RZECZNIK PRAW OBYWATELSKICH

Marcin Wiącek

Warszawa, 13-01-2022 r.

VII.501.306.2021.KZ

Pan
Mateusz Morawiecki
Prezes Rady Ministrów

Kancelaria
Prezesa Rady Ministrów
ePUAP

Szanowny Panie Premierze,

do Rzecznika Praw Obywatelskich wpływają zapytania obywateli dotyczące dopuszczalności wykorzystywania w toku kontroli operacyjnej oprogramowania szpiegowskiego Pegasus[1]**.** W związku z tym Rzecznik Praw Obywatelskich pragnie przypomnieć, że wielokrotnie występował już z wnioskami dotyczącymi konieczności podjęcia prac legislacyjnych w związku z niezgodnością przepisów inwigilacyjnych ze standardami – odpowiednio – konstytucyjnym, określonym przez polski Trybunał Konstytucyjny (TK), oraz międzynarodowym i unijnym, określanymi w orzecznictwie Europejskiego Trybunału Praw Człowieka (ETPC) i Trybunału Sprawiedliwości Unii Europejskiej (TSUE). Brak jakichkolwiek działań naprawczych w sferze prawodawstwa wymaga kolejnej interwencji ze strony Rzecznika. Wobec powyższego uprzejmie proszę o przyjęcie i uwzględnienie poniższych uwag i zaleceń wraz z przypomnieniem dotychczasowego normatywnego tła w przedmiotowym zakresie oraz niezbędnego orzecznictwa sądowego.

Działalność operacyjna, zarówno Policji, jak też innych służb, realizowana w warunkach niejawności, pozostaje w naturalnym i – jak się wydaje – nieusuwalnym konflikcie

[1] Szerzej na temat sposobu działalności tego systemu: K. Brylak-Hudyma *Konstytucyjne prawa i wolności w obliczu nowych systemów inwigilacji*, Prawo Mediów Elektronicznych, 2/2020, s. 12-19.

z niektórymi prawami zasadniczymi jednostki. Dotyczy to przede wszystkim prawa jednostki do prywatności, konstytucyjnej wolności komunikowania się i związanej z tym ochrony tajemnicy komunikowania się oraz ochrony autonomii informacyjnej, a także konstytucyjnej gwarancji sądowej ochrony praw jednostki[2]. Prawa te gwarantowane są w tym kontekście nie tylko przez polską ustawę zasadniczą, lecz również przez Europejską Konwencję Praw Człowieka oraz porządek prawny Unii Europejskiej[3], w tym przede wszystkim Kartę Praw Podstawowych UE[4]. Kwestia zgodności w szczególności programów nieomal nieograniczonej inwigilacji ze standardami ochrony praw człowieka jest problemem istotnym i wciąż zyskującym na aktualności. Współcześnie, dzięki postępowi techniki skutkującym większą dostępnością tego typu systemów, narzędzia służące ofensywnej i szerokiej inwigilacji są przedmiotem obrotu tak jak inne zaawansowane systemy informatyczne[5] i również państwa muszą by gotowe, aby sprostać tym wyzwaniom.

Na wstępie niniejszego wystąpienia przypomnieć należy wyrok Trybunału Konstytucyjnego[6] w sprawie o sygn. akt K 4/04, w której Trybunał wypowiedział się w kwestii uprawnień przyznanych wywiadowi skarbowemu. Trybunał wskazał w tym wyroku, że **doniosłość prawa do prywatności, o którym mowa w art. 47 Konstytucji RP, w systemie konstytucyjnej ochrony praw i wolności człowieka i obywatela uwidacznia m. in. okoliczność, że prawo to jest – zgodnie z art. 233 ust. 1 Konstytucji RP – nienaruszalne nawet w ustawach ograniczających inne prawa, wydawanych w stanie wojennym i wyjątkowym.** Oznacza to zatem, że nawet warunki tak wyjątkowe i ekstremalne nie zezwalają ustawodawcy na złagodzenie przesłanek, przy spełnieniu których można wkroczyć w sferę życia prywatnego nie narażając się na zarzut niekonstytucyjnej arbitralności[7]. Ponadto należy zaznaczyć, że władze publiczne mogą pozyskiwać, gromadzić oraz udostępniać wyłącznie takie informacje o obywatelach, które są niezbędne w demokratycznym państwie prawnym. Konstytucja RP zaś realizuje najbardziej zasadnicze elementy składające się na treść prawa do ochrony życia prywatnego – respekt dla autonomii informacyjnej jednostki (obowiązek udostępnienia danych ograniczony do

[2] W. Hermeliński, *Bezpieczeństwo publiczne a prawo jednostki do prywatności*, Palestra 58/1-2 (661-662), s. 17.
[3] A. Grzelak, M. Wróblewski, *Ochrona praw podstawowych w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości w Unii Europejskiej*, [w:] System Prawa Unii Europejskiej. Tom 8. Współpraca sądowa w sprawach cywilnych, karnych i współpraca policyjna, red. J. Barcz, Warszawa 2021, s. 705-858.
[4] M. Wróblewski, *Karta Praw Podstawowych Unii Europejskiej*, [w:] System Prawa Unii Europejskiej. Tom 1. Podstawy i źródła prawa Unii Europejskiej, red. S. Biernat, Warszawa 2020, s. 725-775.
[5] M. Rojszczak, *Nieograniczone programy inwigilacji elektronicznej a koncepcja państwa autorytarnego*, Studia nad Autorytaryzmem i Totalitaryzmem 42, nr 2, 2020, str. 222.
[6] Wyrok TK z 20.06.2005 r., sygn. akt K 4/04, OTK ZU 6A/2005, poz. 64.
[7] Również w wyroku TK z 20.11.2002 r., sygn. akt K 41/02, OTK ZU nr 6/A/2002, poz. 83.

ściśle określonych ustawowo sytuacji) oraz jednoczesne ograniczenie w tym zakresie arbitralności ustawodawcy (ustawa nie może zakresu obowiązku kształtować dowolnie)[8].

W powołanym wyżej wyroku, stwierdzając niekonstytucyjność części zaskarżonych przepisów, Trybunał Konstytucyjny podkreślił również, że **konstruując przepis, który ingeruje głęboko w sferę prywatności jednostki, ustawodawca musi uwzględnić nie tylko zasady przyzwoitej legislacji, w tym zasadę precyzyjności regulacji, ale także rozważyć proporcjonalność zastosowanego środka** (art. 31 ust. 3 Konstytucji RP). Powołując się na orzecznictwo Europejskiego Trybunału Praw Człowieka, TK przypomniał podstawową wytyczną dla ustawodawcy, zgodnie z którą prawo musi być dostatecznie jasne w swych sformułowaniach, by dać obywatelom odpowiednie wskazówki w zakresie okoliczności i warunków, w jakich władze publiczne są uprawnione do działania w tajemnicy i do potencjalnie niebezpiecznej ingerencji w prawo do życia prywatnego i tajemnicy korespondencji[9].

Oceną zgodności z Konstytucją RP policyjnych przepisów inwigilacyjnych Trybunał Konstytucyjny zajmował się w sprawie o sygn. akt K 34/04. Trybunał orzekł wtedy o częściowej niezgodności z Konstytucją RP tych przepisów. W uzasadnieniu wyroku[10] TK wskazał, że sprzeczność między koniecznością istnienia legalnej, prawnie umocowanej działalności operacyjnej organów państwa i zagrożeniem dla konstytucyjnych wolności i praw jednostki wymaga przede wszystkim wyważenia właściwej proporcji w prawnej ochronie obu sfer, pozostających w konflikcie.

Instrumentarium prawne mające na celu wyważenie stosownego kompromisu obejmuje z jednej strony regulację materialnoprawną (określającą granice stawiane przez system prawa wkroczeniu przez władzę w poszczególne sfery prywatności jednostki), z drugiej zaś – gwarancje proceduralne, towarzyszące temu wkroczeniu, tj. konieczność zgłoszenia kontroli organowi pozapolicyjnemu i jej legalizacji przez ten organ, przesłanki i procedury legalizacji – przez organ zewnętrzny i poprzez udostępnienie zainteresowanemu (choćby w pewnym zakresie i od pewnego momentu czasowego) wiedzy o kontroli i jej rezultatach, środki kontroli na wypadek ekscesu organu przeprowadzającego kontrolę. Należy w tym miejscu zaznaczyć, że nie można jednak mówić o osiągnięciu właściwego kompromisu wówczas, gdy poziom ochrony materialnoprawnej będzie wprawdzie wysoki, zaś na poziomie proceduralnym będzie brakowało efektywnych, a więc „dających się uruchomić" przez poszkodowanego, procedur i środków umożliwiających realizację ochrony

[8] Również w wyroku TK z 12.11.2002 r., sygn. akt SK 40/01, OTK ZU nr 6/A/2002, poz. 81.
[9] Wyrok ETPC z 02.08.1984 r. w sprawie *Malone przeciwko Zjednoczonemu Królestwu*, skarga nr 8691/79.
[10] Wyrok TK z 12.12.2005 r., sygn. akt K 32/04, OTK ZU 11A/2005, poz. 132.

zagwarantowanej w przepisach materialnoprawnych, a także – dostępnej dla zainteresowanego – ochrony przed możliwymi ekscesami i szykanami ze strony organów państwa.

Przy ocenie natomiast czy ingerencja w wolności i prawa jednostki była wyrazem konieczności i została przeprowadzona tylko w niezbędnym wymiarze uwzględnia się specyfikę poszczególnych praw i wolności. Zdaniem Trybunału Konstytucyjnego, surowsze standardy dotyczą praw osobistych i politycznych, niż ekonomicznych i socjalnych. W przypadku konkurencyjności chronionych konstytucyjnie dóbr, konflikt pomiędzy konstytucyjnym prawem do prywatności i tajemnicą porozumiewania się, a względami bezpieczeństwa publicznego wymaga od ustawodawcy zachowania czytelnej równowagi między interesami pozostającymi w kolizji[11].

Trybunał Konstytucyjny odniósł się w badanej sprawie również do spraw zawisłych przed ETPC w zakresie, w jakim orzekł[12] on, że Konwencja o ochronie praw człowieka i podstawowych wolności wymaga od krajowego ustawodawstwa, aby ustawa definiowała:

1) kategorię osób, wobec których można stosować kontrolę operacyjną, na podstawie nakazu sądu;
2) rodzaj przestępstw, wobec których można taki nakaz wydać;
3) maksymalną długość czasu kontroli;
4) procedurę raportów o treści zarejestrowanych rozmów (w sprawach chodziło o podsłuchy telefoniczne);
5) środki gwarantujące przekazanie zapisów w stanie nienaruszonym i w całości umożliwiającym ich skontrolowanie przez sędziego i obronę;
6) określenie wypadków gdy zapisy mogą lub muszą być zniszczone, zwłaszcza gdy śledztwo umorzono lub sąd uniewinnił skazanego.

Należy również zaznaczyć, że Rzecznik Praw Obywatelskich podejmował szereg inicjatyw dotyczących spraw inwigilacyjnych. Zainicjował między innymi w 2011 roku postępowanie przed Trybunałem Konstytucyjnym (sprawa o sygn. akt K 23/11[13]), w wyniku którego Trybunał stwierdził niekonstytucyjność części zaskarżonych wówczas przepisów. W uzasadnieniu wyroku[14] w powołanej powyżej sprawie, TK stwierdził, że **konstytucyjną ochroną wynikającą z art. 47, art. 49 i art. 51 ust. 1 Konstytucji RP objęte są wszelkie sposoby przekazywania wiadomości, w każdej formie**

[11] Również w wyroku TK z 23.06.2009 r., sygn. akt K 54/07, OTK z 2009 r., Nr 6/A, poz. 86.
[12] Wyroki ETPC z 24.04.1990 r. w sprawie *Kruslin przeciwko Francji*, skarga nr 11801/85 oraz w sprawie *Huvig przeciwko Francji*, skarga nr 11105/84.
[13] Zawisłe przed Trybunałem Konstytucyjnym sprawy oznaczone sygnaturami akt: K 23/11, K 29/11, K 34/11, K 15/12, K 21/12 i K 28/12 połączone zostały do rozpoznania pod wspólną sygnaturą: K 23/11 (wnioski RPO dostępne na stronie internetowej https://ipo.trybunal.gov.pl/ipo/view/sprawa.xhtml?&pokaz=dokumenty&sygnatura=K%2023/11, dostęp 02.01.2022).
[14] Wyrok TK z 30.07.2014 r., sygn. akt K 23/11, OTK ZU 7A/2014, poz. 80.

komunikowania się, bez względu na fizyczny ich nośnik (np. rozmowy osobiste i telefoniczne, korespondencja pisemna, faks, wiadomości tekstowe i multimedialne, poczta elektroniczna) Trybunał przedstawił bardzo obszerną argumentację uzasadniającą konieczność stosowania przez służby różnych metod operacyjnych. Bez wątpienia bowiem rozwój nowych technologii oraz zagrożenia z nimi związane generują potrzebę powierzenia wyspecjalizowanym organom władzy publicznej, jakimi są służby policyjne i służby ochrony państwa, adekwatnych uprawnień, dzięki którym będą one w stanie zapobiegać przestępstwom i je wykrywać, ścigać ich sprawców, a także dostarczać informacji na temat zagrożeń dóbr prawnie chronionych. Demokratyczne państwo prawa nie może bowiem ignorować rosnącego znaczenia nowych technologii, a ponadto skali ich wykorzystywania, niekiedy również w celu naruszania prawa. Komunikaty zaś przekazywane za pośrednictwem sieci teleinformatycznych w postaci rozmów telefonicznych, wiadomości tekstowych lub multimedialnych, a nawet metadane dotyczące nawiązywanego połączenia (dane o ruchu i lokalizacji), pozwalają na taką rekonstrukcję społecznych zachowań jednostek objętych obserwacją, że nie ma potrzeby osobistego prowadzenia działań operacyjnych wymagających zaangażowania wielu osób, długiego czasu oraz ponadprzeciętnej ostrożności przed dekonspiracją.

Rzecznik Praw Obywatelskich nie kwestionuje zatem, zgodnie z utrwalonym orzecznictwem Trybunału Konstytucyjnego, potrzeby prowadzenia takich działań w sytuacjach, które są uzasadnione i przy założeniu, że działania te podejmowane są zgodnie z zasadą proporcjonalności. Ponadto Rzecznik pragnie przypomnieć, że w omawianym wyroku TK zwrócił również uwagę na to, że niejawne pozyskiwanie informacji o jednostkach w toku czynności operacyjno-rozpoznawczych musi być środkiem subsydiarnym, a więc stosowanym wówczas, gdy inne rozwiązania są nieprzydatne lub nieskuteczne. To znaczy, że niejawna ingerencja w wolności i prawa, ma stanowić w demokratycznym państwie środek ostateczny (*ultima ratio*).

Wskazując na elementy, które powinien uwzględnić ustawodawca projektując przyszłe przepisy Trybunał w sprawie o sygn. akt K 23/11 wskazał również na potrzebę **wprowadzenia obowiązku poinformowania jednostki o podjętych wobec niej działaniach operacyjno-rozpoznawczych oraz pozyskaniu informacji na jej temat, i to bez względu na to, czy były to osoby podejrzane o naruszenie prawa, czy osoby postronne, które przypadkowo stały się obiektem kontroli**. Powiadomienie jednostki na etapie wykonywania działań operacyjno-rozpoznawczych i gromadzenia informacji, co oczywiste, narażałoby je na nieskuteczność, wobec czego **ustawodawca winien zagwarantować późniejsze poinformowanie o tym fakcie.** Zapewnienie informacji jest bowiem przesłanką skorzystania przez jednostki z wynikającego z art. 51 ust. 3 Konstytucji RP prawa dostępu do urzędowych dokumentów i zbiorów danych. Co do zasady, wszystkie zgromadzone i przetwarzane przez władze publiczne dane o jednostce – chociażby nawet

nie tworzyły jednego zorganizowanego zbioru – powinny być udostępniane tej osobie, jeżeli wystąpi ona ze stosownym żądaniem. Warunkiem podstawowym skorzystania z prawa unormowanego w art. 51 ust. 3 Konstytucji RP jest wiedza o zgromadzeniu określonych danych i istnieniu ich zbioru. Zaniechanie poinformowania o zebraniu o jednostkach informacji przez władze publiczne samo w sobie stanowi naruszenie art. 51 ust. 3 i 4 Konstytucji RP. Skoro jednostka nie wie o zebraniu na jej temat określonych informacji – ponieważ dokonało się to w sposób niejawny, bez jej wiedzy i zgody – nie dysponuje możliwością uzyskania dostępu do nich i nie może żądać ich sprostowania lub usunięcia na warunkach określonych w art. 51 ust. 4 Konstytucji RP. Obowiązek informacyjny w powyższym zakresie ma eliminować ryzyko niekontrolowanego tworzenia oraz utrzymywania zbiorów danych nieprzydatnych dla postępowań prowadzonych przez organy państwa, lecz potencjalnie wartościowych z punktu widzenia przyszłych, bliżej nieokreślonych czynności.

Ponadto Trybunał Konstytucyjny przypomniał również późniejsze (niż w sprawie o sygn. akt K 32/04) orzecznictwo ETPC, zgodnie z którym w ustawie regulującej kwestie inwigilacyjne sprecyzowane muszą być przesłanki niejawnego pozyskiwania informacji i dotyczyć one mogą wyłącznie wykrywania i ścigania poważnych przestępstw oraz zapobiegania im[15], a także konieczności unormowania w ustawie procedury zarządzenia czynności operacyjno-rozpoznawczych, obejmującej w szczególności wymóg uzyskania zgody niezależnego organu na niejawne pozyskiwanie informacji[16].

Należy przypomnieć, że w związku z wyrokiem w sprawie o sygn. akt K 32/04 stwierdzającym częściową niekonstytucyjność zaskarżonych przepisów **Trybunał Konstytucyjny wydał postanowienie sygnalizacyjne**[17] **mające na celu zasygnalizowanie Sejmowi RP potrzebę podjęcia inicjatywy ustawodawczej w przedmiocie zagwarantowania w ustawie o Policji konstytucyjnych praw osób poddanych kontroli operacyjnej**. W przedmiotowej sygnalizacji wskazano na nieprzekraczalne „warunki brzegowe", które uchronią od zarzutu niekonstytucyjności regulację ustawową działań operacyjnych Policji, nieodzownych we współczesnym państwie. Sygnalizacja miała również charakter prewencyjny i jej zadaniem było ułatwienie ustawodawcy dokonania ewentualnej korekty ustaw nieobjętych kontrolą konstytucyjności, w których znajdują się zbliżone do uchylonych przepisy. W tym celu w postanowieniu tym TK podkreślił, że nie jest możliwy zabieg interpretacyjny polegający na tym, że następczą zgodę sądu na „zachowanie

[15] Wyroki ETPC z 29.06.2006 r. w sprawie *Weber i Saravia przeciwko Niemcom*, skarga 54934/00 oraz z 10.02.2009 r. w sprawie *Iordachi i inni przeciwko Mołdawii*, skarga nr 25198/02.
[16] Wyrok ETPC z 02.09.2010 r. w sprawie *Uzun przeciwko Niemcom*, skarga nr 35623/05.
[17] Postanowienie TK z 25 stycznia 2006 r., sygn. akt S 2/06.

nielegalnie zebranych materiałów operacyjnych" uzna się za wystarczającą do uznania, że zarazem zostały one w sposób legalny „zebrane" – czego bezspornie wymaga art. 51 ust. 4 Konstytucji RP.

Należy również przypomnieć, że Najwyższa Izba Kontroli już w 2013 roku[18] wskazywała w informacji o wynikach kontroli, iż *„[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*". Wnioski kontroli były spójne z poglądami ówczesnego Rzecznika Praw Obywatelskich, który już wcześniej podejmował działania w tym zakresie, w tym omówioną wcześniej kontrolę abstrakcyjną przepisów ustawy o Policji zainicjowaną przez Rzecznika.

W grudniu 2015 roku do laski marszałkowskiej wpłynął poselski projekt ustawy, która w ocenie wnioskodawców miała dostosowywać system prawa do wyroku TK w sprawie o sygn. akt K 23/11 (druk nr 154)[19]. Projekt ustawy przewidywał nowelizację: ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2015 r. poz. 355 ze zm.), ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2014 r. poz. 1402 ze zm.), ustawy z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2015 r. poz. 553 ze zm.), ustawy z dnia 21 sierpnia 1997 r. – Prawo o ustroju sądów wojskowych (Dz. U. z 2012 r. poz. 952 ze zm.), ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych (Dz. U. z 2015 r. poz. 133 ze zm.), ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. z 2013 r. poz. 568 ze zm.), ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2015 r. poz. 1929 ze zm.), ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną

[18] Kontrola nr P/12/191 – „*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*" z 2013 r. (https://www.nik.gov.pl/plik/id,5421,vp,7038.pdf, dostęp 30.12.2021).

[19] Projekt dostępny na stronie internetowej Sejmu RP https://www.sejm.gov.pl/sejm8.nsf/druk.xsp?nr=154 (dostęp 03.01.2021). Podobny projekt został złożony do Sejmu 29.07.2015 r. jako senacka inicjatywa ustawodawcza (https://www.sejm.gov.pl/sejm7.nsf/PrzebiegProc.xsp?id=EFEA200545F64605C1257E9200487C8A, dostęp 04.01.2022)

(Dz. U. z 2013 r. poz. 1422 ze zm.), ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243 ze zm.), ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2014 r. poz. 253 ze zm.), ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2014 r. poz. 1411 ze zm.), ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej (Dz. U. z 2013 r. poz. 1404 ze zm.). Projekt ustawy został krytycznie przyjęty przez organizacje pozarządowe zajmujące się ochroną praw człowieka, w szczególności prawa do prywatności[20]. Ponadto Generalny Inspektor Ochrony Danych Osobowych w konkluzji swojej opinii wskazał na to, że zaproponowane przepisy nie stwarzają wystarczających gwarancji ochrony prywatności i tajemnicy komunikowania się obywateli, a tym samym nie stanowią pełnej realizacji wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r. (sygn. akt K 23/11)[21]. Rzecznik Praw Obywatelskich natomiast, niezależnie od prac parlamentarnych, zgłosił swoje uwagi i zastrzeżenia do projektowanych przepisów Ministrowi Cyfryzacji[22], gdyż część zmian wprowadzanych w projektowanej nowelizacji dotyczyła dostępu przez Policję i inne wymienione w powyższych przepisach służby do danych internetowych w ramach czynności operacyjno-rozpoznawczych.

Ustawa z dnia 5 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz. U. poz. 147) **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. Oznaczać to może ryzyko poważnych nadużyć. Służby mogą na tej podstawie między innymi precyzyjnie odtwarzać różne aspekty życia prywatnego obywatela, zbierać dane o trybie życia, poglądach, upodobaniach czy skłonnościach. Nie ma też realnej kontroli pobierania

[20] Uwagi HFPC, https://www.hfhr.pl/wp-content/uploads/2015/12/HFPC_opinia_ustawa_o_policji_30122015.pdf (dostęp 03.01.2022); Stanowisko Fundacji Panoptykon https://panoptykon.org/sites/default/files/leadimage-biblioteka/panoptykon_ustawa_o_policji_opinia_27.12.2015_0.pdf, (dostęp 03.01.2022).

[21] Opinia GIODO, https://bip.brpo.gov.pl/sites/default/files/Opinia_GIODO_projekt_ustawy_o_Policji.pdf (dostęp 03.01.2022).

[22] Wystąpienie Rzecznika Praw Obywatelskich do Ministra Cyfryzacji z dnia 04.01.2016, znak VII.501.178.2015.MW (https://bip.brpo.gov.pl/sites/default/files/Do_MC_ws_dostepu_sluzb_do_danych_internetowych_w_projekcie_ustawy_o_Policji_0.pdf, dostęp 03.01.2022).

danych obywateli. Sąd okręgowy ma wprawdzie prawo do kontroli, ale jedynie na podstawie zbiorczych półrocznych sprawozdań służb. Sąd nie musi, ale tylko może weryfikować, czy dane te pobrano zasadnie. Tajne sprawozdania służb nie są udostępniane jako informacja publiczna, choć zawierają informacje dotyczące liczby pozyskanych danych telekomunikacyjnych, pocztowych lub internetowych i kwalifikacji prawnej czynów, w związku z którymi o nie wystąpiono.

W lutym 2016 roku Rzecznik Praw Obywatelskich zaskarżył znowelizowane przepisy[23]. Rzecznik Praw Obywatelskich w swoim wniosku przywołał wytyczne wynikające w wcześniejszego wyroku TK w sprawie o sygn. akt K 23/11 wraz ze wskazywanym w wyroku orzecznictwem omawiając je i rozwijając. RPO zwrócił również uwagę na sprawę, którą rozstrzygnął ETPC w dniu 4 grudnia 2015 r.[24] **ETPC uznał w swoim wyroku, że doszło do naruszenia art. 8 Konwencji, a system niejawnej kontroli rozmów telefonicznych z telefonów komórkowych obowiązujący w Rosji narusza prawo do poszanowania życia prywatnego i korespondencj**i. Chociaż skarżący nie wykazał, by jego rozmowy były podsłuchiwane lub by operatorzy przekazywali jego dane nieuprawnionym osobom, to jednak ETPC postanowił o przeprowadzeniu abstrakcyjnej analizy tego prawa. Z wyroku wynika, że **ETPC zwrócił w szczególności uwagę na naruszenie standardów konwencyjnych poprzez brak:**

1) jakiegokolwiek sprecyzowania okoliczności, w jakich organy władzy mogą podsłuchiwać rozmowy obywateli,
2) prawnego nakazu zakończenia podsłuchu, gdy ustały przesłanki uzasadniające jego stosowanie,
3) uregulowania procedur przechowywania i niszczenia zarejestrowanych danych, co w praktyce oznaczało bezterminowe przechowywanie takich danych,
4) procedur zezwalania na prowadzenie niejawnej kontroli, nieuregulowanie zasad nadzoru nad prowadzeniem takiej kontroli,
5) uregulowania zasad informowania obywateli o prowadzeniu kontroli oraz środkach prawnych przysługującym obywatelom w razie podsłuchiwania ich telefonów komórkowych.

Rzecznik Praw Obywatelskich podniósł we wniosku skierowanym do TK, że zakwestionowane przepisy stanowią ingerencję w prawa rekonstruowane z art. 47 Konstytucji RP i z art. 8 Konwencji. Przepisy będące przedmiotem zarzutów RPO wzbudziły także poważne

[23] Rzecznik Praw Obywatelskich był jednak zmuszony wycofać wniosek, o którym mowa, gdyż w składzie orzekającym znalazły się osoby, których nie tylko status sędziowski, ale i bezstronność w sprawie uprawnień służb była kwestionowana. Przy tym Rzecznik podkreślił, że wycofując wniosek nie rezygnuje z działań, mających doprowadzić do tego aby zasady inwigilacji odpowiadały standardom konstytucji oraz prawa europejskiego.
[24] Wyrok ETPC 04.12.2015 r. w sprawie *Zakharov przeciwko Rosji*, skarga nr 47413/06.

wątpliwości w świetle art. 49 Konstytucji RP. Ponadto Rzecznik wskazał, iż z uwagi na to, że każda regulacja dotycząca działań władzy publicznej w obszarze czynności operacyjno-rozpoznawczych prowadzi do ograniczeń w korzystaniu z wolności i praw, ustawodawca powinien wykazać w każdym przypadku, że proponowane rozstrzygnięcie normatywne spełnia kryteria testu proporcjonalności. Ustawodawca bowiem powinien w pierwszej kolejności ustalić cel proponowanej normy, wykazać jej konieczność w świetle zamierzonego celu, jej przydatność w jego osiągnięciu, a w końcu przeprowadzić test preferencji implikowany przez kolizję między dobrem, które chce chronić, a dobrem powiązanym z prawami i wolnościami, które planowana regulacja narusza.

Ponadto należy zaznaczyć, że uchwalona w 2016 r. nowelizacja ustawy o Policji naruszyła zasady i wytyczne wskazywane również przez Trybunał Sprawiedliwości Unii Europejskiej, w szczególności w wyroku w sprawach połączonych C-293/12 i C-594/12 (dalej jako: *Digital Rights Ireland*)[25]. TSUE stwierdzając w tej sprawie nieważność tzw. dyrektywy retencyjnej[26] 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 Karty Praw Podstawowych UE** (KPP) **za spełnione i uzasadniające ingerencję w prawa podstawowe**. TSUE doszedł do wniosku, że dyrektywa retencyjna wykraczała poza to, co jest ściśle niezbędne dla osiągnięcia założonego celu. Nie przewidując jakiegokolwiek rozróżniania, ograniczania czy wyjątków obejmowała osoby, których dane zatrzymywane były nawet wtedy, gdy nie było wobec nich żadnych podstaw do wszczęcia postępowania karnego oraz brakowało jakichkolwiek dowodów – nawet pośrednich – sugerujących ich związek – nawet daleki – z poważnymi przestępstwami.

Wyrok Trybunału Sprawiedliwości UE był szeroko komentowany przede wszystkim w związku z koniecznością poddania głębokiej analizie między innymi polskiego ustawodawstwa[27]. TSUE wskazał bowiem na szereg istotnych czynników niezbędnych dla prawidłowych regulacji dotyczących zbierania danych:

---

[25] Wyrok TSUE (Wielka Izba) z 8.04.2014 r. *w sprawach połączonych: C-293/12, Digital Rights Ireland Ltd przeciwko Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General* i C-594/12, *Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others*.

[26] Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z 15.03.2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE (Dz. Urz. UE L 105 z 2006 r., s. 54).

[27] A. Grzelak *Granica między skuteczną walką z przestępczością a prawem do prywatności i do ochrony danych osobowych – glosa do wyroku TS z 8.04.2014 r. w sprawach połączonych C-293/12 i C-594/12 Digital Rights Ireland*, Europejski Przegląd Sądowy, 07/2014, s. 45-52.

1) konieczność rozróżnienia zbierania danych osób podejrzewanych czy powiązanych z działalnością przestępczą i wszelkich innych;
2) wprowadzany okres i typ przechowywanych danych w poszczególnych sprawach musi mieć wyraźny związek z konkretnym celem ich zbierania;
3) niezbędne są prawne gwarancje przed nadużyciem danych, czy też nieuprawnionym do nich dostępem;
4) dostęp do danych musi być przedmiotem kontroli sądowej lub kontroli niezależnego organu administracyjnego.

Jakkolwiek unieważnienie dyrektywy retencyjnej nie oznaczało utraty mocy obowiązującej krajowych aktów normatywnych implementujących, to jednak wymagało od ustawodawców krajowych uwzględnienia tego wyroku przy ocenie zgodności regulacji krajowej z KPP. Nie ulega również wątpliwości, że przepisy implementujące dyrektywę retencyjną, mimo stwierdzenia jej nieważności, leżą w zakresie zastosowania prawa UE w rozumieniu art. 51 ust. 1 KPP, jako wyjątek od reguł, o których mowa w art. 15 ust. 1 dyrektywy 2002/58/WE oraz jednocześnie odstępstwo od swobód rynku wewnętrznego.

Kolejną sprawą, którą polski ustawodawca winien zbadać w kontekście konieczności przeglądu polskich przepisów inwigilacyjnych oraz potrzeby ich zmiany, jest wyrok TSUE w sprawach połączonych C-203/15 i C-698/15 (dalej jako: *Tele2*)[28]. W wyroku tym rozwinięte zostały tezy zaproponowane w wyroku *Digital Rights Ireland*, zaś tezy te szczególnie są istotne dla wykładni przepisów krajowych w państwach, które utrzymały obowiązki nałożone na operatorów telekomunikacyjnych w niezmienionym kształcie[29]. **TSUE potwierdził dotychczasowe orzecznictwo, zgodnie z którym wyjątki od prawa do prywatności muszą pozostawać w granicach tego, co jest absolutnie konieczne**[30]. TSUE w swoim orzeczeniu, wskazując na obowiązki informacyjne po stronie odpowiednich organów sięgających po dane jednostki, przywołał dwa bardzo ważne wyroki ETPC, omówiony już wyżej wyrok w sprawie *Zakharov przeciw*

[28] Wyrok TS z 21.12.2016 r. w sprawach połączonych C-203/15 i C-698/15 *Tele2 Sverige AB przeciwko Post- och telestyrelsen oraz Secretary of State for the Home Department przeciwko Tom Watson, Peter Brice, Geoffrey Lewis*, EU:C:2016:970.
[29] A. Grzelak *Trybunał Sprawiedliwości ponownie o relacji między koniecznością zwalczania przestępczości a prawem do prywatności – glosa do wyroku TS z 21.12.2016 r. w sprawach połączonych C-203/15 Tele2 Sverige AB oraz C-698/15 Watson, Brice, Lewis*, Europejski Przegląd Sądowy, 03/2017, str. 31-36.
[30] Również w wyrokach TSUE: z 16.12.2008 w sprawie C-73/07, Satakunnan Markkinapörssi and Satamedia, EU:C:2008:727; wyrok z 9.11.2010 r. w sprawach C-92/09 i C-93/09, Volker und Markus Schecke i Eifert, EU:C:2010:662; wyrok w sprawie Digital Rights Ireland oraz wyrok z 6.11.2015 r. w sprawie C-362/14, Schrems, EU:C:2015:650.

Rosji oraz wyrok w sprawie *Szabó i Vissy przeciwko Węgrom*[31]. Odnosząc się do drugiego z przywołanych wyroków należy wskazać, iż ETPC zaznaczył w nim również, że kontrola sądowa sprawowana w trybie następczym może okazać się wystarczającym środkiem chroniącym przed arbitralnością władzy tylko, jeżeli nie jest przeprowadzana w sposób fragmentaryczny i wyrywkowy.

W wyroku w sprawie *Tele2* TSUE rozwinął, zasygnalizowany już w wyroku w sprawie *Digital Rights Ireland*, wątek dotyczący konieczności zapewnienia uprzedniej kontroli dokonywanej przez sąd bądź niezależny organ administracji dokonywanej na wniosek organów prowadzących postępowania karne. **Dopuszczenie kontroli następczej w ocenie TSUE może być uzasadnione jedynie w sytuacjach pilnych**. Trybunał Konstytucyjny w sprawie o sygn. akt K 23/11 wskazał jedynie, że uprzednia kontrola uzasadniona może być w przypadku prowadzenia działań operacyjnych wobec szczególnej kategorii podmiotów, nie zaś wszystkich podmiotów co do zasady. W tym zakresie orzecznictwo TSUE wyznaczyło zatem nieco szerszy parasol ochronny nad jednostkami.

Kolejne ważne dla pożądanego kształtu polskiej regulacji inwigilacyjnej orzecznictwo Trybunału Sprawiedliwości UE to wyroki w sprawie C-623/17 (dalej jako: *Privacy International*)[32] oraz w sprawach połączonych C-511/18, C-512/18 i C-520/18 (dalej jako: *La Quadrature du Net*)[33]. W powyższych wyrokach TSUE zajmował się działalnością agencji wywiadowczych i potwierdził, że zakresem stosowania dyrektywy 2002/58/WE objęte jest uregulowanie krajowe umożliwiające organowi państwa zobowiązanie dostawców usług łączności elektronicznej do przekazywania danych służbom wywiadu i bezpieczeństwa narodowego. Ponadto TSUE wskazał, że art. 15 ust. 1 dyrektywy 2002/58/WE w związku z art. 4 ust. 2 TUE, a także art. 7, art. 8, art. 11 oraz art. 52 ust. 1 ust. 1 KPP należy interpretować w taki sposób, że stoi on na przeszkodzie uregulowaniu krajowemu umożliwiającemu organowi państwa nałożenie na dostawców usług łączności elektronicznej obowiązku uogólnionego i niezróżnicowanego transmitowania służbom wywiadu i bezpieczeństwa danych o ruchu i danych o lokalizacji do celów ochrony bezpieczeństwa narodowego. **Nie ulega zatem wątpliwości, że uchwalone w 2016 roku krajowe przepisy zwiększające uprawnienia inwigilacyjnie polskich służb wraz z jednoczesnym brakiem działań naprawczych dotyczących obowiązków nałożonych na operatorów telekomunikacyjnych nie**

[31] Wyrok ETPCz z 12.01.2016 r. w sprawie *Szabó i Vissy przeciwko Węgrom*, skarga nr 37138/14.
[32] Wyrok TSUE z 6.10.2020 r. w sprawie C-623/17, Privacy International przeciwko Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service, EU:C:2020:790.
[33] Wyrok TSUE z 6.10.2020 r. w sprawach połączonych C-511/18, C-512/18 i C-520/18, La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net przeciwko Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées oraz Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX przeciwko Conseil des ministres, EU:C:2020:791.

wypełniają standardów wyznaczonych w orzecznictwie TSUE oraz ETPC[34]**, co również podkreślane jest w doktrynie**[35].

Konsekwencje zaś takiego stanu rzeczy mogą oznaczać kwestionowanie w postępowaniu karnym dopuszczalności zgromadzonych dowodów, czy wręcz podnoszenia naruszenia prawa do sprawiedliwego procesu. Połączenie funkcji Ministra Sprawiedliwości i Prokuratora Generalnego, zgodnie z orzecznictwem TSUE[36], nie daje gwarancji niezależności organów prokuratorskich. Autoryzacja zatem stosowania środków inwigilacyjnych przez polską prokuraturę, wobec której podnoszone mogą być wątpliwości w zakresie jej niezależności[37], nie mogą być również uznane jako realizujące wymóg kontroli *ex-ante*, o której jest mowa w wyroku TSUE w sprawie C-746/18[38], mającej za przedmiot wniosek o wydanie, na podstawie art. 267 TFUE, orzeczenia w trybie prejudycjalnym, złożony przez Riigikohus (Sąd Najwyższy Estonii) w postępowaniu karnym. Trybunał Sprawiedliwości UE wskazał w tej sprawie na brak możliwości stosowania dowodów pochodzących z niezgodnej z prawem inwigilacji, jeżeli jednostce nie zapewniono możliwości podważenia przedstawionych dowodów na drodze sądowej. Potwierdził również, że określenie przepisów dotyczących dopuszczalności i oceny dowodów w ramach postępowania karnego zależy wyłącznie do materii prawa krajowego, co jest bezpośrednim skutkiem braku ustanowienia wspólnych norm unijnych w tej dziedzinie. **Niezależnie jednak od powyższego TSUE wskazał, że poszanowanie zasady skuteczności prawa UE stoi na przeszkodzie dopuszczeniu w postępowaniu karnym dowodów zgromadzonych w sposób niezgodny z Kartą Praw Podstawowych UE**. TSUE wskazał bowiem w swoim orzeczeniu, że „*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*".

Mając na uwadze powyższe wskazać należy na konieczność przeanalizowania przydatności oraz legalności (w świetle wszystkich wcześniejszych rozważań) **pozyskiwania różnego rodzaju danych.** Uchwalona w dniu 15 stycznia 2016 r. ustawa o zmianie ustawy o Policji

---

[34] Zob. także jeden z najnowszych wyroków: wyrok ETPC z 25.05.2021 r., skargi nr 58170/13, 62322/14 i 24960/15, *Big Brother Watch i in. przeciwko Zjednoczonemu Królestwu*.

[35] A. Grzelak, K. S. Zielińska *Między prawem do prywatności i ochrony danych osobowych a zapewnieniem bezpieczeństwa publicznego i walką z przestępczością. Problemu retencji danych ciąg dalszy – glosa do wyroków Trybunału Sprawiedliwości z 6.10.2020 r.: C-623/17, Privacy International, oraz w sprawach połączonych C-511/18, C-512/18, C-520/18, La Quadrature du Net i in.*, Europejski Przegląd Sadowy, 07/2021, s. 28-36.

[36] Wyrok TSUE z 27.05.2019 r. w sprawach połączonych C-508/18 i C-82/19 PPU, *Parquet de Lübeck*, EU:C:2019:456.

[37] M. Rojszczak *Polskie przepisy inwigilacyjne w świetle najnowszego orzecznictwa Trybunału Sprawiedliwości – wnioski krytyczne po wyroku Trybunału Sprawiedliwości z 2.03.2021 r., C-746/18, postępowanie karne przeciwko H.R.*, Europejski Przegląd Sądowy, 11/2021, s. 48-59.

[38] Wyrok TS z 2.03.2021 r. C-746/18, postępowanie karne przeciwko H.K., EU:C:2021:152.

oraz niektórych innych ustaw zmieniła również przepisy o Straży Granicznej, Żandarmerii Wojskowej i wojskowych organach porządkowych, o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu, o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego, o Centralnym Biurze Antykorupcyjnym. W wyniku tej nowelizacji powyższe służby uzyskały 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 powyższe służby uzyskały dostęp to:**

1) dane telekomunikacyjne – na podstawie art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2021 r. poz. 576);
2) dane pocztowe – na podstawie art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. z 2020 r. poz. 1041);
3) dane internetowe – na podstawie art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344).

W przepisach inwigilacyjnych uchwalonych w 2016 roku dostęp do metadanych pochodzących z łączności elektronicznej nie jest w ogóle poprzedzony jakąkolwiek formą kontroli wstępnej, a kontrola następcza ma charakter ogólny i jest przeprowadzana raz na sześć miesięcy, co sprawia, iż jest to kontrola iluzoryczna, pozbawiona możliwości rzetelnej oceny sytuacji (bo prowadzona w formie analizy sprawozdań). Należy również zaznaczyć, że w powołanej już wcześniej sprawie *Szabó i Vissy przeciwko Węgrom* ETPC ocenił wartość kontroli sprawowanej wyrywkowo i fragmentarycznie jako niewystarczającą.

Należy wskazać, że uchwalone w 2016 roku przepisy mimo wycofanego z TK wniosku, o którym mowa była wcześniej, budzą nadal bardzo poważne wątpliwości Rzecznika Praw Obywatelskich w zakresie ich zgodności z art. 30, 47, 49, 51 ust. 2 Konstytucji RP w zw. z art. 2 Konstytucji RP statuującym zasadę ochrony zaufania do państwa i stanowionego przez nie prawa. Ponadto, w ocenie Rzecznika, naruszają one również zasadę określoności przepisów prawa poprzez odwołanie się do definicji pojęcia „dane internetowe", które nie jest jasne i precyzyjne, wobec czego normy te naruszają wymóg przewidywalności przepisów ograniczających prawo do prywatności, prawo do ochrony danych osobowych oraz zasadę autonomii informacyjnej jednostki. 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 . 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 usługobiorca, informacje o rozpoczęciu, zakończeniu oraz zakresie każdorazowego korzystania z usługi świadczonej drogą elektroniczną, informacje o skorzystaniu przez usługobiorcę z usług świadczonych drogą elektroniczną.

Przypomnieć w tym miejscu należy, że prawo określające granice ingerencji państwa w prawa człowieka i obywatela musi spełniać określone wymogi jakościowe. Musi być ono dostępne oraz przewidywalne dla jednostek, zaś z prawa muszą także 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.

Ponadto należy przypomnieć, że nie tylko Rzecznik Praw Obywatelskich oraz organizacje pozarządowe kwestionowali uchwalone w 2016 roku przepisy inwigilacyjne. W czerwcu 2016 r. również Komisja Wenecka[39] 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 zaś składania sądom ogólnych sprawozdań przez służby będzie nieskuteczny. Komisja Wenecka zaleciła m. in. by pozyskiwanie najważniejszych danych telekomunikacyjnych i internetowych ograniczyć do najgroźniejszych sytuacji, aby skrócić czas przechowywania danych oraz zadbać o nienaruszanie tajemnicy adwokackiej.

Odnotować również należy, że Rzecznik Praw Obywatelskich w dniu 10 grudnia 2021 roku[40] zgłosił swój udział w postępowaniu przed Trybunałem Konstytucyjnym w sprawie skargi konstytucyjnej (sygn. akt SK 60/21). W sprawie tej Rzecznik wniósł o stwierdzenie, że art. 19 ust. 20 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2021 r. poz. 1882) w zakresie, w jakim przepis ten nie przyznaje osobie, wobec której stosowana była kontrola operacyjna, prawa wniesienia zażalenia na postanowienie sądu w przedmiocie stosowania tej kontroli, jest niezgodny z art. 45 ust. 1 oraz art. 78 w zw. z art. 176 ust. 1 Konstytucji RP. Po zakończonej kontroli operacyjnej bowiem obywatel winien mieć prawo do złożenia zażalenia na decyzje sądu w zakresie przeprowadzonych względem niego czynności operacyjnych. Zgodnie natomiast z obecnie obowiązującym stanem prawnym, obywatel nie jest informowany o zarządzonej wobec niego kontroli operacyjnej. Brak zapewnienia jednostce uprawnienia polegającego na możliwości zaskarżenia decyzji sądu, a tym samym na następcze uzyskanie informacji o prowadzonych czynnościach operacyjnych jest niezgodny z konstytucyjnymi standardami, w szczególności z prawem do zaskarżalności i zasadą dwuinstancyjności postępowania.

Konstytucyjny standard zaskarżalności orzeczeń określony jest w art. 176 ust. 1 oraz art. 78 Konstytucji RP. Art. 176 ust. 1 Konstytucji RP gwarantuje, że postępowanie sądowe jest co najmniej dwuinstancyjne, z kolei art. 78 Konstytucji RP, że każda ze stron ma prawo do zaskarżania orzeczeń i decyzji wydanych w pierwszej instancji. Wyjątki zaś od zasady zaskarżalności oraz tryb zaskarżania

[39] *Poland - Opinion on the Act of 15 January 2016 amending the Police Act and certain other Acts, adopted by the Venice Commission at its 107th Plenary Session* (Venice, 10-11 June 2016), CDL-AD(2016)012-e (https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD%282016%29012-e, dostęp 05.01.2022).
[40] Pismo RPO do TK z 10.12.2021 r., znak II.511.810.2021.MM (https://bip.brpo.gov.pl/sites/default/files/2021-12/Stanowisko_RPO_inwigilacja_TK%2C10.12.2021.pdf, dostęp 06.01.2022).

określa ustawa[41]. Konstytucyjna zasada dwuinstancyjności postępowania sądowego zakłada w szczególności:

1) dostęp do sądu drugiej instancji, a co za tym idzie przyznanie stronom odpowiednich środków zaskarżenia, które uruchamiają rzeczywistą kontrolę rozstrzygnięć wydanych przez sąd pierwszej instancji;
2) powierzenie rozpoznania sprawy w drugiej instancji - co do zasady - sądowi wyższego szczebla, a w konsekwencji nadanie środkowi zaskarżenia charakteru dewolutywnego;
3) odpowiednie ukształtowanie procedury przed sądem drugiej instancji, tak aby sąd ten mógł wszechstronnie zbadać rozpoznawaną sprawę i wydać rozstrzygnięcie merytoryczne. Dwuinstancyjność postępowania sądowego ma na celu zapewnienie zapobiegania pomyłkom i arbitralności w pierwszej instancji[42].

Należy również przypomnieć raport grupy ekspertów[43], który opracowany został w 2019 roku, na zaproszenie Rzecznika Praw Obywatelskich. W raporcie tym przedstawione zostały postulaty najważniejszych zmian ustrojowych oraz legislacyjnych, które mogłyby doprowadzić do respektowania zasad konstytucyjnych w kontekście działalności służb specjalnych. Raport oparto na założeniu, że nadzór nad służbami to element sprawnie funkcjonującego państwa, w którym funkcjonowanie służb jest również niezbędne. Celem zatem przygotowanego dokumentu nie było ograniczanie skuteczności działania służb, lecz znalezienie optymalnej równowagi między ochroną praw i wolności obywatelskich a przeciwdziałaniem zagrożeniom dla bezpieczeństwa państwa oraz porządku publicznego, w szczególności związanych z działalnością terrorystyczną, działalnością obcych służb oraz działalnością przestępczą.

Wobec powyższego oraz mając na uwadze dotychczasowe zaangażowanie Rzecznika Praw Obywatelskich w sygnalizowanie problemów wynikających z utrzymywania w mocy przepisów inwigilacyjnych budzących szereg omówionych w niniejszym piśmie wątpliwości, 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 ze zm.), **zwracam się do Pana Premiera o podjęcie pilnych działań mających**

[41] Wyrok TK z 2.06.2010 r., sygn. akt SK 38/09, OTK ZU 5A/2010, poz. 46.
[42] Wyrok TK z 9.02.2010 r., sygn. akt SK 10/09, OTK ZU 2A/2010, poz. 10.
[43] A. Bodnar, T. Borkowski, J. Cichocki, W. Klicki, P. Kładoczny, A. Rapacki, Z. Rudzińska-Bluszcz, *Osiodłać Pegaza. Przestrzeganie praw obywatelskich w działalności służb specjalnych – założenia reformy*, Warszawa, 2019 (https://panoptykon.org/sites/default/files/osiodlac_pegaza_jak_powinien_wygladac_nadzor_nad_sluzbami._raport_ekspertow.pdf, dostęp 06.01.2022).

na celu dostosowanie obowiązującego w tym zakresie stanu prawnego do standardów konstytucyjnych oraz europejskich.

Jednocześnie uprzejmie proszę o przekazanie Rzecznikowi wszelkich informacji o podjętych do tej pory działaniach, w szczególności o rozpoczętych analizach i pracach legislacyjnych poprzedzających opracowanie stosownego projektu aktu normatywnego, o ile takie zostały podjęte. Ponadto uprzejmie proszę o szczegółowe odniesienie się do wszystkich kwestii oraz wątpliwości podniesionych przez Rzecznika w niniejszym wystąpieniu.

Łączę wyrazy szacunku

Marcin Wiącek

Rzecznik Praw Obywatelskich

/-podpisano elektronicznie/

<u>Do wiadomości:</u>

Pan Marian Banaś

Prezes Najwyższej Izby Kontroli

ePUAP