przepisy ustaw w żadnym przypadku nie przewidują przeprowadzenia kontroli uprzedniej. Dzięki takiemu mechanizmowi przypadki sięgania po dane mogłyby podlegać rzetelnej ocenie pod względem spełniania kryteriów niezbędności, adekwatności i celowości. Podkreślenia wymaga, że zgodnie z art. 51 ust. 2 Konstytucji RP, władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach, niż niezbędne w demokratycznym państwie prawnym. Aktualna forma kontroli nie gwarantuje w sposób realny przestrzegania tych zasad, a przede wszystkim nie blokuje

możliwości pozyskiwania danych nawet wtedy, gdyby miało ono nastąpić z naruszeniem tychże zasad.

Należy również dodać, że zgodnie z art. 20ca ust. 5 ustawy o Policji (i odpowiednio w przypadku pozostałych służb) żadnej kontroli nie podlega uzyskiwanie danych, pozyskiwanych na podstawie art. 20cb ust. 1 ustawy o Policji. Ustawa o Policji i analogicznie pozostałe ustawy spod jakiejkolwiek kontroli wyłączają zatem pozyskiwanie danych nie tylko określonych w art. 179 ust. 9 Prawa telekomunikacyjnego, ale również całego art. 161 Prawa telekomunikacyjnego, co znacząco poszerza zakres dostępu do danych wyłączonych spod jakiejkolwiek kontroli. Zauważyć należy w szczególności, że art. 161 ust. 3 Prawa telekomunikacyjnego zawiera odniesienie do bliżej nieokreślonych „innych danych".

Jak wskazał TSUE w powołanym wyroku, dyrektywa o prywatności i łączności elektronicznej, interpretowana w świetle Karty Praw Podstawowych UE, stoi na przeszkodzie przepisom krajowym przyznającym prokuraturze, której zadaniem jest kierowanie postępowaniem przygotowawczym oraz sprawowanie funkcji oskarżyciela publicznego w ramach późniejszego postepowania, kompetencję do udzielania zezwoleń na dostęp organu władzy publicznej do danych o ruchu i danych o lokalizacji do celów postępowania przygotowawczego. Istotne jest jednak, aby sąd dokonujący uprzedniej kontroli dysponował wszelkimi uprawnieniami i gwarancjami niezbędnymi do pogodzenia poszczególnych wchodzących w grę interesów i praw. W postępowaniu przygotowawczym taka kontrola wymaga, aby sąd był w stanie zapewnić właściwą równowagę pomiędzy interesami związanymi z potrzebami dochodzenia w ramach zwalczania przestępczości oraz prawami podstawowymi do poszanowania życia prywatnego i ochrony danych osobowych osób, których dane są udostępniane.

Tymczasem obowiązujące regulacje nie przewidują realnej kontroli pobierania danych obywateli. Sąd okręgowy ma wprawdzie prawo do kontroli, ale jedynie na podstawie ogólnych, zbiorczych półrocznych sprawozdań służb. Sąd nie musi, ale tylko może weryfikować, czy dane pobrano zasadnie. Tymczasem Konstytucja zakazuje pozyskiwania, gromadzenia i udostępniania informacji o obywatelu innych niż niezbędne. Po kontroli sąd może jedynie poinformować poszczególną służbę o jej wynikach, ale nie może zarządzić np. zniszczenia zgromadzonych danych lub podjęcia innych działań naprawczych. W

praktyce ta kontrola sądów ma zatem charakter iluzoryczny. Tajne sprawozdania służb nie są informacją publiczną, choć zawierają informacje dotyczące liczby pozyskanych danych telekomunikacyjnych, pocztowych lub internetowych i kwalifikacji prawnej czynów, w związku z którymi o nie wystąpiono. Z tych przyczyn również kontrola sądu związana z wyrażeniem uprzedniej zgody na pobieranie danych jest niezgodna z powołaną dyrektywą.

Istotne jest również podkreślenie, że z wyroku TSUE wynika także konieczność wykluczenia informacji i dowodów uzyskanych z naruszeniem przepisów prawa Unii. W istocie bowiem dopuszczenie takich informacji i dowodów stwarza zagrożenie dla poszanowania zasady kontradyktoryjności, a tym samym prawa do rzetelnego procesu. Jak słusznie zauważył TSUE, „[s]ąd, który uważa, że strona nie jest w stanie skutecznie przedstawić stanowiska co do środka dowodowego, który należy do dziedziny niepodlegającej rozpoznaniu przez sąd i który może mieć decydujący wpływ na ocenę okoliczności faktycznych, powinien stwierdzić naruszenie prawa do rzetelnego procesu i wykluczyć ten środek dowodowy, aby uniknąć takiego naruszenia. W związku z tym zasada skuteczności nakłada na krajowy sąd karny obowiązek nieuwzględniania informacji i dowodów uzyskanych w drodze uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji niezgodnego z prawem Unii lub też w drodze sprzecznego z tym prawem dostępu właściwego organu do tych danych, w ramach postępowania karnego wszczętego przeciwko osobom podejrzanym o popełnienie przestępstwa, jeżeli osoby te nie są w stanie skutecznie ustosunkować się do tych informacji i dowodów, należących do dziedziny niepodlegającej rozpoznaniu przez sąd i mogących mieć decydujący wpływ na ocenę okoliczności faktycznych”[23].

Tymczasem, art. 168a Kodeksu postępowania karnego, przewiduje rozwiązanie zgoła odwrotne. Przepis ten zachęca wręcz służby państwowe do pozyskiwania dowodów w drodze popełniania przestępstw i łamania procedur zapewniając, że będą one mogły być wykorzystane w postępowaniu karnym. Tym samym regulacja ta w istocie unieważnia wszelkie i tak szczątkowe, mechanizmy kontroli nad pozyskiwaniem danych o obywatelach. Całkowicie niezbędne jest zatem takie uregulowanie kwestii zakazów dowodowych, aby w sprawie nie mogły zostać wykorzystane dowody, które zostały zgromadzone z naruszeniem prawa, czy to krajowego, czy też unijnego. Takie dowody powinny być wyeliminowane z

[23] Wyrok TSUE z 2.03.2021 r., C-746/18, pkt 44.

materiału dowodowego stanowiącego podstawę rozstrzygnięcia w postępowaniu karnym. Postulować należy więc pilną zmianę treści art. 168a k.p.k., przywracającą mu treść sprzed nowelizacji z 2016 r. W obecnym brzmieniu przepis ten jest bowiem jawnie i oczywiście niekonstytucyjny. Ponure świadectwo o Polsce stanowi utrzymywanie regulacji, która zachęca organy państwa do łamania prawa i zapewnia, że nielegalne działania zostaną usankcjonowane w procesie karnym.

Mając na uwadze powyższe, działając na podstawie art. 16 ust. 2 pkt 1 ustawy z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. z 2020 r. poz. 627) zwracam się z uprzejmą prośbą do Pana Premiera o zajęcie stanowiska w niniejszej sprawie oraz rozważenie zaproponowania właściwych zmian legislacyjnych w tym zakresie, a także o poinformowanie mnie o podjętych działaniach.

Z wyrazami szacunku,

Adam Bodnar

Rzecznik Praw Obywatelskich

/-podpisano elektronicznie/