



Warszawa, 06-01-2023 r.

**RZECZNIK PRAW OBYWATELSKICH**

**Marcin Wiącek**

**VII.501.306.2021.KSZ**

**Szanowny Pan**  
**Mariusz Kamiński**  
**Minister Spraw Wewnętrznych**  
**i Administracji**  
**e-PUAP**

*Szanowny Panie Ministrze,*

uprzejmie dziękuję za odpowiedzi na moje wystąpienia<sup>1</sup> dotyczące niezgodności przepisów inwigilacyjnych ze standardami – odpowiednio – konstytucyjnym, określonym przez polski Trybunał Konstytucyjny (dalej jako: TK), oraz międzynarodowym i unijnym, określanymi w orzecznictwie Europejskiego Trybunału Praw Człowieka (dalej jako: ETPC, Trybunał) oraz Trybunału Sprawiedliwości Unii Europejskiej (dalej jako: Trybunał Sprawiedliwości, TSUE). Obszerna odpowiedź<sup>2</sup> ze strony Pana Ministra, stanowiąca zestawienie opinii wielu podmiotów, poddana została przeze mnie wnikliwej analizie. W związku z tym pragnę przedstawić następujące uwagi:

---

<sup>1</sup> Pisma RPO z 13.01.2022 r. oraz 13.07.2022 r. ([https://bip.brpo.gov.pl/sites/default/files/2022-01/Do\\_premiera\\_zasady\\_inwigilacji\\_13.1.2022.pdf](https://bip.brpo.gov.pl/sites/default/files/2022-01/Do_premiera_zasady_inwigilacji_13.1.2022.pdf), [https://bip.brpo.gov.pl/sites/default/files/2022-07/Do\\_PRM\\_inwigilacja\\_ponowienie\\_13.07.2022.pdf](https://bip.brpo.gov.pl/sites/default/files/2022-07/Do_PRM_inwigilacja_ponowienie_13.07.2022.pdf), dostęp 13.12.2022).

<sup>2</sup> Pismo MSWiA z 01.08.2022 r. ([https://bip.brpo.gov.pl/sites/default/files/2022-08/Odpowiedz\\_MSWiA\\_zasady\\_inwigilacji\\_1.08.2022.pdf](https://bip.brpo.gov.pl/sites/default/files/2022-08/Odpowiedz_MSWiA_zasady_inwigilacji_1.08.2022.pdf), dostęp 13.12.2022).

Nie mogę podzielić tezy, zgodnie z którą „*obowiązujący obecnie model stosowania metod pracy operacyjnej, takich jak kontrola operacyjna czy uzyskiwanie danych telekomunikacyjnych, został wypracowany w wyniku wdrożenia do polskiego porządku prawnego wyroku Trybunału Konstytucyjnego sygn. K 23/11 z dnia 30 lipca 2014 r., która przyjęła formę ustawy z 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw*”. Informację zaś, zgodnie z którą „*zasady działania służb nie ulegną zmianie i będzie obowiązywał podobny model postępowania przy uzyskiwaniu danych telekomunikacyjnych, internetowych i pocztowych. Natomiast wejście w życie art. 47 i art. 49 projektu PKE [Prawa komunikacji elektronicznej]<sup>3</sup> pozwoli na skuteczniejszą reakcję na przestępczość związaną z funkcjonowaniem sieci Internet*” przyjmuję do wiadomości i deklaruję, że z mojej strony podejmowane będą kolejne próby wykazania potrzeby zmiany tego stanu rzeczy z uwagi na konieczność zapewnienia ochrony praw człowieka.

Nie wdaję się w polemikę dotyczącą odmiennych stanowisk w zakresie spełniania przez polskie przepisy wytycznych zawartych w orzecznictwie TK<sup>4</sup>, a także w

---

<sup>3</sup> W zakresie opinii dotyczącej projektowanych przepisów zob.: K. S. Zielińska, „*Powracający problem retencji danych telekomunikacyjnych. Potrzeba zapewnienia bezpieczeństwa narodowego czy może chęć utrzymania niekontrolowanej inwigilacji? – glosa do wyroku Trybunału Sprawiedliwości z 5.04.2022 r., C-140/20, G.D. przeciwko The Commissioner of the Garda Síochána i in.*”, Europejski Przegląd Sądowy, 11/2022, str. 47-48.

<sup>4</sup> Wyroki TK: 1) z 12.11.2002 r., sygn. akt SK 40/01, OTK ZU nr 6/A/2002, poz. 81; 2) z 20.11.2002 r., sygn. akt K 41/02, OTK ZU nr 6/A/2002, poz. 83; 3) z 20.06.2005 r., sygn. akt K 4/04, OTK ZU 6A/2005, poz. 64; 4) z 12.12.2005 r., sygn. akt K 32/04, OTK ZU 11A/2005, poz. 132; 5) z 23.06.2009 r., sygn. akt K 54/07, OTK z 2009 r., Nr 6/A, poz. 86; 6) z 2.06.2010 r., sygn. akt SK 38/09, OTK ZU 5A/2010, poz. 46; 7) z 9.02.2010 r., sygn. akt SK 10/09, OTK ZU 2A/2010, poz. 10; 8) z 30.07.2014 r., sygn. akt K 23/11, OTK ZU 7A/2014, poz. 80 (dalej: wyrok TK w sprawie K 23/11), a także postanowienie sygnalizacyjne z 25 stycznia 2006 r., sygn. akt S 2/06.

orzecznictwie ETPC<sup>5</sup> oraz Trybunału Sprawiedliwości<sup>6</sup>, chciałbym przywołać kolejne argumenty przemawiające za koniecznością dokonania głębokiej refleksji nad stanem prawodawstwa w tym zakresie.

We wrześniu 2022 r. Trybunał Sprawiedliwości orzekł w dwóch kolejnych sprawach obejmujących problematykę retencji danych<sup>7</sup>. Trybunał orzekł, że art. 12 ust. 2 lit. a i d dyrektywy 2003/6/WE Parlamentu Europejskiego i Rady z dnia 28 stycznia 2003 r. w sprawie wykorzystywania poufnych informacji i manipulacji na rynku (nadużyć na rynku) oraz art. 23 ust. 2 lit. g i h rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 596/2014 z dnia 16 kwietnia 2014 r. w sprawie nadużyć na rynku (rozporządzenia w sprawie nadużyć na rynku) i uchylającego dyrektywę 2003/6 i dyrektywy Komisji 2003/124/WE, 2003/125/WE, 2004/72/WE, w związku z 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), zmienionej dyrektywą Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r., oraz w świetle art. 7, 8, 11 i art. 52 ust. 1 Karty Praw Podstawowych Unii Europejskiej należy interpretować w ten sposób, że **sprzeciwiają się one środkom ustawodawczym przewidującym zapobiegawczo w celu zwalczania przestępstw polegających na nadużyciach na rynku, do których zalicza się wykorzystywanie**

---

<sup>5</sup> Wyroki ETPC: 1) z 02.08.1984 r. w sprawie *Malone przeciwko Zjednoczonemu Królestwu*, skarga nr 8691/79; 2) z 24.04.1990 r. w sprawie *Kruslin przeciwko Francji*, skarga nr 11801/85 oraz w sprawie *Huvig przeciwko Francji*, skarga nr 11105/84; 3) z 29.06.2006 r. w sprawie *Weber i Saravia przeciwko Niemcom*, skarga 54934/00; 4) z 10.02.2009 r. w sprawie *Iordachi i inni przeciwko Mołdawii*, skarga nr 25198/02; 5) z 02.09.2010 r. w sprawie *Uzun przeciwko Niemcom*, skarga nr 35623/05; 6) z 04.12.2015 r. w sprawie *Zakharov przeciwko Rosji*, skarga nr 47413/06; 7) z 12.01.2016 r. w sprawie *Szabó i Vissy przeciwko Węgrom*, skarga nr 37138/14.

<sup>6</sup> Wyroki TSUE: 1) z 16.12.2008 w sprawie C-73/07, *Satakunnan Markkinapörssi and Satamedia*, EU:C:2008:727; 2) z 9.11.2010 r. w sprawach C-92/09 i C-93/09, *Volker und Markus Schecke i Eifert*, EU:C:2010:662; 3) 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*; 4) z 6.11.2015 r. w sprawie C-362/14, *Schrems*, EU:C:2015:650; 5) 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; 6) 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 (dalej: wyrok TSUE w sprawie *La Quadrature du Net* i in).

<sup>7</sup> Wyrok TS z 20.09.2022 r. w sprawach połączonych C-339/20 i C-397/20, *VD i SR*, ECLI:EU:C:2022:703.

## **informacji poufnych, ogólne i niezróżnicowane zatrzymywanie danych o ruchu przez rok od dnia ich zapisu.**

Ponadto Trybunał orzekł, że prawo UE należy interpretować w ten sposób, że sprzeciwia się ono temu, by sąd krajowy ograniczył w czasie skutki stwierdzenia nieważności, którego na mocy prawa krajowego ma on dokonać w odniesieniu do przepisów krajowych, które z jednej strony nakładają na operatorów świadczących usługi łączności elektronicznej uogólniony i niezróżnicowany obowiązek zatrzymywania danych o ruchu, a z drugiej strony pozwalają na przekazywanie tych danych organowi właściwemu w sprawach finansowych bez uprzedniego zezwolenia sądu lub niezależnego organu administracyjnego, ze względu na niezgodność tych przepisów z art. 15 ust. 1 dyrektywy 2002/58, zmienionej dyrektywą 2009/136, interpretowanym w świetle Karty Praw Podstawowych Unii Europejskiej. Dopuszczalność dowodów uzyskanych na podstawie krajowych przepisów ustawowych niezgodnych z prawem Unii podlega, zgodnie z zasadą autonomii proceduralnej państw członkowskich, prawu krajowemu, z zastrzeżeniem poszanowania w szczególności zasad równowagi i skuteczności.

W konsekwencji **przepisy przewidujące prewencyjne uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych dotyczących lokalizacji do celów zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego, są sprzeczne z prawem unijnym**. TSUE zastrzegł jednocześnie, że państwa członkowskie Unii Europejskiej mogą, w celu walki z poważną przestępczością i w ścisłym poszanowaniu zasady proporcjonalności<sup>8</sup>, przewidzieć ukierunkowane czy też szybkie zatrzymywanie takich danych, jak również uogólnione i niezróżnicowane zatrzymywanie adresów IP.

Powołany wyrok potwierdził dotychczasową linię orzeczniczą w sprawach retencyjnych<sup>9</sup>. Państwa członkowskie powinny badać zarówno wagę ingerencji, którą jest ograniczenie praw i wolności, a także sprawdzać, czy znaczenie celu ogólnego, do którego zmierza to ograniczenie, pozostaje w relacji do tej wagi. Przestępczość zaś,

---

<sup>8</sup> Elementem zasady proporcjonalności jest ważenie dobra poświęcanego i dobra, któremu służy ingerencja, co określane jest mianem zbilansowania. Dla oceny dopuszczalności ingerencji ustawodawcy w prawa i wolności konstytucyjne stosowany jest trójstopniowy test proporcjonalności, sprowadzający się do udzielenia odpowiedzi na pytania: czy wprowadzona regulacja jest w stanie doprowadzić do zamierzonych przez nią skutków, czy jest ona niezbędna dla ochrony interesu publicznego, z którym jest powiązana, czy rezultaty wprowadzonej regulacji pozostają w odpowiedniej proporcji do ciężarów nakładanych na obywatela. Zob.: wyrok TK z 31 stycznia 2013 r., sygn. akt K 14/11, OTK ZU 2013, nr 1A, poz. 7.

<sup>9</sup> M. in. wyrok TSUE w sprawie La Quadrature du Net i in), a także wyrok TSUE z 5.04.2022 r., C-140/20, G.D. przeciwko The Commissioner of the Garda Síochána i in., EU:C:2022:258 (dalej: wyrok w sprawie C-140/20).

nawet szczególnie poważna, w ocenie Trybunału Sprawiedliwości, nie może być zaś utożsamiana z zagrożeniem bezpieczeństwa narodowego, gdyż takie podejście mogłoby wprowadzić kategorię pośrednią między bezpieczeństwem narodowym a bezpieczeństwem publicznym.

## II

Ponadto Trybunał Sprawiedliwości wskazał na swój wyrok w sprawie C-140/20, w szczególności odnosząc się do **konieczności wykluczenia informacji i dowodów uzyskanych z naruszeniem przepisów prawa**. Wskazał na to, że taką konieczność należy oceniać w szczególności w świetle zagrożenia, jakie dopuszczalność takich informacji i dowodów stwarza dla zasady kontrydiktoryjności, a tym samym prawa do rzetelnego procesu. Sąd, 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 bowiem stwierdzić naruszenie prawa do rzetelnego procesu i wykluczyć ten środek dowodowy. W związku z tym sąd karny ma obowiązek nieuwzględniania informacji i dowodów uzyskanych w drodze uogólnionego i nieodróżnionego 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 podejrzanych 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<sup>10</sup>.

Zarówno z postanowień Konstytucji RP (art. 47 w zw. z art. 31 ust. 3, art. 49 oraz art. 50), jak też z orzecznictwa ukształtowanego na tle art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności (dalej jako: Konwencja)<sup>11</sup> wynika standard, zgodnie z którym **w przypadku niejawnego pozyskiwania informacji o jednostce wymagana jest bardzo daleko idąca precyzja regulacji prawnej. Precyzja ta ma zapobiegać ryzyku arbitralności niejawnych działań podejmowanych przez organy władzy publicznej, które – zgodnie ze swoją specyfiką – pozostają poza zasięgiem kontroli publicznej**<sup>12</sup>. Standardu tego nie realizuje obecnie art. 168b ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. z 2022 r. poz.

---

<sup>10</sup> Także wyrok TS w sprawie *La Quadrature du Net i in.*, pkt 226, 227.

<sup>11</sup> Wyrok ETPC z 10.02.2009 r., w sprawie *Lordachi i in. przeciwko Mołdawii* (skarga nr 25198/02).

<sup>12</sup> Dla dopuszczalności wkraczania w sferę wolności i praw konstytucyjnych niezbędne jest istnienie: precyzyjnej i konkretnej podstawy prawnej ingerencji w postaci aktu rangi ustawowej, konieczności wkroczenia w sferę swobód obywatelskich rozważanej przez pryzmat wymogów demokratycznego państwa prawnego oraz celu ingerencji rozumianego jako ranga chronionego interesu publicznego. Zob.: Postanowienie SN z 26.04.2007 r., I KZP 6/07, OSNKW 2007, nr 5, poz. 37.

1375; dalej jako: kpk). Przepis ten reguluje instytucję tzw. zgody następczej na wykorzystanie w postępowaniu karnym, jako dowodów uzyskanych w wyniku inwigilacji, materiałów świadczących o popełnieniu każdego przestępstwa ściganego z urzędu lub przestępstwa skarbowego, a więc nie tylko przestępstwa ściganego z urzędu lub przestępstwa skarbowego, w stosunku do którego można zarządzić kontrolę operacyjną. W ten sposób, a więc wprowadzając nieograniczony katalog przestępstw, które uzasadniają wykorzystanie w postępowaniu karnym materiałów uzyskanych w wyniku niejawnych działań, ustawodawca nie realizuje gwarancyjnego charakteru wymienionych powyżej przepisów.

Przypomnieć należy w tym miejscu wyrok TK w sprawie o sygn. akt K 23/11, zgodnie z którym *„to ustawa ma precyzować przedmiotowe przesłanki zarządzenia takich czynności [czynności operacyjno- rozpoznawczych]. Aby zachować standard konstytucyjny, nie wystarcza odwołanie się do ogólnych zagrożeń dóbr prawnie chronionych, zwłaszcza przez zwroty niedookreślone. Ustawodawca zobowiązany jest wobec tego zdefiniować zamknięty i możliwe wąski katalog poważnych przestępstw, uzasadniających tego rodzaju ingerencję w status jednostki (...)”*<sup>13</sup>. Jak stwierdza TK, *„(...) Precyzyjne ustawowe uregulowanie przedmiotowych przesłanek dopuszczalności kontroli operacyjnej i pozyskiwania danych telekomunikacyjnych jest tym bardziej konieczne, ponieważ w istocie to same służby – działając w ramach ich ustawowych zadań – definiują zagrożenia, którym mają następnie zapobiegać. (...) przesłanki niejawnego pozyskiwania informacji o osobach mają być zdefiniowane przez ustawodawcę wyczerpująco w sposób zamknięty. (...) na podstawie brzmienia przepisu ustawy jednostka ma wiedzieć, jakie zachowania narażają ją nie tylko na ewentualną odpowiedzialność karną, lecz również umożliwią prowadzenie w stosunku do niej czynności operacyjno-rozpoznawczych, głęboko ingerujących w jej prywatność”*<sup>14</sup>.

**Obecnie natomiast nielegalnie zdobyte materiały mogą stanowić dowód w postępowaniu karnym, zaś decyzja w tym zakresie, nieobwarowana jakimikolwiek dodatkowymi warunkami, należy do prokuratora**<sup>15</sup>.

Z kolei art. 168a k.p.k. nie zabrania wykorzystania jako podstawy ustaleń faktycznych w sprawie dowodów uzyskanych z naruszeniem przepisów postępowania, wobec

---

<sup>13</sup> Wyrok TK w sprawie o sygn. akt K 23/11, pkt 5.1.3.1, s. 353.

<sup>14</sup> Ibidem, pkt 5.1.3.1, s. 354.

<sup>15</sup> Powyższe stanowisko nie jest jedynie opinią RPO, ale stanowi także utrwalony pogląd w doktrynie – zob. S. Brzozowski „Wykorzystywanie dowodów uzyskanych w toku kontroli operacyjnej w kontekście art. 168b Kodeksu postępowania karnego”, Palestra 6/2016, str. 20-26; P. Daniluk „Instytucja tzw. zgody następczej po nowelizacji z 11 marca 2016 r. w świetle standardów konstytucyjnych i konwencyjnych”, Studia Prawnicze 3 (211) 2017, str. 81-100; P. Daniluk „Jeszcze raz o konstytucyjności art. 168b kodeksu postępowania karnego (w związku z wnioskiem Prokuratora Generalnego do Trybunału Konstytucyjnego)”, Palestra 12/2020, s. 5-20.

czego jest swoistym zezwoleniem na procesowe wykorzystanie nielegalnie uzyskanych dowodów. Należy przypomnieć, że w sprawie *Hambardzumyan przeciwko Armenii* ETPC<sup>16</sup> uznał, że postanowienie sądu o kontroli operacyjnej było zbyt pobieżne i nie zawierało wskazania konkretnych środków kontroli, co doprowadziło do naruszenia art. 8 Konwencji. Skarżąca podniosła, że nie istniało ważne postanowienie sądu zezwalające na stosowanie wobec niej kontroli operacyjnej w toku postępowania przygotowawczego<sup>17</sup>. ETPC przyznał, że orzeczenie sądu nie było wystarczająco konkretne co do osoby, która ma być poddana kontroli operacyjnej. Ponadto orzeczenie nie wymieniało konkretnych środków, które miały być zastosowane wobec skarżącej, co pozostawiało służbom zbyt dużą dowolność. W związku z powyższym **poważne zastrzeżenia budzą art. 168a i art. 168b k.p.k., które pozwalają organom na wykorzystanie w postępowaniu karnym nielegalnie zebranych dowodów i pozostawiają decyzję w tym zakresie prokuratorowi.**

Należy także odnieść się do argumentu związanego z niezależnością prokuratury. Otóż w aktualnym stanie prawnym **Prokuratorowi Generalnemu przyznano niezwykle silne kompetencje w zakresie nadzoru nad prokuratorami.** W odróżnieniu od regulacji obowiązujących przed wejściem w życie ustawy – Prawo o prokuraturze<sup>18</sup>, **obecnie Prokurator Generalny jest przełożonym wszystkich prokuratorów, mogących wydawać im wiążące polecenia, także co do treści czynności procesowych<sup>19</sup>. W takim stanie prawnym prokuratora nie sposób zatem uznać za organ niezależny, skoro urząd Prokuratora Generalnego sprawuje organ władzy wykonawczej (Minister Sprawiedliwości)<sup>20</sup>.** Orzecznictwo sądów międzynarodowych odnoszące się do niezależności organu decydującego o inwigilacji

---

<sup>16</sup> Wyrok ETPC z 05.12.2019 r. w sprawie *Hambardzumyan przeciwko Armenii*, skarga nr 43478/11.

<sup>17</sup> Jedną z tez przywołanego wyroku było wskazanie na to, że sądy rozpoznające zarzut karny wobec skarżącej nie były w stanie zapewnić skutecznego środka odwoławczego w zakresie, w jakim dotyczyły one jej skarg na podstawie art. 8 Konwencji. Mimo, że sądy te były uprawnione do badania kwestii związanych z dopuszczalnością materiału dowodowego, nie były otwarte na rozpatrzenie istoty skargi, zgodnie z którą ingerencja w prawo skarżącej do poszanowania jej życia prywatnego i korespondencji nie była zgodna z prawem czy niezbędna w społeczeństwie demokratycznym. ETPC doszedł do wniosku, że podniesienie kwestii niejawnego nadzoru przed sądami badającymi zasadność sprawy karnej przeciwko skarżącej, w świetle stanu prawa krajowego i praktyki krajowej, nie może być uznane za skuteczny środek odwoławczy w odniesieniu do jej skarg na podstawie art. 8 Konwencji.

<sup>18</sup> Ustawa z dnia 28 stycznia 2016 r. – Prawo o prokuraturze (Dz. U. z 2022 r. poz. 1247 ze zm.)

<sup>19</sup> Zob. art. 13 ust. 2 w zw. z art. 7 § 3 ustawy – Prawo o prokuraturze.

<sup>20</sup> Zgodnie z brzmieniem art. 1 § 2 ustawy – Prawo o prokuraturze.

uznaje ze niewystarczające, by decyzję w tym zakresie podejmował prokurator pozostający w zależności od władzy wykonawczej<sup>21</sup>.

### III

Mając na względzie wycofanie przez Rzecznika Praw Obywatelskich VII kadencji wniosków skierowanych do Trybunału Konstytucyjnego<sup>22</sup> Rzecznik Praw Obywatelskich VIII kadencji podjął szereg innych inicjatyw mających na celu realizację postulatów dotyczących poszanowania praw człowieka w kontekście niejawnego inwigilacji, kontynuując dotychczasowe wysiłki. Do najważniejszych zaliczyć można przedstawienie stanowiska podczas rozprawy przed ETPC w dniu 27.09.2022 r. w dwóch postępowaniach przeciwko Polsce<sup>23</sup>. Jedno z nich dotyczy konieczności zapewnienia tajemnicy adwokackiej, która jest jednym z fundamentalnych elementów decydujących o faktycznym zapewnieniu prawa do otrzymania pomocy prawnej. Podstawą bowiem zaufania klienta do adwokata jest gwarancja zachowania w tajemnicy wszelkich informacji, które zostały mu przekazane w związku z udzielaniem pomocy prawnej. Tajemnica adwokacka jest nie tylko prawem profesjonalnego pełnomocnika, ale przede wszystkim obowiązkiem względem klienta<sup>24</sup>.

Dotychczasowe orzecznictwo ETPC traktuje tajemnicę adwokacką jako element systemu ochrony praw człowieka. W szczególności w sprawie *Laurent przeciwko Francji*<sup>25</sup> Trybunał orzekł, że ingerencja organów wymiaru sprawiedliwości w korespondencję klienta z adwokatem powinna być dozwolona wyłącznie w wyjątkowych przypadkach, gdy władze mają powody, by sądzić, że tajemnica adwokacka została nadużyta w celu, który zagrażałby bezpieczeństwu państwa, osób lub miałyby charakter przestępczy. W celu stwierdzenia czy powyższe powody uzasadniają taką ingerencję konieczne jest zbadanie ogółu okoliczności sprawy. W tej sprawie ocena ETPC doprowadziła do uznania przejęcia i przeczytania przez

---

<sup>21</sup> Wyrok ETPC z 26 kwietnia 2007 r. w sprawie *Dumitru Popescu przeciwko Rumunii*, skarga nr 71525/01. Także 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.

<sup>22</sup> Wniosek RPO z 18.02.2016 dotyczący nowelizacji ustawy o Policji z 2016 r. (sygn. akt K 9/16) – wycofany 14.03.2018 r., wniosek RPO z 06.05.2016 r. dotyczący dopuszczenia przed sądem dowodów zdobytych nielegalnie przez służby specjalne (sygn. akt K 27/16) – wycofany 09.04.2018 r., wniosek RPO z 11.07.2016 r. dotyczący ustawy antyterrorystycznej z 2016 r. (sygn. akt K 35/16) – wycofany 30.04.2018 r.

<sup>23</sup> Sprawa *Mikołaj Pietrzak p. Polsce*, skarga nr 72038/17 oraz sprawa *Dominika Bychawska-Siniarska i in. przeciwko Polsce*, skarga nr 25237/19

([https://www.echr.coe.int/Pages/home.aspx?p=hearings&w=7203817\\_27092022&language=lang&c=&p=y=2022](https://www.echr.coe.int/Pages/home.aspx?p=hearings&w=7203817_27092022&language=lang&c=&p=y=2022), dostęp 22.12.2022). Wcześniej, 28.07.2020 r., RPO przedstawił opinię przyjaciela sądu.

<sup>24</sup> J. Naumann, *Zbiór Zasad Etyki Adwokackiej i Godności Zawodu. Komentarz*, Warszawa 2017, s. 163.

<sup>25</sup> Wyrok ETPC z 24.5.2018 r., w sprawie *Laurent przeciwko Francji* (skarga nr 28798/13).



funkcjonariusza policji odręcznie napisanych przez adwokata notatek dla klienta za nieuzasadnione naruszenie praw wynikających z art. 8 Konwencji. Natomiast w sprawie *Kopp przeciwko Szwajcarii*<sup>26</sup>, która dotyczyła podsłuchu telefonu adwokata w związku z toczącym się przeciwko niemu postępowaniem karnym, ETPC orzekł, że także doszło do naruszenia art. 8 Konwencji, gdyż przepisy krajowe nie zapewniały możliwości odróżnienia korespondencji prawnika z klientami, która podlegałaby szczególnej ochronie właściwej tajemnicy adwokackiej, od pozostałej komunikacji prowadzonej przez prawnika, a niepodlegającej takiej ochronie.

Podkreślić także należy, że inna funkcja tajemnicy adwokackiej to funkcja gwarancyjna – zapewniająca sprawiedliwość procesu. W sprawie *Niemietz przeciwko Niemcom*<sup>27</sup> Trybunał orzekł, że ingerencja w tajemnicę zawodową może mieć wpływ na prawidłowe działanie wymiaru sprawiedliwości, a przez to na prawa wynikające z art. 6 Konwencji. W tej sprawie ETPC podkreślił, jak ważne jest oddzielenie w trakcie ewentualnego przeszukania kancelarii dokumentów, które faktycznie mogą stanowić przedmiot zainteresowania odpowiednich służb od materiałów i dokumentów objętych tajemnicą adwokacką. Z kolei w sprawie *Öcalan przeciwko Turcji*<sup>28</sup>, Trybunał orzekł, że prawo oskarżonego do komunikowania się ze swoim adwokatem bez udziału osób trzecich jest jednym z podstawowych wymogów sprawiedliwego procesu w społeczeństwie demokratycznym i wynika z art. 6 ust. 3 lit. c Konwencji.

Na szczególną natomiast uwagę zasługuje sprawa *Versini-Campinchi i Crasnianski przeciwko Francji*<sup>29</sup>, w której ETPC ocenił założenie podsłuchu i użycie treści rozmów telefonicznych adwokatów z ich klientami w postępowaniu dyscyplinarnym prowadzonym przeciwko adwokatom. W tej sprawie Trybunał ocenił, że prawo krajowe wyraźnie określało, że poszanowanie prawa do obrony wymaga poufności rozmów telefonicznych między adwokatem i jego klientem i stanowiło przeszkodę w zapisywaniu tych rozmów nawet, jeśli zostały przypadkowo nagrane przy okazji zgodnej z prawem czynności śledczej. Przepisy francuskie przewidują jednak wyjątek od powyższej reguły, zgodnie z którym transkrypt jest możliwy w razie ustalenia, że treść rozmowy przypadkowo nagranej rodzi domniemanie osobistego udziału adwokata w przestępstwie. ETPC ocenił w tej sprawie, że wyjątkowo tajemnica zawodowa adwokacka mająca podstawy w poszanowaniu prawa klienta do obrony, nie stanowi przeszkody w dokonaniu transkryptu rozmowy między adwokatem i jego klientem w ramach zgodnej z prawem kontroli linii telefonicznej tego drugiego, jeśli

---

<sup>26</sup> Wyrok ETPC z 25.03.1998 r., w sprawie *Kopp przeciwko Szwajcarii* (skarga nr 23224/94).

<sup>27</sup> Wyrok ETPC z 16.12.1992 r., w sprawie *Niemietz przeciwko Niemcom* (skarga nr 13710/88).

<sup>28</sup> Wyrok ETPC z 12.05.2005 r., w sprawie *Öcalan przeciwko Turcji* (skarga nr 46221/99).

<sup>29</sup> Wyrok ETPC z 16.06.2016 r., w sprawie *Versini-Campinchi i Crasnianski przeciwko Francji* (skarga nr 49176/11).

treść tej rozmowy rodzi domniemanie udziału samego adwokata w przestępstwie i w zakresie, w jakim transkrypt taki nie ma negatywnego wpływu na prawo do obrony klienta.

Należy w tym miejscu zaznaczyć, że status adwokata jako zawodu zaufania publicznego określony jest w art. 17 Konstytucji RP. Utworzenie samorządów zawodowych, które mają sprawować pieczę nad należytym wykonywaniem zawodów prawniczych w granicach interesu publicznego, łączy się z gwarancją tajemnicy adwokackiej. Możliwość powierzenia wrażliwych informacji przez klientów obrońcy wiąże się z obowiązkiem etycznym po stronie adwokata. Z kolei po stronie samorządów zawodowych tworzy obowiązek kontroli w zakresie przestrzegania tej normy etycznej przez wszystkich przedstawicieli zawodu. **Skoro zatem zadaniem samorządów zawodowych jest szczególna ochrona tajemnicy adwokackiej, to ingerencja państwa zmierzająca do uchylecia tej tajemnicy, powinna mieć charakter absolutnie wyjątkowy.** Na szczególne znaczenie między innymi tajemnicy adwokackiej<sup>30</sup> wskazuje brzmienie art. 180 § 2 ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego. Przepis ten stwierdza, że tajemnicę uchylić może jedynie sąd i jedynie wówczas, jeżeli jest to niezbędne dla dobra wymiaru sprawiedliwości, zaś danej okoliczności nie można ustalić na podstawie innego dowodu.

#### IV

Kolejną sprawą, w którą zaangażowany był Rzecznik Praw Obywatelskich, była sprawa w TK o sygn. akt SK 60/21. W tej sprawie Rzecznik wniósł o stwierdzenie, że art. 19 ust. 20 ustawy z dnia 6 kwietnia 1990 r. o Policji 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. Trybunał Konstytucyjny, postanowieniem z dnia 28 czerwca 2022 r., umorzył postępowanie, wskazując m.in., że przyznanie racji skarżącemu „*musiałoby się wiązać z nowelizacją szeregu przepisów i nie ograniczyłoby się jedynie do uzupełnienia katalogu podmiotów uprawnionych do wniesienia zażalenia. Przede wszystkim ustawodawca musiałby określić, w których warunkach ustały zagrożenia dla toczącego się postępowania już po ustaniu kontroli operacyjnej, a dopiero potem uzupełnić katalog podmiotów wskazanych w zaskarżonych przepisach*”. Do ww. postanowienia zostały zgłoszone dwa zdania odrębne.

---

<sup>30</sup> Ponadto także w powołanym przepisie – tajemnicy notarialnej, radcy prawnego, doradcy podatkowego, lekarskiej, dziennikarskiej, statystycznej i tajemnicy Prokuraturii Generalnej.

Do umorzenia postępowania przez TK doszło wyłącznie z przyczyn procesowych. Tego postanowienia nie należy odczytywać jako merytorycznej aprobaty dla obowiązującego stanu prawnego, lecz raczej jako potwierdzenie, że zmiana obecnie obowiązujących regulacji wymagałaby bardziej kompleksowej reformy. Trybunał podkreślił, że „*brak możliwości wniesienia przez osobę poddaną kontroli operacyjnej zażalenia na postanowienie o jej zarządzeniu stanowi zaniechanie prawodawcze*”. Zdaniem Rzecznika Praw Obywatelskich wyeliminowanie tego zaniechania jest obowiązkiem ustawodawcy związanym z koniecznością zapewnienia zgodności przepisów prawa z konstytucyjnymi standardami ochrony prywatności jednostki. W świetle tych standardów **nie może być tak, że osoba, wobec której stosowana była kontrola operacyjna, jest całkowicie pozbawiona prawa do wniesienia zażalenia na postanowienie sądu wyrażające zgodę na zastosowanie tej kontroli.**

Ponadto pragnę zwrócić uwagę na to, że Rzecznik Praw Obywatelskich zgłosił swój udział w postępowaniu w sprawie o sygn. akt SK 58/22 i wniósł o stwierdzenie że art. 459 § 2 kpk w zw. z art. 168b kpk - w zakresie, w jakim przepis ten nie przyznaje podejrzanemu prawa wniesienia zażalenia na postanowienie prokuratora w przedmiocie wykorzystania w postępowaniu karnym dowodu popełnienia przestępstwa, popełnionego przez osobę, wobec której była stosowana kontrola operacyjna innego niż objęte zarządzeniem kontroli operacyjnej, lub popełnionego przez inną osobę niż objęta zarządzeniem kontroli operacyjnej jest niezgodny z art. 45 ust. 1, art. 77 ust. 2 oraz art. 78 w związku z art. 31 ust. 3 i art. 2 Konstytucji RP oraz z art. 32 ust. 1 Konstytucji RP. Problem podniesiony w tym postępowaniu ma związek ze wskazanymi wcześniej zastrzeżeniami co do art. 168b kpk.

## V

Chciałbym także zwrócić uwagę Pana Ministra na raport Parlamentu Europejskiego<sup>31</sup>, w którym wskazano na potwierdzone przez interdyscyplinarne laboratorium *Citizens Lab* przypadki stosowania m.in. w Polsce oprogramowania szpiegowskiego *Pegasus*, stworzonego przez izraelską firmę NSO Group. W świetle wiążących Polskę standardów konstytucyjnych, unijnych i międzynarodowych kontrola operacyjna może polegać wyłącznie na stosowaniu środków, które zostały wskazane w obowiązujących przepisach ustawowych (np. art. 19 ust. 6 ustawy o Policji), a nie dowolnych środków, które umożliwiają pozyskanie danej informacji. Jako że są to przepisy pozwalające na daleko idącą ingerencję w wolność jednostki, powinny być one interpretowane w

---

<sup>31</sup> „*Pegasus and surveillance spyware*”, Policy Department for Citizens’ Rights and Constitutional Affairs Directorate-General for Internal Policies, European Parliament, PE 732.268, 2022 ([https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL\\_IDA\(2022\)732268\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA(2022)732268_EN.pdf), dostęp 23.12.2022).

sposób zwięźający. Po dokonaniu analizy tych przepisów stwierdzam – mając na względzie publicznie dostępne informacje o sposobie działania programów takich jak *Pegasus* – że **w obecnym stanie prawnym nie ma możliwości legalnego użycia tego typu oprogramowań. Nie kwestionując możliwej przydatności stosowania tych systemów dla realizacji zadań służb państwowych, pragnę podkreślić, że aktualnie obowiązujące przepisy prawa nie pozwalają na przełamywanie zabezpieczeń (*hacking*) i przechwytywanie oraz wykorzystywanie treści przekazów komunikacyjnych. W konsekwencji bez zmiany obecnie obowiązujących regulacji stosowania kontroli sądowej oraz operacyjnej, wykorzystywanie tego typu oprogramowania nie powinno mieć miejsca<sup>32</sup>.**

Ponadto należy zaznaczyć, że włamanie się do urządzenia przy użyciu systemu *Pegasus* wiąże się z ingerencją w strukturę danych urządzenia. W połączeniu z możliwością niekontrolowanej ingerencji w funkcjonowanie i pamięć urządzenia, a co za tym idzie możliwość zmiany treści utrwalonych na nim plików oraz wykonywania wszelkiego rodzaju czynności bez zgody i wiedzy użytkownika telefonu, dyskusyjna jest wartość dowodowa danych pozyskanych przy pomocy tego systemu. **Nigdy bowiem nie ma pewności, że zawartość urządzenia nie została zmodyfikowana. Kwestii tej nie da się przy tym w sposób wiarygodny zweryfikować w sądowym postępowaniu dowodowym. Ten aspekt funkcjonowania systemu jest kolejnym argumentem świadczącym o braku dopuszczalności jego stosowania – z uwagi na nieprzydatność na gruncie procesowym<sup>33</sup>.**

Należy dodać, że zastosowanie oprogramowania takiego jak *Pegasus* na konkretnym urządzeniu prowadzi do sytuacji, w której służby *de facto* uzyskują całkowitą nad nim kontrolę, co przy obecnej roli telefonów komórkowych i możliwości technicznych, jakie dają te urządzenia, oznacza praktycznie **przyjęcie pełnej kontroli nad życiem człowieka**. Dotyczy bowiem możliwości dostępu do wszystkich zalogowanych serwisów, dokonywania dyspozycji majątkowych, korespondowania z innymi ludźmi w imieniu użytkownika telefonu, podsłuchiwanie i podglądania w czasie rzeczywistym, w istocie nawet, w ocenie ekspertów, do swoistej kradzieży tożsamości<sup>34</sup>. W konsekwencji stosowanie systemu *Pegasus* w obecnym stanie prawnym nie daje się pogodzić z art. 47, art. 49 i art. 51 ust. 2 Konstytucji RP oraz art. 8 Konwencji, gdyż stanowi zbyt daleko idącą ingerencję w prawa jednostek.

\*

---

<sup>32</sup> M. Bidziński „Ocena legalności i skutków prawnych działań podejmowanych przy użyciu systemu *Pegasus*”, Opinie i ekspertyzy, 0E-426, Kancelaria Senatu, Warszawa, 2022, s. 8.

<sup>33</sup> Ibidem, s. 8.

<sup>34</sup> Ibidem, str. 9.

Mając na względzie przedstawione wyżej zagadnienia, w ocenie Rzecznika Praw Obywatelskich konieczna jest głęboka refleksja nad obowiązującym stanem prawnym w zakresie kompetencji służb do stosowania czynności operacyjno-rozpoznawczych, zasad kontroli działalności służb w tym zakresie, uprawnień osób, wobec których są stosowane czynności operacyjno-rozpoznawcze, a także podjęcie innych działań mających na celu zapewnienie poszanowania praw człowieka.

Łączę wyrazy szacunku,

Marcin Wiącek

Rzecznik Praw Obywatelskich

/-podpisano elektronicznie/

Do wiadomości:

- 1) **Pan Mateusz Morawiecki** – Prezes Rady Ministrów  
e-PUAP Kancelaria Prezesa Rady Ministrów;
- 2) **Pan Marian Banaś** – Prezes Najwyższej Izby Kontroli  
e-PUAP Najwyższa Izba Kontroli;
- 3) **Pan Marcin Bosacki** – Przewodniczący Komisji Nadzwyczajnej do spraw wyjaśnienia przypadków nielegalnej inwigilacji, ich wpływu na proces wyborczy w Rzeczypospolitej Polskiej oraz reformy służb specjalnych  
e-PUAP Kancelaria Senatu RP;
- 4) **Pan Włodzimierz Chróścik**, Prezes Krajowej Rady Radców Prawnych, e-PUAP;
- 5) **Pan Przemysław Rosati**, Prezes Naczelnej Rady Adwokackiej, e-PUAP.