



EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

© Ministerstwo Spraw Wewnętrznych i Administracji, <https://www.gov.pl/mswia>. Permission to republish this translation has been granted by the Polish Ministry of the Interior and Administration for the sole purpose of its inclusion in the Court's database HUDOC.

© Ministerstwo Spraw Wewnętrznych i Administracji, <https://www.gov.pl/mswia>. Zezwolenie na publikację tego tłumaczenia zostało udzielone przez Ministerstwo Spraw Wewnętrznych i Administracji wyłącznie w celu zamieszczenia w bazie Trybunału HUDOC.

SEKCJA PIERWSZA

**SPRAWA PIETRZAK I BYCHAWSKA-SINIARSKA I INNI przeciwko
POLSCE**

(Skargi nr 72038/17 i 25237/18)

WYROK

Art. 8 – Prywatność – Nieadekwatność zabezpieczeń prawnych przed arbitralnością i nadużyciami w odniesieniu do niejawnego nadzoru, przechowywania i dostępu do danych dotyczących komunikacji – Art. 34 – Status skarżących jako ofiar w świetle uzasadnionego badania *in abstracto* zaskarżonych przepisów: niejawni i szeroki zakres środków nadzoru oraz brak skutecznych krajowych środków odwoławczych umożliwiających ich zaskarżenie

Przygotowane przez kancelarię. Nie jest wiążące dla Trybunału.

STRASBURG

28 maja 2024

OSTATECZNY
28/08/2024

Niniejszy wyrok stał się ostateczny w warunkach określonych w artykule 44 ust. 2 Konwencji. Może podlegać drobnym zmianom formalnym.

W sprawie Pietrzak i Bychawska-Siniarska i inni przeciwko Polsce,
Europejski Trybunał Praw Człowieka (sekcja pierwsza), odbywający
posiedzenie w składzie:

Marko Bošnjak,
przewodniczący,
Péter Paczolay,
Krzysztof Wojtyczek,
Erik Wennerström,
Raffaele Sabato,
Lorraine Schembri Orland,
Ioannis Ktistakis,
sędziowie,

oraz Ilse Freiwirth, *sekretarzyni sekcji,*

Po naradzie w Chambre du conseil 11 kwietnia 2024,

Wydaje następujący wyrok, przyjęty w tymże dniu:

WPROWADZENIE

1. Sprawa dotyczy, z punktu widzenia wymogów art. 8 Konwencji, ustawodawstwa krajowego zezwalającego na system niejawnego nadzoru (monitorowanie operacyjne i zatrzymywanie danych telefonicznych, pocztowych i dotyczących łączności elektronicznej [„danych dotyczących komunikacji”] w celu umożliwienia dostępu do nich właściwym organom krajowym). W szczególności dotyczy to kwestii istnienia w prawie krajowym środka prawnego umożliwiającego osobom, które uważają, że zostały poddane niejawnemu nadzorowi, złożenie skargi i zakwestionowanie jej legalności (art. 13 Konwencji o ochronie praw człowieka i podstawowych wolności [„Konwencji”] w związku z jej art. 8).

POSTĘPOWANIE

2. Na początku sprawy mamy do czynienia z dwoma skargami (nos 72038/17 i 25237/18) przeciwko Rzeczypospolitej Polskiej wniesionymi do Trybunału na podstawie art. 34 Konwencji przez pięciu obywateli tego państwa, pana Mikołaja Pietrzaka, pana Wojciecha Klickiego, panią Dominikę Bychawską-Siniarską, panią Barbarę Grabowską-Moroz i panią Katarzynę Szymielewicz („skarżący”) odpowiednio 29 września 2017 oraz 12 lutego 2018.

3. Skarżących reprezentowała adwokat Małgorzata Mączka-Pacholak. Rząd Polski („Rząd”) był reprezentowany przez swojego przedstawiciela, pana Jana Sobczaka z Ministerstwa Spraw Zagranicznych.

4. 27 września 2019 skargi zostały przekazane Rządowi.

5. Upoważnienie do występowania w charakterze interwenienta ubocznego zostało przyznane następującym organizacjom: Europejskiemu Stowarzyszeniu Adwokatów Karnistów („ECBA”), Privacy International, Article 19, Electronic Frontier Foundation, Fair Trials, Stowarzyszeniu ePaństwo, polskiej Naczelnej Radzie Adwokackiej („NRA”), specjalnym sprawozdawcom ONZ ds. promocji i ochrony praw człowieka i podstawowych wolności podczas zwalczania terroryzmu oraz ds. ochrony i promocji wolności słowa, rzecznikowi praw obywatelskich RP oraz

Międzynarodowej Komisji Prawników („MTS”).

6. Zarówno skarżący, jak i Rząd przedstawili pisemne uwagi dotyczące meritum sprawy (artykuł 59 ust. 1). Trybunał otrzymał również uwagi od stron trzecich.

7. 10 maja 2022 izba sekcji pierwszej, do której sprawa została przydzielona, postanowiła przeprowadzić rozprawę. Odbyła się ona publicznie w Palais des droits de l’homme w Strasburgu 27 września 2022.

Stawili się na niej

- ze strony rządu

p. Jan Sobczak, pełnomocnik Rządu,
Marta Bielińska, Ministerstwo Spraw Zagranicznych, doradczyni,
Konrad Malinowski, Kancelaria Prezesa Rady Ministrów, doradca,
Edyta Gołąb, Komenda Główna Policji, doradczyni,
Tomasz Książkiewicz, Centralne Biuro Policji, doradca,
Arkadiusz Matyjasik, Straż Graniczna, doradca;

- ze strony skarżących

Małgorzata Mączka-Pacholak, doradczyni,
Mikołaj Pietrzak,
Dominika Bychawska-Siniarska, Barbara Grabowska-Moroz i
Wojciech Klicki, skarżący;

- ze strony Rzecznika Praw Obywatelskich Rzeczypospolitej Polskiej (RPO), interwenienta ubocznego

Mirosław Wróblewski, Dyrektor, Biuro RPO, Kinga Zielińska,
Główny Ekspert, Biuro RPO;

- ze strony ECBA, interwenienta ubocznego

Andreas Alexios Anagnostakis, specjalista ds. praw człowieka;

- ze strony specjalnego sprawozdawcy ONZ ds. promowania i ochrony praw człowieka i podstawowych wolności podczas walki z terroryzmem, interwenienta ubocznego

Anne Charbord, starsza radczyni prawna, i Karen Lorena Reyes Tolosa, specjalistka ds. praw człowieka.

8. Trybunał wysłuchał oświadczeń pana Sobczaka, pani Mączki-Pacholak, pani Grabowskiej-Moroz i pana Pietrzaka oraz ich odpowiedzi na pytania zadane przez przewodniczącego i sędziów Wennerströma, Wojtyczka, Sabato, Ktistakisa, Schembri Orland, Derenčinović i Bošnjaka. Pani Charbord, pan Wróblewski, pani Zielińska i pan Anagnostakis również złożyli oświadczenia.

FAKTY

I. KONTEKST

9. Odpowiednio 15 stycznia i 10 czerwca 2016 polski parlament przyjął Ustawę o zmianie ustawy o Policji oraz niektórych innych ustaw („ustawa z 15 stycznia 2016”) oraz Ustawę o działaniach antyterrorystycznych (ustępy

51–57 poniżej).

10. Przepisy te zostały skrytykowane w szczególności przez polskiego Rzecznika Praw Obywatelskich („RPO”), Generalnego Inspektora Ochrony Danych Osobowych, Krajową Radę Sądownictwa, Krajową Radę Adwokatur i Stowarzyszeń Prawniczych oraz posłów opozycji. Szereg organizacji społeczeństwa obywatelskiego posiadających doświadczenie w tej dziedzinie uznało, że nowe przepisy, pod pozorem wykonania wyroku Trybunału Konstytucyjnego K 23/11 (ust. 73 poniżej), wzmocniły uprawnienia nadzorcze władz w wielu obszarach i były niezgodne z niektórymi międzynarodowymi zobowiązaniami Polski w zakresie praw człowieka. W swojej opinii CDL-AD (2016) 012 z 13 czerwca 2016 (ust. 92 poniżej) Komisja Wenecka wyraziła zastrzeżenia do ustawy z 15 stycznia 2016.

II. OKOLICZNOŚCI SPRAWY

11. Skarżący urodzili się odpowiednio w latach 1973, 1982, 1987, 1981 i 1986 i mieszkają w Warszawie. Skarżący Mikołaj Pietrzak jest adwokatem i byłym prezesem Okręgowej Rady Adwokackiej w Warszawie. Pozostali skarżący są pracownikami organizacji pozarządowych z siedzibą w Warszawie; skarżąca Barbara Grabowska-Moroz jest wykładowczynią akademicką i ekspertką zewnętrzną Helsińskiej Fundacji Praw Człowieka, a skarżąca Dominika Bychawska-Siniarska jest członkinią tej samej fundacji. Skarżący Wojciech Klicki i skarżąca Katarzyna Szymielewicz są członkami Fundacji Panoptykon.

A. Wnioski o dostęp do informacji publicznej składane przez skarżącego Klickiego i skarżącą Szymielewicz

12. 14 marca 2016, powołując się na przepisy art. 2 ustawy o dostępie do informacji publicznej (ust. 59 poniżej), skarżący Klicki i skarżąca Szymielewicz zwrócili się do szefa Agencji Bezpieczeństwa Wewnętrznego (ABW) o poinformowanie ich, czy, w okresie od 1 stycznia 2012 do 29 lutego 2016 byli inwigilowani w sposób niejawnny przez podległe mu służby oraz czy służby te gromadziły bez ich wiedzy dane dotyczące komunikacji.

13. 31 marca 2016 szef ABW odrzucił wnioski złożone przez oboje skarżących. Odnosząc się do przepisów Ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, które jego zdaniem miały znaczenie w niniejszej sprawie, stwierdził, że chociaż informacje, których ujawnienia domagali się zainteresowani, zostały uznane za „publiczne” w rozumieniu art. 1 Ustawy o dostępie do informacji publicznej, to nie mogły zostać im udostępnione z przyczyn określonych w ustawie z 5 sierpnia 2010 o ochronie danych niejawnnych, pkt. 60 poniżej. Wskazał również, że stosowane przez ABW środki kontroli operacyjnej miały charakter niejawnny, a ich stosowanie przez funkcjonariuszy odpowiednich służb nie wymagało zgody zainteresowanych osób i odbywało się bez ich wiedzy. Dodał również, że rejestry, w których zapisywano informacje uzyskane w ramach wyżej wymienionych środków, są poufne i że podana do wiadomości publicznej może zostać jedynie liczba osób, które podlegały nadzorowi w okresie referencyjnym, zgodnie ze sprawozdaniem przedkładanym corocznie Sejmowi i Senatowi przez prokuratora generalnego. Wyjaśnił, że zgodnie

z art. 39 ustawy o ABW tylko właściwe sądy i prokuratorzy mogli mieć dostęp, pod pewnymi warunkami i za jego zgodą, jako szefa ABW, do informacji wynikających ze środków nadzoru, a ponadto dokumenty dotyczące kontroli operacyjnej były przysyłane premierowi w sposób zgodny z przepisami dotyczącymi ochrony danych niejawnych. Dodał, że informacje, o które zwrócili się skarżący, zostały przetworzone zgodnie z wymogami art. 3 ust. 1 ustawy o dostępie do informacji publicznej, a zatem mogły zostać ujawnione zainteresowanym stronom tylko wtedy, gdy przemawiał za tym ważny interes publiczny.

14. 31 marca 2016 szef ABW odrzucił podobny wniosek skierowany do niego przez skarżącego Szymielewicz.

15. 6 maja 2016 szef ABW odrzucił wniosek skarżącego Klickiego o ponowne rozpatrzenie jego sprawy. Uznał, że zasady określone w odpowiednim orzecznictwie sądów administracyjnych nie pozwalają mu zgodzić się z argumentami zainteresowanego, który twierdził, że przyznano mu rozszerzone prawo dostępu do informacji, o które wnioskował. Na marginesie swojej decyzji wskazał, że może ona zostać zaskarżona do sądu administracyjnego.

B. Skargi złożone przez skarżących na podstawie z art. 227 kodeksu postępowanie administracyjnego (KPA)

16. Między czerwcem a lipcem 2017 każdy ze skarżących złożył skargę na podstawie art. 227 KPA (ust. 67 poniżej) do prezesa Rady Ministrów i odpowiednich szefów różnych służb policyjnych i wywiadowczych, w tym ABW, Centralnego Biura Antykorupcyjnego (CBA), Krajowej Administracji Skarbowej (KAS), Służby Kontrwywiadu Wojskowego (SKW), Policji, Straży Granicznej (SG) i Żandarmerii Wojskowej (ŻW) dotyczącą niektórych przepisów krajowych odnośnie do traktujących o niejawnym nadzorze. W skargach tych skarżący krytykowali zaskarżone przepisy w szczególności za to, że ich zdaniem umożliwiały one przedstawicielom wspomnianych służb monitorowanie ich połączeń telekomunikacyjnych i gromadzenie, bez ich wiedzy, informacji ich dotyczących, o których mowa w art. 180 lit. c) i d) ustawy z 16 lipca 2004 – Prawo telekomunikacyjne (pkt. 61 poniżej) oraz w art. 18 ust. 1–5 ustawy z 18 lipca 2002 o świadczeniu usług drogą elektroniczną (pkt. 63 poniżej). Uznali oni, że biorąc pod uwagę ich działalność zawodową i publiczną, jest wysoce prawdopodobne, że taki nadzór został wobec nich przeprowadzony. Dodali, że funkcjonariusze przedmiotowych służb nie byli zobowiązani do informowania ich o jakimkolwiek zastosowaniu wobec nich takiego środka, nawet po jego zaprzestaniu, i argumentowali, że taki brak udzielenia informacji był sprzeczny z art. 51 ust. 3 i 4 Konstytucji (zob. pkt 26 poniżej) i uniemożliwił im kontrolę legalności nadzoru przez sąd. Zainteresowane strony twierdziły, że niepowiadomienie zainteresowanych osób o środkach niejawnego nadzoru, w połączeniu z brakiem skutecznego monitorowania tych środków i niedociągnięciami w odpowiednich przepisach krajowych, było sprzeczne z zasadą rządów prawa w demokracji i naruszało ich uzasadnione interesy.

17. Między czerwcem a wrześniem 2017 szefowie wyżej wymienionych służb policyjnych i wywiadowczych odpowiedzieli na skargi skarżących.

18. Szef ABW wskazał zainteresowanemu, że informacje dotyczące

niejawnego nadzoru osób fizycznych są poufne i chronione odpowiednimi przepisami ustawy o ABW oraz służbach wywiadowczych i ustawy o ochronie danych niejawnych. Stwierdził, że ABW jako instytucja działająca zgodnie z prawem, nie może udzielić skarżącym żadnych informacji na ten temat ani odpowiedzieć na ich pytanie, czy stosowane są wobec nich środki nadzoru. Dodał, że wdrażanie niejawnych środków nadzoru przez agentów pod jego nadzorem było monitorowane przez prokuraturę i właściwe sądy.

19. Szef CBA wyjaśnił natomiast skarżącym, że zgodnie z odpowiednimi przepisami Konstytucji i Ustawy o Centralnym Biurze Antykorupcyjnym czynności operacyjno-rozpoznawcze były prowadzone przez funkcjonariuszy pod jego nadzorem, a osoba, która była przedmiotem tych czynności, nie była o nich informowana, chyba że informacje uzyskane za pomocą tych czynności zostały następnie wykorzystane jako dowód w postępowaniu karnym przeciwko niej. Wskazał, że nawet zakładając, że skarżący byli celem tego rodzaju środków, decyzja o ich zastosowaniu musiałaby zostać podjęta zgodnie z procedurami przewidzianymi w tym celu w odpowiednich przepisach. Przypomniął, że wszelkie monitorowanie komunikacji pierwszego skarżącego podlegałoby również wzmocnionemu systemowi ochrony przewidzianemu w art. 18 ustawy o CBA w odniesieniu do tajemnicy adwokackiej. Dodał, że w ustawodawstwie krajowym nie ma zapisów, które uniemożliwiłoby funkcjonariuszom CBA stosowanie środków nadzoru wobec adwokatów.

20. Komendant Główny ŻW poinformował z kolei skarżących, że podlegli mu funkcjonariusze mogą teoretycznie wszcząć wobec nich czynności operacyjno-rozpoznawcze, jeżeli spełnione zostały warunki określone w tym celu w odpowiednich przepisach. Zauważył, że twierdzenia skarżących co do rzekomego istnienia takich środków ich dotyczących nie zostały udowodnione, a sama ich wiarygodność nie została ustalona. Dodał, że zgodnie z przedmiotowymi przepisami, których konstytucyjność, jego zdaniem, nigdy nie została jeszcze zakwestionowana, Żandarmeria Wojskowa nie miała uprawnień do powiadamiania zainteresowanych osób o niejawnych środkach nadzoru, nawet po ich zniesieniu. Podkreślił również, że gromadzenie przez agentów pod jego nadzorem danych dotyczących komunikacji telefonicznej, komunikacji pocztowej i komunikacji cyfrowej osób objętych nadzorem podlegało kontroli właściwego wojskowego sądu okręgowego.

21. Jeśli chodzi o Komendanta Głównego SG, poinformował on skarżących, że odpowiednie przepisy krajowe zasadniczo nie nakładają na jego służby obowiązku informowania zainteresowanych osób o zastosowanych wobec nich środkach w zakresie rozpoznawania, przeszukiwania i gromadzenia danych związanych z łącznością telekomunikacyjną, cyfrową i pocztową, z wyjątkiem przypadku, o którym mowa w art. 10 c ust. 9 ustawy o Straży Granicznej z 12 października 1990. Dodał, że osoba objęta niejawnym nadzorem była o nim powiadamiana tylko wtedy, gdy uzyskane informacje były wykorzystywane w postępowaniu karnym, w którym była ona stroną. Określił również, że niejawne środki nadzoru były prowadzone przez agentów pod jego nadzorem wyłącznie w celu zapobiegania przestępstwom, o których mowa w art. 9 e ust. 1 akapit 1–9 e ustawy o SG, wykrywania sprawców tych przestępstw i gromadzenia danych, o których mowa w art. 10 b ust. 1 tej samej ustawy. Wskazał również, że realizacja tego nadzoru przez agentów SG była monitorowana przez prokuraturę i odpowiednie sądy.

22. Szef SKW ze swej strony poinformował skarżących, że stosowanie środków gromadzenia danych wskazanych w art. 32 ust. 1 ustawy Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego z 9 czerwca 2006 nie może być kwestionowane na podstawie art. 227 KPA, ale mimo to podlegała kontroli Sądu Okręgowego w Warszawie na podstawie odpowiednich przepisów art. 32a tej samej ustawy.

23. Służby komendy głównej Policji potwierdziły, że funkcjonariusze Policji mogą prowadzić niejawne środki nadzoru w przypadkach wyraźnie objętych ustawą o Policji i zgodnie z jej wymogami. Zauważając, że w swoich skargach zainteresowane osoby pytały Komendanta Głównego Policji o to, czy funkcjonariusze Policji prowadzili wobec nich niejawną nadzór, uznali, że nie są w stanie odpowiedzieć na to pytanie ze względu na hipotetyczny i ich zdaniem niewystarczająco precyzyjny charakter pytania.

24. Szef KAS poinformował skarżących z kolei, że czynności operacyjno-rozpoznawcze miały charakter niejawną, a osoby im poddane nie mogły składać zażaleń na ich zastosowanie, z wyjątkiem sytuacji określonych w art. 117 ust. 3 ustawy o Krajowej Administracji Skarbowej z 16 listopada 2016 oraz że w związku z tym funkcjonariusze KAS gromadzili i przetwarzali informacje wynikające z przedmiotowych czynności bez powiadamiania osoby zainteresowanej i bez uzyskiwania jej zgody. Wskazał on, że z odpowiednich przepisów wspomnianej ustawy wynika, że stosowanie środków operacyjno-rozpoznawczych wobec danej osoby nie zależy w żaden sposób od jej działalności zawodowej lub publicznej. Wskazał, że prawo określone w art. 51 ust. 3 Konstytucji (zob. pkt 26 poniżej) może podlegać ograniczeniom określonym w ustawie, takim jak, w niniejszej sprawie, ustawa o KAS. Dodał, że odpowiednie przepisy wystarczająco określają okoliczności, w których nadzór może być podejmowany przez podlegających mu funkcjonariuszy.

25. Wreszcie, odpowiednie działy Kancelarii Prezesa Rady Ministrów poinformowały skarżących, że według ich przełożonego, szefowie różnych służb policyjnych i wywiadowczych wyczerpująco odpowiedzieli na ich pytania dotyczące hipotetycznego nadzoru. Stwierdzili oni, że wykonując swoje zadania, specjalne służby państwowe stosowały niejawną nadzór przewidziane w odpowiednich przepisach, a środki i metody, których używały w tym celu, były poufne i chronione na mocy przepisów regulujących dane służby oraz ustawy o ochronie danych poufnych.

WŁAŚCIWE RAMY PRAWNE I PRAKTYKA

I. WŁAŚCIWE KRAJOWE RAMY PRAWNE I PRAKTYKA

A. Konstytucja

26. Właściwe zapisy Konstytucji Rzeczypospolitej Polskiej brzmią następująco:

Artykuł 31

„(...)

3. Ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są

konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw”.

Artykuł 47

„Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym”.

Artykuł 51

„1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.

2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.

3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.

4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.

5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa”.

Artykuł 61

„1. Obywatel ma prawo do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne. Prawo to obejmuje również uzyskiwanie informacji o działalności organów samorządu gospodarczego i zawodowego a także innych osób oraz jednostek organizacyjnych w zakresie, w jakim wykonują one zadania władzy publicznej i gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa.

2. Prawo do uzyskiwania informacji obejmuje dostęp do dokumentów oraz wstęp na posiedzenia kolegialnych organów władzy publicznej pochodzących z powszechnych wyborów, z możliwością rejestracji dźwięku lub obrazu.

3. Ograniczenie prawa, o którym mowa w ust. 1 i 2, może nastąpić wyłącznie ze względu na określone w ustawach ochronę wolności i praw innych osób i podmiotów gospodarczych oraz ochronę porządku publicznego, bezpieczeństwa lub ważnego interesu gospodarczego państwa.

4. Tryb udzielania informacji, o których mowa w ust. 1 i 2, określają ustawy, a w odniesieniu do Sejmu i Senatu ich regulaminy”.

Artykuł 79

„1. Każdy, czyje konstytucyjne wolności lub prawa zostały naruszone, ma prawo, na zasadach określonych w ustawie, wnieść skargę do Trybunału Konstytucyjnego w sprawie zgodności z Konstytucją ustawy lub innego aktu normatywnego, na podstawie którego sąd lub organ administracji publicznej orzekł ostatecznie o jego wolnościach lub prawach albo o jego obowiązkach określonych w Konstytucji”.

B. Krajowe ramy prawne odnoszące się do niejawnego nadzoru obowiązuje w okresie objętym postępowaniem

27. ¹Polskie ramy prawne dotyczące niejawnego nadzoru obejmują szereg ustaw, w tym ustawy regulujące odpowiednie działania różnych służb policyjnych i wywiadowczych.

Wszystkie odpowiednie przepisy przewidują praktycznie identyczny model nadzoru, przy czym ustawa o Policji służy jako przykład *mutatis mutandis* dla innych organów.

28. Artykuł 19 ustawy o Policji zawiera przepisy dotyczące kontroli operacyjnej (określane w anglojęzycznej tradycji terminem „operational control”, zob. ust. 31–44 poniżej), a artykuł 20c ustawy o Policji dotyczy danych dotyczących komunikacji (zob. ust. 45–50 poniżej). Kontrola operacyjna często poprzedza i uzasadnia wszczęcie postępowania przygotowawczego, ale nie zawsze prowadzi do wszczęcia postępowania karnego (kontrola pozaprocesowa). Informacje uzyskane w ten sposób mogą być następnie przedstawione jako dowód w postępowaniu karnym. Środki nadzoru wszczęte w toku postępowania karnego (kontrola procesowa) są regulowane odpowiednimi przepisami Kodeksu postępowania karnego (KPK) (ust. 58 poniżej).

29. Ogólnie rzecz biorąc, nadzór niejawny jest prowadzony w celu powstrzymania przestępczości, a wywiad jest prowadzony dla celów bezpieczeństwa narodowego. Cele, do których mogą być wykorzystywane środki nadzoru podejmowane przez różne służby policyjne i wywiadowcze, są określone w przepisach regulujących ich zadania.

30. Jeśli chodzi o nadzór niejawny, ustawodawstwo krajowe przewiduje dwa odrębne systemy prawne: jeden dotyczy kontroli operacyjnej, a drugi reguluje zatrzymywanie i przetwarzanie danych dotyczących komunikacji. Te dwa rodzaje nadzoru różnią się pod względem podstaw, na jakich są zarządzane oraz zasad proceduralnych, które mają do nich zastosowanie.

1. Kontrola operacyjna

31. Zgodnie z ust. 6 art. 19 ustawy o Policji, środki takie jak podsłuch, utrwalanie treści rozmów telefonicznych lub korespondencji prowadzonej za pośrednictwem sieci telekomunikacyjnych i sieci łączności cyfrowej (poczta elektroniczna, komunikatory itp.) oraz m.in. nagrania dźwiękowe, wykonywanie zdjęć prywatnych miejsc i środków transportu, utrwalanie

¹ Ustawa z 6 kwietnia 1990 o Policji, ustawa z 24 maja 2002 o ABW oraz Służbie Wywiadu, ustawa z 9 czerwca 2006 o CBA, ustawa z 9 czerwca 2006 o SKW oraz Służbie Wywiadu Wojskowego, ustawa z 16 listopada 2016 o KAS, ustawa z 12 października 1990 o SG, ustawa z 24 sierpnia 2001 o Żandarmerii Wojskowej i wojskowych organach porządkowych.

danych na informatycznych nośnikach danych, urządzeniach telekomunikacyjnych lub w systemach informatycznych i teleinformatycznych oraz monitorowanie przesyłek pocztowych wchodzi w zakres kontroli operacyjnej. Ten rodzaj nadzoru umożliwia Policji ustalenie treści komunikacji między osobami, które myślą, że komunikują się w sposób poufny.

32. Art. 19 ust. 1 ustawy o Policji zawiera wyczerpującą listę przestępstw, które mogą stanowić podstawę do zastosowania środków kontroli operacyjnej. Przepis ten stanowi również, że kontrola operacyjna może być zarządzona, gdy Policja stosuje czynności operacyjno-rozpoznawcze w celu zapobieżenia lub wykrycia danych przestępstw, wykrycia sprawców tych przestępstw oraz zebrania i utrwalenia dowodów, gdy inne środki wydają się nieskuteczne lub zbędne.

33. Zgodnie z art. 19 ust. 1, 1a, 2 i 7 tej samej ustawy kontrola operacyjna może zostać zarządzona przez właściwy sąd, który orzeka wówczas na pisemny wniosek złożony przez upoważnionego do tego funkcjonariusza danej służby policyjno-wywiadowczej (tj. komendanta głównego Policji krajowej lub komendanta wojewódzkiego Policji) i uprzednio zatwierdzony przez właściwego prokuratora (tj. prokuratora generalnego prokuratury krajowej lub prokuratora regionalnego). Wniosek o ustanowienie kontroli operacyjnej musi być uzasadniony. Musi on wskazywać w szczególności numer akt lub ich kryptonim, elementy stanu faktycznego odnoszące się do przestępstwa oraz, jeśli to możliwe, ich kwalifikację prawną, okoliczności uzasadniające zastosowanie kontroli operacyjnej, w tym te wskazujące, że inne środki byłyby nieskuteczne lub nieodpowiednie, elementy pozwalające na jednoznaczną identyfikację przedmiotu kontroli operacyjnej, jak również miejsce, w którym będzie ona prowadzona oraz środki, za pomocą których zostanie przeprowadzona, a także cel, czas stosowania i rodzaj danej kontroli operacyjnej.

34. Zgodnie z art. 19 ust. 8 wyżej wymienionej ustawy nadzór jest dozwolony przez okres nieprzekraczający trzech miesięcy. Przedłużenie tego okresu na kolejny okres do trzech miesięcy może zostać zarządzane decyzją sądu na wniosek odpowiedniej służby i za pisemną zgodą prokuratora, jeśli pierwotne powody nadzoru są nadal aktualne. W należycie uzasadnionych przypadkach (jeśli pojawienie się nowych faktów wymaga podjęcia działań w celu zapobiegania lub wykrywania działalności przestępczej lub śledzenia osób zaangażowanych w taką działalność i gromadzenia dowodów), nadzór może zostać przedłużony przez sąd wyższej instancji na kilka kolejnych okresów ustalonych przez ten sąd, na maksymalny łączny okres dwunastu miesięcy. Całkowity okres nadzoru nie może przekroczyć osiemnastu miesięcy. Sąd orzekający w przedmiocie wniosku o rozszerzenie kontroli operacyjnej bierze pod uwagę dowody przedstawione na poparcie wniosku, w tym dowody zgromadzone już w toku kontroli operacyjnej.

35. Artykuł 19 ust. 3 tej samej ustawy stanowi, że wyjątkowo, w wyjątkowo pilnych przypadkach, a w szczególności, gdy istnieje ryzyko utraty informacji lub manipulacji dowodami, Policja może prowadzić niejawną nadzór bez zezwolenia, który to nadzór musi zostać przerwany, jeśli zezwolenie sądowe nie zostanie uzyskane w ciągu pięciu dni od rozpoczęcia stosowania tego środka. W tym drugim przypadku informacje zebrane w tym okresie muszą zostać zniszczone przez komisję protokołową.

36. Zgodnie z art. 19 ust. 11 ww. ustawy, sąd rozpoznający wniosek o

zastosowanie kontroli operacyjnej jest sądem jednoosobowym. Ten ostatni przeprowadza poszczególne czynności procesowe na zasadach analogicznych do tych, które zostały określone dla przekazywania, przechowywania i udostępniania informacji niejawnych oraz z uwzględnieniem, w odpowiednim zakresie, przepisów wydanych na podstawie art. 181 ust. 2 Kodeksu postępowania karnego (KPK). W posiedzeniu sądu, które odbywa się przy drzwiach zamkniętych, biorą udział wyłącznie prokurator i przedstawiciel organu wnioskującego.

37. Art. 19 ust. 12 tej samej ustawy nakłada na przedsiębiorców telekomunikacyjnych, operatorów pocztowych i dostawców usług świadczonych drogą elektroniczną obowiązek zapewnienia na własny koszt warunków technicznych i organizacyjnych umożliwiających Policji stosowanie kontroli operacyjnej.

38. Art. 19 ust. 13 i 14 tej ustawy stanowi, że kontrola operacyjna musi zostać zakończona niezwłocznie po ustaniu przyczyn, które uzasadniały jej ustanowienie, a najpóźniej z upływem okresu, na jaki została zatwierdzona. Po zniesieniu monitoringu operacyjnego organ Policji, o którym mowa w art. 19 ust. 1, informuje właściwego prokuratora o dokonanych ustaleniach oraz na żądanie prokuratora, o sposobie przeprowadzenia nadzoru.

39. Zgodnie z art. 19 ust. 15 wspomnianej ustawy, w przypadku, gdy organy zgromadziły dowody pozwalające na wszczęcie postępowania karnego lub mające znaczenie dla toczącego się postępowania karnego, właściwy organ (tj. Komendant Główny Policji, Komendant Centralnego Biura Śledczego lub komendant regionalnego oddziału Policji) przekazuje prokuratorowi, o którym mowa w ust. 1 tego artykułu, wszystkie dowody uzyskane w toku czynności operacyjno-rozpoznawczych. Przepisy art. 393 ust. 1 ust. 1 KPK (pkt 58 poniżej) stosuje się *mutatis mutandis* do postępowania przed sądem w odniesieniu do tych kwestii.

40. Artykuł 19 ust. 15 tej samej ustawy określa procedurę postępowania w przypadku informacji objętych tajemnicą zawodową. Właściwi funkcjonariusze Policji muszą zniszczyć informacje objęte ochroną bezwzględnej tajemnicy zawodowej przysługującej adwokatom i duchownym (art. 19 ust. 15 lit. f pkt 1 ustawy o Policji w związku z art. 178 KPK) oraz przekazać prokuratorowi, a następnie sądowi, zebrane informacje objęte mniejszą ochroną tajemnicy zawodowej, tak jak ma to miejsce w przypadku tajemnicy zawodowej notariusza, adwokata i radcy prawnego (o ile nie występuje w charakterze obrońcy), doradcy podatkowego, lekarza, rzecznika praw i dziennikarza (art. 19 ust. 15 lit. f akapit 2 i 15 g ustawy w zw. z art. 178 a i 180 ust. 2 i 3 KPK). Sąd orzeka niezwłocznie i może albo zezwolić na wykorzystanie informacji w postępowaniu karnym, jeżeli uzna, że wymaga tego interes prawidłowego administrowania wymiarem sprawiedliwości i że istotna okoliczność nie może zostać ustalona za pomocą innych dowodów, albo jeżeli tego nie uczyni, nakazać ich zniszczenie. Postanowienie sądu nakazujące zniszczenie informacji uzyskanych za pomocą monitoringu operacyjnego może zostać zaskarżone w drodze zażalenia przysługującego wyłącznie prokuratorowi. Dany organ Policji musi zastosować się do nakazu zniszczenia wydanego przez sąd w odniesieniu do elementów, o których mowa w ust. 15 lit. h), i musi niezwłocznie zarządzić ich zniszczenie przez komisję protokolarną. Niezwłocznie poinformuje również prokuratora, o którym mowa w art. 19 ust. 15 lit. g), o zniszczeniu przedmiotowych przedmiotów.

41. Art. 19 ust. 16 przedmiotowej ustawy stanowi, że osoba objęta kontrolą

operacyjną nie może mieć dostępu do informacji zgromadzonych podczas tej kontroli.

42. ²Zgodnie z art. 19 ust. 17 tej ustawy elementy uzyskane w wyniku kontroli operacyjnej, które nie doprowadziły do wszczęcia postępowania karnego, podlegają niezwłocznemu zniszczeniu przez komisję protokolarną. Takie usunięcie jest przeprowadzane na mocy decyzji organu Policji, który wystąpił o zezwolenie na wdrożenie danego środka.

43. Właściwy prokurator krajowy, sąd, prokurator i organ Policji odnotowują wnioski i decyzje dotyczące kontroli operacyjnej w specjalnych rejestrach. Centralny rejestr jest również prowadzony przez komendanta głównego Policji. Rejestry, o których mowa, są tworzone w formie elektronicznej, z zastrzeżeniem odmiennych przepisów dotyczących ochrony informacji niejawnych.

44. Art. 19 ust. 22 wspomnianej ustawy stanowi, że minister spraw wewnętrznych przedkłada Sejmowi i Senatowi roczne sprawozdania dotyczące działalności Policji regulowanej w art. 19 ust. 1–21, które to sprawozdania zawierają dane i informacje, o których mowa w art. 20 ust. 3 wspomnianej ustawy. Są one przedkładane Sejmowi i Senatowi do 30 czerwca każdego kolejnego roku.

2. Zatrzymywanie (retencja) danych dotyczących komunikacji

45. System prawny dotyczący zatrzymywania (retencji) danych dotyczących komunikacji jest wynikiem przeniesienia do prawa krajowego dyrektywy w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem publicznych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniającej dyrektywę 2002/58/WE, przyjętej 15 marca 2006 („dyrektywa w sprawie zatrzymywania danych”, pkt 97 poniżej), które to przeniesienie odbyło się za pomocą ustawy z 24 kwietnia 2009 o zmianie prawa telekomunikacyjnego oraz innych ustaw.

46. Artykuł 20 c ustawy o Policji reguluje ten rodzaj nadzoru. Zgodnie z tym przepisem Policja może zatrzymywać dane dotyczące komunikacji w celu zapobiegania lub wykrywania działalności przestępczej, ratowania życia lub ochrony zdrowia, lub prowadzenia akcji poszukiwawczych i ratowniczych. Dostęp do danych nie ujawnia treści prywatnych komunikatów. Termin „dane dotyczące komunikacji” obejmuje dane związane z telekomunikacją w rozumieniu art. 180 lit. c) i d) prawa telekomunikacyjnego (pkt 61 poniżej), dane pocztowe w rozumieniu art. 82 ust. 1 pkt 1 prawa pocztowego (pkt 62 poniżej), a także dane cyfrowe w rozumieniu art. 18 ust. 1–5 ustawy o świadczeniu usług drogą elektroniczną (pkt 63 poniżej). Obejmuje to również takie informacje, jak wykonane lub odebrane połączenia telefoniczne, wybierane numery, czas trwania połączenia, położenie geograficzne urządzeń mobilnych w danym momencie, odwiedzane strony internetowe, połączenia z witrynami, ustawienia osobiste i adresy e-mail. Dane zebrane w ten sposób są przetwarzane bez wiedzy lub zgody osoby, której dotyczą. Dostawcy usług technologii informacyjno-komunikacyjnych

² Zgodnie z art. 15f i 16 ustawy o ABW oraz Służbach Wywiadowczych, ABW może zatrzymać informacje zebrane w ramach kontroli operacyjnej, które mają znaczenie dla bezpieczeństwa państwa. Ponadto art. 123 ustawy o KAS stanowi, że KAS może zatrzymać informacje uzyskane w wyniku kontroli operacyjnej, które mają znaczenie dla postępowania w sprawie naruszenia przepisów prawa podatkowego.

(„usługi ICT”) są zobowiązani do zapewnienia właściwym funkcjonariuszom Policji swobodnego dostępu do przedmiotowych danych (art. 20 c ust. 2 wspomnianej ustawy). Każda z pozostałych służb państwowych może gromadzić dane dotyczące komunikacji, o ile jest to konieczne do osiągnięcia ustawowych celów danej służby.

47. Art. 20 c ust. 3 ustawy o Policji zezwala Policji na zawieranie poufnych umów z dostawcami usług teleinformatycznych, dając jej bezpośredni dostęp do danych dotyczących komunikacji bez udziału personelu dostawcy usług. Właściwi funkcjonariusze Policji prowadzą poufne rejestry elektroniczne, w których rejestrowane są wnioski o dostęp do danych. Środki techniczne, za pomocą których Policja wdraża środki zatrzymywania danych dotyczących komunikacji, również są poufne.

48. Dane, o których mowa w art. 20 c ust. 1 ww. ustawy, przydatne w związku z prowadzonym postępowaniem karnym, właściwi funkcjonariusze Policji przekazują właściwemu prokuratorowi, który decyduje o ich wykorzystaniu. Dane, które nie są już przydatne w postępowaniu karnym, są niezwłocznie niszczone przez komitet protokolarny³.

49. Artykuł 20 ca tej samej ustawy reguluje kontrolę pozyskiwania danych dotyczących komunikacji przez Policję. Przepis ten nakłada na Policję obowiązek przedkładania właściwemu sądowi okręgowemu półrocznego sprawozdania zawierającego ogólne informacje na temat liczby przypadków dostępu do danych wymienionych w wykazie w danym okresie, wraz ze wskazaniem rodzaju danych, których to dotyczyło, oraz kwalifikacji prawnych, których dotyczyły wnioski o dostęp do danych, a także informacji na temat uzyskania danych w celu ochrony życia i zdrowia ludzkiego lub wsparcia misji poszukiwawczych lub ratowniczych. W celu bardziej dogłębnego zbadania niektórych z tych spraw, właściwy sąd może wziąć pod uwagę treść elementów, które uzasadniały zastosowanie wspomnianego środka przez Policję. Sąd poinformuje Policję o swoich ustaleniach w ciągu trzydziestu dni od zakończenia kontroli.

50. Artykuł 20 cb ustawy dotyczy przetwarzania danych związanych z subskrypcjami (abonamentami). Zgodnie z art. 20 ca 5, pozyskiwanie i przetwarzanie tych danych jest wyłączone z kontroli a posteriori przewidzianej w tym przepisie.

3. Ustawa o działaniach antyterrorystycznych

51. Ustawa o działaniach antyterrorystycznych reguluje metody stosowane w walce z terroryzmem i współpracę między właściwymi organami w tej dziedzinie.

52. Artykuł 2 tej ustawy definiuje kluczowe pojęcia dla celów stosowania ustawy. Zgodnie z tym przepisem, pojęcie „działań antyterrorystycznych” obejmuje wszelkie środki, które władze mogą wdrożyć w celu zapobiegania „zdarzeniom o charakterze terrorystycznym”, przygotowania do przejęcia kontroli nad takimi zdarzeniami, reagowania na ich wystąpienie i ułatwiania usuwania ich skutków, w tym poprzez wykorzystanie zasobów przeznaczonych do ich zwalczania. „Działania kontr terrorystyczne”, w rozumieniu tejże ustawy, to działania podejmowane wobec sprawców

³ ABW i Służby Wywiadu Wojskowego mogą również zatrzymywać dane dotyczące komunikacji istotne odpowiednio dla bezpieczeństwa i obronności państwa (art. 28 ustawy o ABW oraz Służbach Wywiadu Wojskowego oraz art. 32 ustawy o SKW oraz Służbach Wywiadu Wojskowego).

przestępstw o charakterze terrorystycznym, o których mowa w art. 115 ust. 2 Kodeksu karnego (KK), oraz ich współsprawców, przy użyciu specjalnych środków, metod i planów działania w przypadku bezpośredniego zagrożenia dla życia, zdrowia, wolności osobistej oraz mienia. Pojęcie „zdarzeń o charakterze terrorystycznym” obejmuje wszystkie sytuacje, które mogą być spowodowane popełnieniem przestępstwa o charakterze terrorystycznym w rozumieniu art. 115 ust. 2 KK lub ujawniające istnienie ryzyka popełnienia takiego przestępstwa.

53. Środki nadzoru mogą być stosowane wobec cudzoziemców podejrzanych o działalność terrorystyczną.

54. Art. 9 ust. 1 tej ustawy wymienia środki, które funkcjonariusze ABW mogą stosować niejawnie, przez okres nieprzekraczający trzech miesięcy, wobec cudzoziemców, o których mowa. Obejmuje ono w szczególności rejestrowanie treści rozmów telefonicznych i korespondencji prowadzonej za pośrednictwem sieci telekomunikacyjnych i sieci łączności cyfrowej, nagrania dźwiękowe, wykonywanie zdjęć prywatnych miejsc i środków transportu, rejestrowanie danych na nośnikach informatycznych, urządzeniach telekomunikacyjnych lub systemach komputerowych i telekomunikacyjnych oraz monitorowanie przesyłek pocztowych. Decyzję o zastosowaniu tych środków podejmuje i uzasadnia szef ABW. Ten ostatni niezwłocznie informuje ministra odpowiedzialnego za nadzór nad państwowymi służbami specjalnymi oraz prokuratora generalnego Prokuratury Krajowej. Prokurator generalny może nakazać zakończenie stosowania podjętych środków nadzoru.

55. Zgodnie z art. 9 ust. 5 tej samej ustawy, wprowadzone środki niejawnego nadzoru mogą zostać przedłużone na warunkach określonych w art. 27 ustawy o ABW oraz służbach wywiadowczych⁴.

56. Szef ABW niezwłocznie informuje prokuratora generalnego Prokuratury Krajowej o wnioskach wynikających z zastosowania środków niejawnego nadzoru oraz na jego żądanie, o sposobie zastosowania tych środków, przed przekazaniem mu materiałów zgromadzonych w toku tych środków. Prokurator generalny Prokuratury Krajowej decyduje o zakresie i sposobie wykorzystania tych informacji. Postanowienia artykułów 238 ust. 3–5 i 239 KPK (pkt 58 poniżej) stosuje się *mutatis mutandis*.

57. Prokurator generalny Prokuratury Krajowej zarządza zniszczenie elementów uzyskanych z niejawnych środków nadzoru, jeżeli nie stanowią one dowodu popełnienia przestępstwa i nie mają znaczenia dla bezpieczeństwa państwa.

4. Kodeks postępowania karnego

58. Właściwe zapisy KPK brzmią następująco:

Artykuł 178

„Nie wolno przesłuchiwać jako świadków: 1) obrońcy albo adwokata lub radcy prawnego działającego na podstawie art. 245 ust. 1, co do

⁴ Przedłużenie może nastąpić na mocy orzeczenia sądu, na wniosek szefa ABW i za pisemną zgodą prokuratora generalnego Prokuratury Krajowej, na okres kolejnych trzech miesięcy. W należycie uzasadnionych przypadkach nadzór może zostać przedłużony przez właściwy sąd na kilka kolejnych okresów, przy czym łączny okres nadzoru nie może przekroczyć dwunastu miesięcy.

faktów, o których dowiedział się udzielając porady prawnej lub prowadząc sprawę;

2) duchownego co do faktów, o których dowiedział się przy spowiedzi”.

Art 178a

„Nie wolno przesłuchiwać jako świadka mediatora co do faktów, o których dowiedział się od oskarżonego lub pokrzywdzonego prowadząc

postępowanie mediacyjne, z wyłączeniem informacji o przestępstwach, o których

mowa w art. 240 ust. 1 Kodeksu karnego”.

Artykuł 179

„Ust. 1. Osoby obowiązane do zachowania w tajemnicy informacji niejawnych o klauzuli tajności „tajne” lub „ściśle tajne” mogą być przesłuchane co do okoliczności, na które rozciąga się ten obowiązek, tylko po zwolnieniu tych osób od

obowiązku zachowania tajemnicy przez uprawniony organ przełożony.

Ust. 2. Zwolnienia wolno odmówić tylko wtedy, gdyby złożenie zeznania wyrządzić mogło poważną szkodę państwu.

Ust. 3. Sąd lub prokurator może zwrócić się do właściwego naczelnego organu administracji państwowej o zwolnienie świadka od obowiązku zachowania tajemnicy, jeżeli ustawy szczególne nie stanowią inaczej”.

Artykuł 180

„Ust. 1. Osoby obowiązane do zachowania w tajemnicy informacji niejawnych o klauzuli tajności „zastrzeżone” lub „poufne” lub tajemnicy związanej z wykonywaniem zawodu lub funkcji mogą odmówić zeznań co do okoliczności, na które rozciąga się ten obowiązek, chyba że sąd lub prokurator dla dobra wymiaru sprawiedliwości zwolni te osoby od obowiązku zachowania tajemnicy, jeżeli ustawy szczególne nie stanowią inaczej. Na postanowienie w tym przedmiocie przysługuje zażalenie.

Ust. 2. Osoby obowiązane do zachowania tajemnicy notarialnej, adwokackiej, radcy prawnego, doradcy podatkowego, lekarskiej, dziennikarskiej lub statystycznej oraz tajemnicy Prokuratury Generalnej, mogą być przesłuchiwane co do faktów objętych tą tajemnicą tylko wtedy, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu. W postępowaniu przygotowawczym w przedmiocie przesłuchania lub zezwolenia na przesłuchanie decyduje sąd, na posiedzeniu bez udziału stron, w terminie nie dłuższym niż 7 dni od daty doręczenia wniosku prokuratora. Na postanowienie sądu przysługuje zażalenie.

Ust. 3. Zwolnienie dziennikarza od obowiązku zachowania tajemnicy nie może dotyczyć danych umożliwiających identyfikację autora materiału prasowego, listu do redakcji lub innego materiału o tym charakterze, jak również identyfikację osób udzielających informacji opublikowanych lub przekazanych do opublikowania, jeżeli osoby te zastrzegły nieujawnianie powyższych danych.

Ust. 4. Przepisu § 3 nie stosuje się, jeżeli informacja dotyczy przestępstwa, o którym mowa w art. 240 § 1 Kodeksu karnego.

Ust. 5. Odmowa przez dziennikarza ujawnienia danych, o których mowa w § 3, nie uchyla jego odpowiedzialności za przestępstwo, którego dopuścił się publikując informację”.

Artykuł 238

Ust. 1. Kontrola i utrwalanie rozmów telefonicznych mogą być wprowadzone najwyżej na okres 3 miesięcy, z możliwością przedłużenia, w szczególnie uzasadnionym wypadku, na okres najwyżej dalszych 3 miesięcy.

Ust. 2. Kontrola powinna być zakończona niezwłocznie po ustaniu przyczyn wymienionych w art. 237 § 1–3, najpóźniej jednak z upływem okresu, na który została wprowadzona.

Ust. 3. Prokurator po zakończeniu kontroli wnosi o zarządzenie zniszczenia wszystkich utrwalonych zapisów, jeżeli w całości nie mają znaczenia dla postępowania karnego. Sąd orzeka w przedmiocie wniosku niezwłocznie, na posiedzeniu bez udziału stron.

Ust. 4. Po zakończeniu postępowania przygotowawczego prokurator wnosi o zarządzenie zniszczenia utrwalonych zapisów w części, w jakiej nie mają znaczenia dla postępowania karnego, w którym zarządzono kontrolę i utrwalanie rozmów telefonicznych, oraz nie stanowią dowodu, o którym mowa w art. 237a. Sąd orzeka w przedmiocie wniosku na posiedzeniu, w którym mogą wziąć udział strony.

Ust. 5. Z wnioskiem o zarządzenie zniszczenia utrwalonych zapisów, nie wcześniej niż po zakończeniu postępowania przygotowawczego, może wystąpić także osoba wymieniona w art. 237 § 4. Sąd orzeka w przedmiocie wniosku na posiedzeniu, w którym mogą wziąć udział strony oraz wnioskodawca”.

Artykuł 239

Ust. 1. Ogłoszenie postanowienia o kontroli i utrwalaniu rozmów telefonicznych osobie, której ono dotyczy, może być odroczone na czas niezbędny ze względu na dobro sprawy.

Ust. 2. Ogłoszenie postanowienia, o którym mowa w § 1, w postępowaniu przygotowawczym może być odroczone nie później niż do czasu

zakończenia tego postępowania”.

Artykuł 321

Ust. 1. Jeżeli istnieją podstawy do zamknięcia śledztwa, na wniosek podejrzanego lub jego obrońcy o końcowe zaznajomienie z materiałami postępowania, prowadzący postępowanie powiadamia podejrzanego i obrońcę o terminie końcowego zaznajomienia, pouczając ich o prawie uprzedniego przejrzenia akt w terminie odpowiednim do wagi lub złożoności sprawy, określonym przez organ procesowy. W celu przejrzenia akt prokurator może udostępnić akta w postaci elektronicznej.

Ust. 2. Termin zaznajomienia podejrzanego z materiałami postępowania powinien być tak wyznaczony, aby od daty doręczenia zawiadomienia o nim podejrzanemu i jego obrońcy upłynęło co najmniej 7 dni.

Ust. 3. W czynnościach zaznajomienia podejrzanego z materiałami postępowania ma prawo uczestniczyć obrońca.

Ust. 4. Nieusprawiedliwione niestawiennictwo podejrzanego lub jego obrońcy nie tamuje dalszego postępowania.

Ust. 5. W terminie 3 dni od daty zaznajomienia podejrzanego z materiałami postępowania strony mogą składać wnioski o uzupełnienie śledztwa. Przepis art. 315 § 2 stosuje się odpowiednio.

Ust. 6. Jeżeli nie zachodzi potrzeba uzupełnienia śledztwa, wydaje się postanowienie o jego zamknięciu i ogłasza się je lub o jego treści zawiadamia się podejrzanego oraz jego obrońcę”.

Artykuł 393

Ust. 1. Wolno odczytywać na rozprawie protokoły oględzin, przeszukania i zatrzymania rzeczy, opinie biegłych, instytutów, zakładów lub instytucji, dane o karalności, wyniki wywiadu środowiskowego oraz wszelkie dokumenty urzędowe złożone w postępowaniu przygotowawczym lub sądowym albo w innym postępowaniu przewidzianym przez ustawę. Nie wolno jednak odczytywać notatek dotyczących czynności, z których wymagane jest sporządzenie protokołu.
(...)”.

5. Ustawa z 6 września 2001 o dostępie do informacji publicznej

59. Właściwe zapisy ustawy o dostępie do informacji publicznej brzmią następująco:

Artykuł 1

1. Każda informacja o sprawach publicznych stanowi informację publiczną w rozumieniu ustawy i podlega udostępnieniu na zasadach i w trybie określonych w niniejszej ustawie.

2. Przepisy ustawy nie naruszają przepisów innych ustaw określających odmienne zasady i tryb dostępu do informacji będących informacjami publicznymi”.

Artykuł 2

1. Każdemu przysługuje, z zastrzeżeniem art. 5, prawo dostępu do informacji publicznej, zwane dalej ‘prawem do informacji publicznej’.

2. Od osoby wykonującej prawo do informacji publicznej nie wolno żądać wykazania interesu prawnego lub faktycznego.
(...)”.

Artykuł 5

Prawo do informacji publicznej podlega ograniczeniu w zakresie i na zasadach określonych w przepisach o ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo chronionych.
(...)”.

Artykuł 10

Informacja publiczna, która nie została udostępniona w Biuletynie Informacji Publicznej lub portalu danych, jest udostępniana na wniosek.
(...)”.

Artykuł 16

1. Odmowa udostępnienia informacji publicznej oraz umorzenie postępowania o udostępnienie informacji w przypadku określonym w art. 14 ust. 2 przez organ władzy publicznej następują w drodze decyzji.

2. Do decyzji, o których mowa w ust. 1, stosuje się przepisy Kodeksu postępowania administracyjnego, z tym, że:

1) odwołanie od decyzji rozpoznaje się w terminie 14 dni;

2) uzasadnienie decyzji o odmowie udostępnienia informacji zawiera także imiona, nazwiska i funkcje osób, które zajęły stanowisko w toku postępowania o udostępnienie informacji oraz oznaczenie podmiotów, ze względu na których dobra, (...) wydano decyzję o odmowie udostępnienia informacji”.

6. Ustawa z 5 sierpnia 2010 o ochronie informacji niejawnych

60. Właściwe zapisy ustawy o ochronie danych niejawnych stanowią, co następuje:

Artykuł 4

1. Informacje niejawne mogą być udostępnione wyłącznie osobie dającej

rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonywania przez nią pracy lub pełnienia służby na zajmowanym stanowisku albo wykonywania czynności zleconych.

2. Zasady zwalniania od obowiązku zachowania w tajemnicy informacji niejawnych oraz sposób postępowania z aktami spraw zawierającymi informacje niejawne w postępowaniu przed sądami i innymi organami określają przepisy odrębnych ustaw.

3. Jeżeli przepisy odrębnych ustaw uprawniają organy, służby lub instytucje albo ich upoważnionych pracowników do dokonywania kontroli, w szczególności do swobodnego dostępu do pomieszczeń i materiałów, a jej zakres dotyczy informacji niejawnych, uprawnienia te są realizowane z zachowaniem przepisów niniejszej ustawy”.

Artykuł 5

1. Informacjom niejawnym nadaje się klauzulę ‘ściśle tajne’, jeżeli ich nieuprawnione ujawnienie spowoduje wyjątkowo poważną szkodę dla

Rzeczypospolitej Polskiej przez to, że:

- 1) zagrazi niepodległości, suwerenności lub integralności terytorialnej Rzeczypospolitej Polskiej;
- 2) zagrazi bezpieczeństwu wewnętrznemu lub porządkowi konstytucyjnemu Rzeczypospolitej Polskiej;
- 3) zagrazi sojuszom lub pozycji międzynarodowej Rzeczypospolitej Polskiej;
- 4) osłabi gotowość obronną Rzeczypospolitej Polskiej;
- 5) doprowadzi lub może doprowadzić do identyfikacji funkcjonariuszy (...) służb odpowiedzialnych za realizację zadań wywiadu lub kontrwywiadu (...), jeżeli zagrazi to bezpieczeństwu wykonywanych czynności lub może doprowadzić do identyfikacji osób udzielających im pomocy w tym zakresie;
- 6) zagrazi lub może zagrazić życiu lub zdrowiu funkcjonariuszy, żołnierzy lub pracowników, którzy wykonują czynności operacyjno-rozpoznawcze, lub osób udzielających im pomocy w tym zakresie;
- 7) zagrazi lub może zagrazić życiu lub zdrowiu świadków koronnych lub osób dla nich najbliższych, osób, którym udzielono środków ochrony i pomocy przewidzianych w ustawie z dnia 28 listopada 2014 r. o ochronie i pomocy dla pokrzywdzonego i świadka (Dz. U. z 2015 r. poz. 21), albo świadków, o których mowa w art. 184 ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego, lub osób dla nich najbliższych.

2. Informacjom niejawnym nadaje się klauzulę „tajne”, jeżeli ich

nieuprawnione ujawnienie spowoduje poważną szkodę dla Rzeczypospolitej Polskiej przez to, że:

- 1) uniemożliwi realizację zadań związanych z ochroną suwerenności lub porządku konstytucyjnego Rzeczypospolitej Polskiej;
- 2) pogorszy stosunki Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi;
- 3) zakłóci przygotowania obronne państwa lub funkcjonowanie Sił Zbrojnych Rzeczypospolitej Polskiej;
- 4) utrudni wykonywanie czynności operacyjno-rozpoznawczych prowadzonych w celu zapewnienia bezpieczeństwa państwa lub ścigania sprawców zbrodni (...);
- 5) w istotny sposób zakłóci funkcjonowanie organów ścigania i wymiaru sprawiedliwości;
- 6) przyniesie stratę znacznych rozmiarów w interesach ekonomicznych Rzeczypospolitej Polskiej.

3. Informacjom niejawnym nadaje się klauzulę „poufne”, jeżeli ich nieuprawnione ujawnienie spowoduje szkodę dla Rzeczypospolitej Polskiej przez to, że:

- 1) utrudni prowadzenie bieżącej polityki zagranicznej Rzeczypospolitej Polskiej;
- 2) utrudni realizację przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową Sił Zbrojnych Rzeczypospolitej Polskiej;
- 3) zakłóci porządek publiczny lub zagrazi bezpieczeństwu obywateli;
- 4) utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów Rzeczypospolitej Polskiej;
- 5) utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za

ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości;

- 6) zagrazi stabilności systemu finansowego Rzeczypospolitej Polskiej;
- 7) wpłynie niekorzystnie na funkcjonowanie gospodarki narodowej.

4. Informacjom niejawnym nadaje się klauzulę „zastrzeżone”, jeżeli nie nadano im wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony

narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej.

5. Informacje niejawne przekazane przez organizacje międzynarodowe lub inne państwa na podstawie umów międzynarodowych oznacza się polskim odpowiednikiem posiadanej klauzuli tajności”.

7. Ustawa z 16 lipca 2004 – Prawo telekomunikacyjne

61. Właściwe zapisy prawa telekomunikacyjnego stanowią, co następuje:

Artykuł 159

1. Tajemnica komunikowania się w sieciach telekomunikacyjnych, zwana dalej „tajemnicą telekomunikacyjną”, obejmuje:

1) dane użytkownika;

(...)”

3) dane transmisyjne, które oznaczają dane przetwarzane dla celów przekazywania komunikatów w sieciach telekomunikacyjnych lub naliczania opłat za usługi telekomunikacyjne, w tym dane lokalizacyjne, które oznaczają wszelkie dane przetwarzane w sieci telekomunikacyjnej lub w ramach usług telekomunikacyjnych wskazujące położenie geograficzne urządzenia końcowego użytkownika publicznie dostępnych usług telekomunikacyjnych;

4) dane o lokalizacji, które oznaczają dane lokalizacyjne wykraczające poza dane niezbędne do transmisji komunikatu lub wystawienia rachunku;

5) dane o próbach uzyskania połączenia między zakończeniami sieci, w tym dane o nieudanych próbach połączeń, oznaczających połączenia między telekomunikacyjnymi urządzeniami końcowymi lub zakończeniami sieci, które zostały zestawione i nie zostały odebrane przez użytkownika końcowego lub nastąpiło przerwanie zestawianych połączeń.

(...)”

Artykuł 161

1. Z zastrzeżeniem ust. 2, treści lub dane objęte tajemnicą telekomunikacyjną mogą być zbierane, utrwalane, przechowywane, opracowywane, zmieniane, usuwane lub udostępniane tylko wówczas, gdy czynności te, zwane dalej „przetwarzaniem”, dotyczą usługi świadczonej użytkownikowi albo są niezbędne do jej wykonania. Przetwarzanie w innych celach jest dopuszczalne jedynie na podstawie przepisów ustawowych.

(2) Dostawca publicznie dostępnych usług telekomunikacyjnych może przetwarzać następujące dane tego użytkownika będącego osobą fizyczną.

- 1) imię i nazwisko;
- 2) imiona rodziców;
- 3) miejsce i data urodzenia;
- 4) adres miejsca zamieszkania i adres korespondencyjny – jeżeli jest on inny niż adres miejsca zamieszkania;
- 5) numer PESEL – w przypadku obywatela Rzeczypospolitej Polskiej;
- 6) nazwę, serię i numeru dokumentu potwierdzającego tożsamość, a w przypadku cudzoziemca, który nie jest obywatelem państwa członkowskiego albo Konfederacji Szwajcarskiej – numer paszportu lub karty pobytu;
- 7) informacje zawarte w dokumentach poświadczających zdolność [użytkownika] do zapłaty roszczeń wobec dostawcy publicznie dostępnych usług telekomunikacyjnych wynikających z umowy o świadczenie [takich] usług.

(3) Oprócz danych, o których mowa w ust. 2, dostawca publicznie dostępnych usług telekomunikacyjnych może, za zgodą użytkownika będącego osobą fizyczną, przetwarzać inne dane tego użytkownika w związku ze świadczoną usługą, w szczególności numer konta bankowego lub karty płatniczej, a także numery telefonów kontaktowych”.

Artykuł 179

(...)

(9) Przedsiębiorca telekomunikacyjny świadczący publicznie dostępne usługi telekomunikacyjne jest obowiązany prowadzić elektroniczny wykaz abonentów, użytkowników lub zakończeń sieci, uwzględniając w nim dane uzyskiwane przy zawarciu umowy”.

Artykuł 180a

1. Z zastrzeżeniem art. 180c ust. 2 pkt 2, operator publicznej sieci telekomunikacyjnej oraz dostawca publicznie dostępnych usług telekomunikacyjnych są obowiązani na własny koszt:

- 1) zatrzymywać i przechowywać dane, o których mowa w art. 180c, generowane w sieci telekomunikacyjnej lub przez nich przetwarzane, na terytorium Rzeczypospolitej Polskiej, przez okres 12 miesięcy, licząc od dnia połączenia lub nieudanej próby połączenia, a z dniem upływu tego okresu dane te niszczyć, z wyjątkiem tych, które zostały zabezpieczone, zgodnie z przepisami odrębnymi;

2) udostępniać dane, o których mowa w pkt 1, uprawnionym podmiotom, a także sądowi i prokuratorowi, na zasadach i w trybie określonych w przepisach odrębnych;

3) chronić dane, o których mowa w pkt 1, przed przypadkowym lub bezprawnym zniszczeniem, utratą lub zmianą, nieuprawnionym lub bezprawnym przechowywaniem, przetwarzaniem, dostępem lub ujawnieniem (...).

2. Z zastrzeżeniem ust. 3, obowiązek, o którym mowa w ust. 1, uważa się za wykonany, jeżeli operator publicznej sieci telekomunikacyjnej lub dostawca publicznie dostępnych usług telekomunikacyjnych w przypadku zaprzestania działalności telekomunikacyjnej, przekaże dane do dalszego przechowywania, udostępniania oraz ochrony innemu operatorowi publicznej sieci telekomunikacyjnej lub dostawcy publicznie dostępnych usług telekomunikacyjnych.

3. Jeżeli ogłoszono upadłość operatora publicznej sieci telekomunikacyjnej lub dostawcy publicznie dostępnych usług telekomunikacyjnych, upadły operator lub dostawca ma obowiązek przekazania danych, o których mowa w ust. 1, do dalszego przechowywania, udostępniania oraz ochrony Prezesowi UKE.
(...)”

5. Obowiązkowi, o którym mowa w ust. 1, podlegają dane dotyczące połączeń zrealizowanych i nieudanych prób połączeń, o których mowa w art. 159 ust. 1 pkt 5.

6. Obowiązek, o którym mowa w ust. 1, powinien być realizowany w sposób, który nie powoduje ujawniania przekazu telekomunikacyjnego.

7. Udostępnianie danych, o którym mowa w ust. 1 pkt 1, może nastąpić za pomocą sieci telekomunikacyjnej, chyba że przepisy odrębne stanowią inaczej.

Artykuł 180c

1. Obowiązkiem, o którym mowa w art. 180a ust. 1, objęte są dane niezbędne do:

1) ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego:

a) inicjującego połączenie,

b) do którego kierowane jest połączenie;

2) określenia:

a) daty i godziny połączenia oraz czasu jego trwania,

b) rodzaju połączenia,

c) lokalizacji telekomunikacyjnego urządzenia końcowego.

2. Minister właściwy do spraw informatyzacji w porozumieniu z ministrem właściwym do spraw wewnętrznych (...) określi, w drodze rozporządzenia:

1) szczegółowy wykaz danych, o których mowa w ust. 1;

2) rodzaje operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do zatrzymywania i przechowywania tych danych”.

Artykuł 180d

Przedsiębiorcy telekomunikacyjni są obowiązani do zapewnienia warunków dostępu i utrwalania oraz do udostępniania uprawnionym podmiotom, a także sądowi i prokuratorowi, na własny koszt, przetwarzanych przez siebie danych, o których mowa w art. 159 ust. 1 pkt 1 i 3–5, w art. 161 oraz w art. 179 ust. 9, związanych ze świadczoną usługą telekomunikacyjną, na zasadach i przy zachowaniu procedur określonych w przepisach odrębnych”.

8. *Ustawa z 23 listopada 2012 – Prawo pocztowe*

62. Właściwe zapisy prawa pocztowego brzmią następująco:

Artykuł 82

„1. Operator pocztowy, począwszy od dnia rozpoczęcia działalności pocztowej, jest obowiązany do nieodpłatnego zapewnienia, w ramach wykonywanej przez siebie działalności pocztowej, technicznych i organizacyjnych możliwości wykonywania przez Policję, Straż Graniczną, Agencję Bezpieczeństwa Wewnętrznego, Służbę Kontrwywiadu Wojskowego, Żandarmerię Wojskową, Centralne Biuro Antykorupcyjne, Krajową Administrację Skarbową, Biuro Nadzoru Wewnętrznego, Inspektorat Wewnętrzny Służby Więziennej i Służbę Ochrony Państwa (...) oraz przez prokuraturę i sądy, ich zadań określonych odrębnymi przepisami, wymagających:

1) uzyskania danych o operatorze pocztowym, świadczonych usługach pocztowych oraz informacji umożliwiających identyfikację korzystających z tych usług,

2) udostępniania przesyłek pocztowych w celu kontroli treści korespondencji lub zawartości przesyłek,

3) udostępniania zatrzymanej przez operatora przesyłki pocztowej w przypadku podejrzenia, że stanowi przedmiot przestępstwa, do oględzin przez uprawnione podmioty,

4) dopuszczenia do dalszego przewozu przesyłki pocztowej zawierającej przedmioty przestępstwa (...) – zgodnie z zasadami i trybem określonymi w przepisach odrębnych.

9. Ustawa z 18 lipca 2002 o świadczeniu usług drogą elektroniczną

63. Ustawa o świadczeniu usług drogą elektroniczną stanowi, co następuje:

Artykuł 18

1. Usługodawca może przetwarzać następujące dane osobowe usługobiorcy niezbędne do nawiązania, kształtowania treści, zmiany lub rozwiązania stosunku prawnego między nimi:

- 1) nazwisko i imiona usługobiorcy;
- 2) numer ewidencyjny PESEL lub – gdy ten numer nie został nadany – numer paszportu, dowodu osobistego lub innego dokumentu potwierdzającego tożsamość;
- 3) adres zameldowania na pobyt stały;
- 4) adres do korespondencji, jeżeli jest inny niż adres, o którym mowa w pkt 3;
- 5) dane służące do weryfikacji podpisu elektronicznego usługobiorcy;
- 6) adresy elektroniczne usługobiorcy.

2. W celu realizacji umów lub dokonania innej czynności prawnej z usługobiorcą, usługodawca może przetwarzać inne dane niezbędne ze względu na właściwość świadczonej usługi lub sposób jej rozliczenia.

3. Usługodawca wyróżnia i oznacza te spośród danych, o których mowa w ust. 2, jako dane, których podanie jest niezbędne do świadczenia usługi drogą elektroniczną.

4. Usługodawca może przetwarzać, za zgodą usługobiorcy i dla celów reklamy, badania rynku oraz zachowań i preferencji usługobiorców z przeznaczeniem wyników tych badań na potrzeby polepszenia jakości usług świadczonych przez usługodawcę, inne dane dotyczące usługobiorcy, które nie są niezbędne do świadczenia usługi drogą elektroniczną.

5. Usługodawca może przetwarzać następujące dane charakteryzujące sposób korzystania przez usługobiorcę z usługi świadczonej drogą elektroniczną (dane eksploatacyjne):

- 1) oznaczenia identyfikujące usługobiorcę nadawane na podstawie danych, o których mowa w ust. 1;

2) oznaczenia identyfikujące zakończenie sieci telekomunikacyjnej lub system teleinformatyczny, z którego korzystał usługobiorca;

3) informacje o rozpoczęciu, zakończeniu oraz zakresie każdorazowego korzystania z usługi świadczonej drogą elektroniczną;

4) informacje o skorzystaniu przez usługobiorcę z usług świadczonych drogą elektroniczną.

6. Usługodawca nieodpłatnie udostępnia dane, o których mowa w ust. 1–5, organom państwa uprawnionym na podstawie odrębnych przepisów na potrzeby prowadzonych przez nie postępowań.

10. Ustawa z 28 stycznia 2016 – Prawo o prokuraturze

64. Właściwe zapisy prawa o prokuraturze brzmią następująco:

Artykuł 1

(...)

Ust. 2. Prokurator Generalny jest naczelnym organem prokuratury. Urząd Prokuratora Generalnego sprawuje Minister Sprawiedliwości. (...)”

Artykuł 11

Ust. 1. Prokurator Generalny przedstawia Sejmowi i Senatowi jawną roczną informację o łącznej liczbie osób, wobec których został skierowany wniosek o zarządzenie kontroli i utrwalania rozmów lub wniosek o zarządzenie kontroli operacyjnej, ze wskazaniem liczby osób, co do których:

1) sąd zarządził kontrolę i utrwalanie rozmów lub kontrolę operacyjną,

2) sąd odmówił zarządzenia kontroli i utrwalania rozmów lub kontroli operacyjnej,

3) wniosek o kontrolę operacyjną nie uzyskał zgody prokuratora

(...)”

Ust. 2. Informacja, o której mowa w § 1, powinna być przedstawiona Sejmowi i Senatowi do dnia 30 czerwca roku następnego po roku nią objętym”.

Artykuł 13

„Ust. 1. Prokurator Generalny kieruje działalnością prokuratury (...).

Ust. 2. Prokurator Generalny jest przełożonym prokuratorów (...)”

11. Ustawa z 9 czerwca 2006 o Centralnym Biurze Antykorupcyjnym

65. Art. 12 ust. 3 i 4 tej ustawy stanowi, że szef CBA musi przedłożyć premierowi i komisji parlamentarnej nadzorującej służby specjalne najpóźniej do 31 marca roczne sprawozdanie zawierające informacje o operacjach przeprowadzonych w poprzednim roku przez podległe mu służby, oraz że musi poinformować Sejm i Senat o wynikach operacji, które nie wchodzą w zakres przepisów o ochronie danych niejawnych.

12. Ustawa z 27 lipca 2001 – Prawo o ustroju sądów powszechnych

66. Art. 175b ust. 1 i 2 tej ustawy stanowi, że każdego roku prezesi właściwych miejscowo sądów okręgowych przekazują ministrowi spraw wewnętrznych informacje na temat przetwarzania danych dotyczących telekomunikacji, łączności pocztowej i łączności internetowej, wraz ze szczegółowymi danymi na temat liczby pozytywnie rozpatrzonych wniosków o dostęp do przedmiotowych danych oraz wniosków z kontroli zarządzanych przez nich w tym obszarze. Przewiduje również, że co roku minister sprawiedliwości przekazuje Sejmowi i Senatowi kompendium informacji na temat przetwarzania wyżej wymienionych danych, a także wnioski z kontroli, które przeprowadził w tym obszarze.

13. Kodeks postępowania administracyjnego

67. Właściwe zapisy KPA brzmią następująco:

Artykuł 227

Przedmiotem skargi może być w szczególności zaniedbanie lub nienależyte wykonywanie zadań przez właściwe organy albo przez ich pracowników, naruszenie praworządności lub interesów skarżących, a także przewlekłe lub biurokratyczne załatwianie spraw.

Artykuł 228

Skargi składa się do organów właściwych do ich rozpatrzenia.

Artykuł 238

Ust. 1. Zawiadomienie o sposobie załatwienia skargi powinno zawierać: oznaczenie organu, od którego pochodzi, wskazanie, w jaki sposób skarga została załatwiona, oraz podpis z podaniem imienia, nazwiska i stanowiska służbowego osoby upoważnionej do załatwienia skargi (...). Zawiadomienie o odmownym załatwieniu skargi powinno zawierać ponadto uzasadnienie faktyczne i prawne oraz pouczenie o treści

art. 239.

Ust. 2. W zawiadomieniu, o którym mowa w § 1, w jednostkach organizacyjnych resortu obrony narodowej, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego,

Służby Wywiadu Wojskowego oraz Centralnego Biura Antykorupcyjnego można pominąć imię i nazwisko osoby upoważnionej do załatwienia skargi”.

14. Kodeks cywilny (KC)

68. Zgodnie z art. 417¹ ust. 1, 2 i 4 KC każdy, kto uważa, że poniósł szkodę w wyniku przyjęcia aktu ustawodawczego, może wystąpić z roszczeniem o odszkodowanie, jeżeli po przeprowadzeniu odpowiedniego postępowania stwierdzono, że dany akt ustawodawczy jest niezgodny z Konstytucją, umową międzynarodową lub ustawą. Każda osoba, która uważa, że poniosła szkodę w wyniku orzeczenia sądowego lub decyzji wydanej przez organ władzy publicznej, może, o ile ustawa nie stanowi inaczej, wystąpić z roszczeniem o odszkodowanie, jeżeli po zakończeniu odpowiedniego postępowania stwierdzono, że dane orzeczenie jest nieprawidłowe lub ustalono, że akt normatywny będący jego podstawą był sprzeczny z Konstytucją, umową międzynarodową lub ustawą. Jeżeli szkoda została wyrządzona przez nieprzyjęcie aktu prawnego, którego uchwalenie było obowiązkowe z mocy prawa, sąd orzekający w sprawie o odszkodowanie wniesionej przez poszkodowanego musi ustalić, czy sytuacja wynikająca ze wspomnianego zaniechania legislacyjnego była zgodna z prawem.

15. Ustawa o Trybunale Konstytucyjnym

69. Zgodnie z art. 77 ust. 1 tej ustawy skarga konstytucyjna może być wniesiona po wyczerpaniu wszystkich przysługujących środków zaskarżenia, o ile takie istnieją, w terminie trzech miesięcy od dnia doręczenia orzeczenia, decyzji lub innego ostatecznego aktu.

16. Orzecznictwo Trybunału Konstytucyjnego

a) Orzeczenie K 32/04 z 12 grudnia 2005

70. W sprawie rozstrzygniętej wyrokiem K 32/04 z 12 grudnia 2005 rzecznik praw obywatelskich złożył wniosek do Trybunału Konstytucyjnego, w którym zgłosił między innymi, że art. 19 ust. 16 ustawy o Policji był niezgodny z kilkoma przepisami Konstytucji w zakresie, w jakim nie nakładał na funkcjonariuszy Policji, którzy prowadzili kontrolę operacyjną, obowiązku zawiadomienia osoby, wobec której była ona prowadzona (z wyjątkiem jedynie oskarżonego i jego obrońcy), o kontroli po jej przeprowadzeniu, w sytuacji gdy zawiadomienie takie mogło być dokonane bez narażenia na szkodę celu danej kontroli.

71. W swoim orzeczeniu Trybunał Konstytucyjny orzekł, że kwestionowany przepis wyklucza powiadomienie zainteresowanej osoby o środku nadzoru operacyjnego w trakcie jego trwania, ale nie wyklucza powiadomienia po przeprowadzeniu danego środka nadzoru, jeżeli nie doprowadziło to do wszczęcia postępowania karnego przeciwko zainteresowanej osobie. Trybunał Konstytucyjny orzekł, że po przeprowadzeniu nadzoru operacyjnego osoby fizyczne powinny mieć możliwość skorzystania z prawa zagwarantowanego w art. 51 ust. 3 Konstytucji do uzyskania informacji o danych zgromadzonych bez ich wiedzy w ramach przedmiotowego nadzoru. Jednocześnie zauważył, że należy dokonać rozróżnienia między, z jednej strony, sytuacją, w której

obowiązujące przepisy w żaden sposób nie uniemożliwiały powiadomienia o kontroli operacyjnej osoby, która była nią objęta, jeżeli osoba ta tego zażądała, a z drugiej strony sytuacją, w której służby państwowe, które przeprowadziły kontrolę operacyjną, miały obowiązek powiadomienia zainteresowanej osoby o zakończeniu kontroli. Uznał, że wprowadzenie takiego obowiązku dla zainteresowanych służb państwowych byłoby pożądane i przydatne dla skutecznej proceduralnej realizacji prawa określonego w art. 51 ust. 4 Konstytucji. Wskazał również, że inne państwa europejskie napotkały podobny problem, co doprowadziło do zwiększenia poziomu ochrony proceduralnej jednostek (powołując się na przykład niemieckiego ustawodawcy, który działając w następstwie sprawy *Klass i inni* [*Klass i inni przeciwko Niemcom*, wyrok z 6 września 1978, seria A nr 28] wprowadził obowiązek informowania przez właściwe organy publiczne osoby, której dane dotyczą, po przeprowadzeniu kontroli operacyjnej, o środku nadzoru zastosowanym bez jej wiedzy). Stwierdził, że w tym przypadku zarzut RPO, że zainteresowana osoba nie została powiadomiona o kontroli operacyjnej, wynikał z niedociągnięcia legislacyjnego, którego nie mógł naprawić w kontekście kontroli konstytucyjności przepisów.

b) Orzeczenie S 2/06 z 25 stycznia 2006

72. W decyzji S 2/06 z 25 stycznia 2006, która zapadła po wydaniu ww. wyroku K 32/04, Trybunał Konstytucyjny, udzielając z urzędu wskazówek ustawodawcy, uznał za konieczne przyjęcie dodatkowych środków ochronnych dla osób podlegających nadzorowi na podstawie ustawy o Policji oraz dokonanie analogicznej nowelizacji ustaw, których przepisy były podobne do tych, które były przedmiotem jego kontroli w ww. wyroku.

c) Wyrok K 23/11 z 30 lipca 2014

73. Sprawa, w której zapadł wyrok K 23/11 z 30 lipca 2014, dotyczyła konstytucyjności kilku przepisów regulujących prowadzenie kontroli operacyjnej przez różne służby policyjne i wywiadowcze. Trybunał Konstytucyjny, orzekając w sprawie wniosków złożonych odpowiednio przez rzecznika praw obywatelskich i prokuratora generalnego Prokuratury Krajowej, uznał niektóre z zaskarżonych przepisów za sprzeczne z Konstytucją. W uzasadnieniu wyroku Trybunał zauważył, co następuje:

– niektóre przepisy określające katalog przestępstw, w związku z którymi mogą być prowadzone kontrole operacyjne, były niejasno zdefiniowane. Dotyczyło to w szczególności odpowiednich przepisów ustawy o ABW oraz Służbach Wywiadowczych, które określały prawo służb ABW do prowadzenia kontroli operacyjnej w zakresie przestępstw „skierowanym przeciwko podstawom gospodarczym państwa”. Z kolei przepisy dotyczące Policji, kontroli skarbowej, Żandarmerii Wojskowej i Straży Granicznej, na podstawie których służby te były uprawnione do stosowania kontroli operacyjnej w odniesieniu do przestępstw „karalnych na podstawie umów i porozumień międzynarodowych”, były zgodne z Konstytucją, o ile były interpretowane jako odnoszące się wyłącznie do przestępstw karalnych na podstawie polskiego Kodeksu karnego i ratyfikowanych przez parlament umów międzynarodowych (mających rangę ustawy). To samo dotyczyło odpowiednich przepisów ustawy o ABW oraz Służbach Wywiadowczych, zgodnie z którymi właściwe organy ABW mogły stosować kontrolę

operacyjną w odniesieniu do „innych” przestępstw „przeciwko bezpieczeństwu państwa”;

– argument RPO dotyczący niejasności przepisów określających środki techniczne, które służby państwowe mogą stosować w kontekście kontroli operacyjnej, powinien zostać odrzucony. Chociaż lista środków była obszerna, nie była ona nieograniczona. Zbyt zwięzłe regulacje w tym obszarze byłyby szkodliwe dla imperatywów bezpieczeństwa publicznego i sprawnego funkcjonowania operacji prowadzonych przez odpowiednie służby państwowe. Najważniejsze w tym kontekście było to, że obowiązujące przepisy oferowały zainteresowanym osobom solidne gwarancje ochrony przed możliwymi nadużyciami ze strony wspomnianych służb państwowych. Jednakże jednym z zabezpieczeń przewidzianych w omawianych przepisach był obowiązek określenia przez operatorów we wnioskach o zezwolenie na wprowadzenie monitorowania operacyjnego środków technicznych, za pomocą których byłby prowadzony przedmiotowy nadzór. Ponadto informacje te musiały być zawarte w nakazach sądowych zezwalających na nadzór. Ponadto procedura zatwierdzania kontroli operacyjnych, która odbywała się w kilku etapach, sama w sobie stanowiła ważną gwarancję ochrony przed arbitralnością w odniesieniu do wprowadzonych środków nadzoru. Z informacji, którymi dysponowała, jasno wynikało, że istniejąca sądowa kontrola legalności nadzoru i stosowności środków, za pomocą których był on prowadzony, była skuteczna;

– przepisy dotyczące przekazywania przez operatorów publicznych sieci telekomunikacyjnych i dostawców usług telekomunikacyjnych danych dotyczących komunikacji Policji i służbom wywiadowczym były sprzeczne z Konstytucją, ponieważ nie przewidywały żadnego mechanizmu zapewniającego niezależny nadzór służb państwowych nad takim przekazywaniem. To samo dotyczyło odpowiednich przepisów ustawy o ABW oraz Służbach Wywiadowczych, ustawy o CBA oraz ustawy o SKW w zakresie, w jakim wyraźnie wykluczały one jakikolwiek niezależny nadzór zewnętrzny w tym obszarze. Z przepisów określających przestępstwa, w odniesieniu do których można zastosować dany środek nadzoru, wynikało, że może on dotyczyć każdego przestępstwa, w tym najbardziej błahego. Ponadto, władze uciekające się do takiego środka nie były zobowiązane do wykazania, że jest on zgodny z zasadą pomocniczości i że jest konieczny w danych okolicznościach. Fakt, że tylko agenci odpowiednich służb państwowych z wymaganym poświadczeniem bezpieczeństwa mogli prowadzić tego rodzaju nadzór, nie zapewniał zainteresowanej osobie wystarczająco solidnej gwarancji przeciwko jakimkolwiek nadużyciom z ich strony. Specyfika przedmiotowego nadzoru doprowadziła Trybunał Konstytucyjny do wniosku, że najbardziej odpowiednim mechanizmem kontroli w tym obszarze jest kontrola a posteriori. W związku z tym nie było potrzeby wprowadzania wymogu uzyskania zezwolenia dla każdego środka nadzoru, niezależnie od stopnia ingerencji w sferę prywatną danej osoby. Ustawodawca powinien był jednak rozważyć wprowadzenie kontroli a priori w odniesieniu do środków podejmowanych w sytuacjach innych niż nagłe lub w przypadku gromadzenia przez służby państwowe prowadzące nadzór informacji objętych tajemnicą zawodową. Przegląd środków nadzoru niekoniecznie musiał mieć charakter sądowy, ale musiał być zgodny z zasadami określonymi w tej dziedzinie przez Europejski Trybunał Praw Człowieka i TSUE, a w szczególności musiał być powierzony organowi niezależnemu od władzy wykonawczej;

– zaskarżone przepisy⁵ w zakresie, w jakim nie przewidywały żadnej procedury niszczenia materiałów objętych tajemnicą adwokacką, dziennikarską lub tajemnicą spowiedzi, które zostały zgromadzone w toku kontroli operacyjnej bez uchylecia tej tajemnicy przez sąd lub w czasie, gdy ustawa uniemożliwiała takie uchYLECIE, były sprzeczne z Konstytucją. Podczas gdy z pewnością nie było właściwe całkowite wyłączenie komunikacji między adwokatami a ich klientami z zakresu nadzoru, konsekwencje takiej komunikacji dla prawa do obrony były takie, że ich poufność musiała być objęta większą ochroną nie tylko na wszystkich etapach postępowania karnego, ale także w kontekście nadzoru prowadzonego poza lub przed takim postępowaniem. Ponieważ monitorowanie komunikacji osób związanych tajemnicą zawodową nie było zakazane samo w sobie, konieczne było, aby towarzyszyły mu odpowiednie zabezpieczenia mające na celu ochronę zainteresowanych osób przed niewłaściwym nadzorem i zapobieganie niewłaściwemu uzyskiwaniu przez służby państwowe informacji objętych tajemnicą zawodową. Mechanizm zwolnienia z tajemnicy zawodowej określony w art. 180 ust. 2 KPK mógłby stanowić wzorzec odniesienia w tym zakresie, a przepisy regulujące stosowanie nadzoru przed wszczęciem postępowania karnego powinny wprowadzać podobny system, który z jednej strony powinien umożliwiać służbom państwowym prowadzącym nadzór identyfikację, przed przekazaniem innym organom, wszelkich zgromadzonych przez nie informacji objętych tajemnicą zawodową, a z drugiej strony powinien prowadzić do zniszczenia przez komisję protokolaną wszystkich elementów, o których mowa;

– odpowiednie zapisy ustawy o ABW oraz Służbach Wywiadowczych, ustawy o SKW oraz Służbach Wywiadu Wojskowego i ustawy o CBA były również sprzeczne z Konstytucją w zakresie, w jakim nie określały żadnych zasad niszczenia danych dotyczących komunikacji, które okazały się zbędne dla procedur, dla których zostały zgromadzone.

d) Orzeczenie K 32/15 z 30 czerwca 2021

74. W grudniu 2015 r. i lutym 2016 r. polski rzecznik praw obywatelskich złożył skargę do Trybunału Konstytucyjnego, wzywając go do zbadania zgodności z Konstytucją niektórych przepisów dotyczących kontroli operacyjnej w brzmieniu obowiązującym po wejściu w życie ustawy z dnia 15 stycznia 2016 r. i ustawy antyterrorystycznej. Przed Sądem Najwyższym argumentował on w szczególności, że sporne przepisy nie wykonywały wyroku Trybunału Konstytucyjnego K 23/11 (cytowanego powyżej), a ponadto, że stanowiły one jeszcze bardziej rażące naruszenia praw i wolności jednostki chronionych przez Konstytucję i odpowiednie normy prawa międzynarodowego niż te, które zostały usankcjonowane w tym wyroku. Główne zarzuty KPO w tym zakresie były następujące:

– maksymalny czas trwania nadzoru, ustalony na osiemnaście miesięcy, był nadmierny i wykraczał poza to, co uznano za „konieczne w demokratycznym społeczeństwie”. Co więcej, ustawodawstwo odnoszące się do niektórych służb policyjnych i wywiadowczych nie przewidywało żadnego maksymalnego limitu czasu trwania nadzoru;

– przepisy stanowiące, że sąd może zezwolić na wykorzystanie informacji

⁵ Ustawa o Policji, ustawa o ABW, ustawa o CBA, ustawa o SKW oraz Służbie Wywiadu Wojskowego, ustawa o SG oraz ustawa o ŻW

objętych tajemnicą zawodową jako dowodu w postępowaniu karnym, jeżeli jego zdaniem „wymaga tego interes prawidłowego administrowania wymiarem sprawiedliwości”, były nieprecyzyjne i naruszały prawo do obrony;

- zaskarżone przepisy nie gwarantowały sądowi orzekającemu w sprawie wniosku o zezwolenie na nadzór dostępu do całości akt, ponieważ nie wymagały od służb państwowych ubiegających się o zezwolenie na nadzór przedłożenia ich w całości;

- sformułowanie przepisów określających listę przestępstw, w związku z którymi można gromadzić dane dotyczące komunikacji, było zbyt szerokie;

- przepisy regulujące gromadzenie danych dotyczących komunikacji umożliwiły służbom państwowym praktycznie nieograniczone korzystanie z przedmiotowego środka, bez poddawania go jakiejkolwiek zewnętrznej kontroli. Kontrola przeprowadzona przez sądy okręgowe na podstawie półrocznych sprawozdań składanych przez odpowiednie służby państwowe zgodnie z ustawą z 15 stycznia 2016 nie była zgodna z wnioskami zawartymi w wyroku Trybunału Konstytucyjnego w sprawie K 23/11 i była nieskuteczna, ponieważ była fakultatywna, jej wnioski były poufne, a sądy okręgowe nie były uprawnione do nakazania zniszczenia materiałów zebranych niezgodnie z prawem w ramach nadzoru;

- władze nie zastosowały się do wyroku Trybunału Konstytucyjnego K 23/11 w następujących kwestiach: nie istniał obowiązek powiadomienia osoby zainteresowanej o decyzji sądu zezwalającej na nadzór, w wyniku czego osoba ta nigdy nie mogła zakwestionować legalności takiego środka; różne kategorie osób, które mogły podlegać nadzorowi, były niewystarczająco określone; nie określono maksymalnego terminu stosowania środka polegającego na gromadzeniu i przetwarzaniu danych dotyczących komunikacji przez służby państwowe, które zainicjowały tego rodzaju środek, a ponadto wdrożenie przedmiotowego środka przez dane służby państwowe nie podlegało żadnej skutecznej kontroli zewnętrznej; obowiązek zniszczenia przez ABW, SKW i Służby Wywiadu Wojskowego zgromadzonych przez nie danych telekomunikacyjnych dotyczył wyłącznie danych, które okazały się nieprzydatne dla postępowania, w ramach którego zostały zgromadzone;

- kilka przepisów ustawy o działaniach antyterrorystycznych dotyczących nadzoru było problematycznych, ponieważ były one nieprecyzyjne i miały zbyt szeroki zakres. Dotyczyło to w szczególności tych, które przewidywały możliwość zastosowania środka nadzoru w przypadku „podejrzenia wystąpienia incydentu o charakterze terrorystycznym”. Ponadto decyzja szefa ABW, na podstawie której wdrożono nadzór, nie podlegała żadnej kontroli zewnętrznej.

75. W kwietniu 2017 RPO wycofał swoje pierwsze odwołanie w zakresie, w jakim dotyczyło ono maksymalnego czasu trwania nadzoru prowadzonego przez Policję krajową, Straż Graniczną, Krajową Administrację Skarbową i Żandarmerię Wojskową. W marcu 2018 RPO uczynił to samo w odniesieniu do drugiego złożonego odwołania, uznając, że bezstronność i status jako sędziów niektórych osób uczestniczących w składzie orzekającym Trybunału Konstytucyjnego były kwestionowane, a w rezultacie skład orzekający w ten sposób nie gwarantował niezależnego i dokładnego zbadania sprawy, a także uznając, że ewentualne orzeczenie Trybunału Konstytucyjnego w tej sprawie mogłoby zapewnić niektórym zainteresowanym służbom państwowym środki legitymizacji ich praktyk, które naruszały obowiązujące normy

konstytucyjne i europejskie.

76. Orzeczeniem K 32/15 z 30 czerwca 2021 Trybunał Konstytucyjny zakończył postępowanie w sprawie pierwszej skargi RPO, przedstawiając następujące uwagi. Zarzut dotyczący maksymalnego czasu trwania nadzoru prowadzonego przez ABW, CBA i SKW był bezprzedmiotowy, gdyż po wejściu w życie ustawy z 15 stycznia 2016 czas ten został skrócony do 12 miesięcy. Część apelacji wskazująca na uchybienia w procedurze zatwierdzania kontroli operacyjnej została oparta na niewłaściwych przepisach konstytucyjnych. Jeśli chodzi o skargę dotyczącą braku powiadomienia zainteresowanych osób o orzeczeniu sądowym zezwalającym na nadzór, dotyczyła ona braku ustawodawstwa, kwestii, w której Trybunał nie był właściwy do orzekania, a zatem nie mógł kontynuować badania tej kwestii.

e) Orzeczenie SK 60/21 z 28 czerwca 2022

77. W marcu 2021 osoba poddana nadzorowi przez Policję złożyła skargę konstytucyjną, argumentując, że zapisy art. 19 ust. 20 ustawy o Policji nie przewidują dla osoby poddanej nadzorowi żadnego środka odwoławczego od decyzji zezwalającej na nadzór, a zatem są sprzeczne z Konstytucją.

78. W orzeczeniu SK 60/21 z 28 czerwca 2022 Trybunał Konstytucyjny postanowił nie badać dalej skargi, powołując się na powody podobne do tych podanych w orzeczeniu K 32/15 (zob. pkt 76 powyżej).

17. Orzecznictwo Naczelnego Sądu Administracyjnego

79. W sprawach opisanych poniżej skarżący złożyli wnioski o udzielenie informacji na temat stosowania niejawnych środków nadzoru przez Policję i służby wywiadowcze, powołując się na odpowiednie przepisy ustawy o dostępie do informacji publicznej. Szefowie wyżej wymienionych służb odrzucili ich wnioski, stwierdzając, że informacje są niejawne i dlatego nie mogą zostać im ujawnione. Skarżący zakwestionowali decyzje odmowne.

a) Wyrok w sprawie I OSK 932/16 z 6 lipca 2017

80. Wyrok I OSK 932/16 z 6 lipca 2017 dotyczy oddalenia przez szefa CBA wniosku Fundacji Helsińskiej w sprawie wykorzystania oprogramowania Xkeycore przez nadzorowane przez niego służby⁶. Odrzucając argumenty skarżącej fundacji, Naczelny Sąd Administracyjny orzekł, że informacje, których ujawnienia domagała się fundacja, dotyczyły metod pracy służb państwowych prowadzących nadzór, a zatem korzystających z ochrony podobnej do tej, która ma zastosowanie do danych niejawnych. Odnosząc się do odpowiednich zapisów art. 5 ustawy o ochronie danych niejawnych, uznał on, że ujawnienie skarżącej wspomnianych informacji mogłoby utrudnić sprawne prowadzenie operacji przez służby CBA. Stwierdził również, że doszedł do takiego wniosku po wyważeniu wymogów prawa skarżącej do informacji o działaniach władz publicznych z interesami gospodarczymi państwa i bezpieczeństwem publicznym. Wraz z

⁶ Program, który umożliwia niemal systematyczne gromadzenie informacji o aktywności każdego użytkownika w Internecie.

uzasadnieniem dodał, że zasada przejrzystości działań publicznych nie powinna być rozumiana jako gwarantująca jawność środków wykorzystywanych przez Policję i służby wywiadowcze do przeprowadzania operacji niejawnych.

b) Wyrok I OSK 2248/16 z 18 lipca 2018

81. Powyższy wyrok dotyczył wniosku organizacji pozarządowej Watchdog Polska do szefa ABW o przekazanie szeregu informacji dotyczących rzekomego wykorzystywania przez nadzorowane przez niego służby systemu automatycznego odczytu i rozpoznawania tablic rejestracyjnych. Kiedy szef ABW wydał decyzję odmowną, organizacja ta odwołała się do sądu administracyjnego o uchylenie tej odmownej decyzji. W swoim orzeczeniu sąd administracyjny uznał, że chociaż informacje, o które zwróciła się organizacja skarżąca, zostały uznane za „publiczne” w znaczeniu nadanym temu pojęciu przez ustawę o dostępie do informacji publicznej, to jednocześnie zostały one objęte ochroną przewidzianą w art. 5 ustawy o ochronie danych niejawnych. Zauważył również, że w tym przypadku przedmiotowe informacje dotyczyły zasobów technicznych wykorzystywanych przez służby ABW w ramach realizacji ich misji ochrony bezpieczeństwa publicznego i uznał, że ich ujawnienie zainteresowanej stronie byłoby sprzeczne z interesem publicznym. Organizacja skarżąca zaskarżyła wyrok do Naczelnego Sądu Administracyjnego. Ten oddalił jej odwołanie, orzekając, że informacje o środkach wykorzystywanych przez służby ABW do realizacji powierzonych im zadań są poufne w świetle odpowiednich przepisów ustawy o ABW i ustawy o ochronie danych niejawnych. Stwierdził również, że właściwe organy publiczne nie są zobowiązane do przedstawienia szczegółowego uzasadnienia swoich decyzji o odrzuceniu wniosków podobnych do tego, którego dotyczy niniejsza sprawa.

c) Wyrok I OSK 579/17 z 23 stycznia 2019

82. Sprawa będąca przedmiotem niniejszego wyroku dotyczyła odrzucenia przez szefa ABW wniosku osoby fizycznej o poinformowanie jej czy nadzorowane przez niego służby stosowały wobec niej środki nadzoru bez jej wiedzy. Naczelny Sąd Administracyjny orzekł, że z uwagi na szczególny charakter działań prowadzonych przez ABW oraz ich wpływ na bezpieczeństwo, wszelkie informacje z nimi związane, w tym dotyczące środków operacyjnych wykorzystywanych przez służby ABW oraz samego faktu stosowania środka nadzoru, powinny pozostać niejawne. Uznał, że przekazanie przedmiotowych informacji zainteresowanemu mogłoby mieć negatywny wpływ na sprawne prowadzenie czynności operacyjnych przez służby ABW, w związku z czym uznał, że szef ABW nie mógł przekazać skarżącemu żadnych informacji związanych z rzekomym prowadzeniem kontroli operacyjnej dotyczącej jego osoby. Dodał, że informacje tego typu, nawet gdyby zostały uznane za „publiczne”, były jednak poufne zgodnie z art. 5 ust. 1 ustawy o dostępie do informacji publicznej.

d) Wyrok I OSK 2687/17 z 27 września 2019

83. Wyrok I OSK 2687/17 z 27 września 2019 dotyczy odmownej

odpowiedzi szefa ABW na wniosek organizacji pozarządowej o udostępnienie informacji statystycznych dotyczących nadzoru prowadzonego przez podległe mu służby na podstawie art. 9 ustawy o działaniach antyterrorystycznych. Uzasadniając swoją decyzję, szef ABW powołał się m.in. na poufny charakter informacji, o które wnioskowała skarżąca organizacja oraz ryzyko, że ich ujawnienie zagroziłoby powodzeniu prowadzonych przez ABW operacji antyterrorystycznych. Gdy sąd administracyjny odrzucił skargę organizacji skarżącej na przedmiotową decyzję, organizacja ta odwołał się do Naczelnego Sądu Administracyjnego. Sąd uchylił zaskarżony wyrok i decyzję odmowną, przekazując sprawę do ponownego rozpoznania szefowi ABW. W uzasadnieniu zauważył, że o ile przekazanie zainteresowanej informacji dotyczących częstotliwości stosowania przez służby ABW środków określonych w art. 9–11 ustawy antyterrorystycznej oraz liczby osób, wobec których zastosowano przedmiotowe środki, mogłoby narazić na szwank skuteczność działania zainteresowanych służb państwowych, o tyle powody przedstawione przez szefa ABW nie uzasadniały tego samego w odniesieniu do informacji dotyczących częstotliwości korzystania przez niego z uprawnień przekazanych mu na podstawie art. 11 ust. 1 tej ustawy. Wskazał, że nie ma wątpliwości, że ujawnienie przez szefa ABW informacji pierwszego rodzaju zainteresowanemu mogłoby zaszkodzić bezpieczeństwu państwa, porządkowi publicznemu i prawidłowemu prowadzeniu działań przez podległe mu służby, co oznacza, że wspomniane informacje muszą pozostać poufne. Zwrócił uwagę, że w podobnym kontekście nawet czysto statystyczne informacje na temat praktyk w zakresie nadzoru danych służb państwowych mogą czasami wydawać się wrażliwe ze względów bezpieczeństwa i podlegać zwiększonej ochronie, równoważnej ochronie mającej zastosowanie do informacji poufnych. Dodał, że w takiej sytuacji ujawnienie takich informacji komukolwiek byłoby zabronione na mocy art. 5 ustawy o dostępie do informacji publicznej.

C. Przedmiotowe dane statystyczne

84. Każda ze stron opracowała statystyki dotyczące stosowania niejawnego nadzoru przez służby państwowe w latach 2017-2022. Informacje, o których mowa, pochodzą głównie z rocznych sprawozdań sporządzanych dla Sejmu i Senatu odpowiednio przez prokuratora generalnego Prokuratury Krajowej, ministra spraw wewnętrznych i ministra sprawiedliwości. Sprawozdania prokuratora generalnego Prokuratury Krajowej odnoszą się do liczby osób objętych wnioskami o zezwolenie na nadzór, a sprawozdania ministra spraw wewnętrznych dotyczą liczby wniosków o zezwolenie złożonych do sądów. Dostarczone dokumenty wskazują, co następuje:

Rok	Liczba osób objętych wnioskami o zezwolenie na nadzór	Liczba osób w stosunku do których prokurator odrzucił wniosek o zgodę na podsłuch lub kontrolę operacyjną	Liczba osób, w odniesieniu do których prokurator zatwierdził wnioski o zezwolenie na nadzór	Liczba osób w przypadku których sąd odrzucił wniosek o zezwolenie na podsłuch lub kontrolę operacyjną	Liczba osób, w przypadku których sąd zezwolił na podsłuch lub kontrolę operacyjną	Odsetek osób, w przypadku których sąd zezwolił na podsłuch lub kontrolę operacyjną	Odsetek osób, w odniesieniu do których prokurator lub sąd zezwolił na podsłuch i kontrolę operacyjną
2021 ¹¹	7071 ¹²	126 ¹³	6945 ¹⁴	25 ¹⁵	6922 ¹⁶	97,8-% ¹⁷	99,66-% ¹⁸

2020	6537	118	6419	35	6384	97,65 %	99,45 %
2019	5839	103	5736	25	5711	97,81 %	99,56 %
2018	6088	148	5940	25	5915	97,16 %	99,58 %
2017	6562	146	6416	14	6402	97,56 %	99,78 %

Rok	Liczba złożonych wniosków o zezwolenie na nadzór	Liczba wniosków o zezwolenie na nadzór odrzuconych przez prokuratora	Liczba wniosków o zezwolenie na nadzór zatwierdzonych przez prokuratora	Liczba wniosków o zezwolenie na nadzór odrzuconych przez sąd	Liczba wniosków o zezwolenie na nadzór zatwierdzonych przez sąd	Liczba spraw, w których w elementach zebranych w ramach nadzoru zostały wykorzystane jako dowód w postępowaniu karnym	Odsetek spraw, w których sąd zezwolił na podsłuch lub kontrolę operacyjną	Odsetek spraw, w których sąd lub prokurator zezwolił na podsłuch lub kontrolę operacyjną	Odsetek przypadków, w których informacje zebrane w ramach nadzoru zostały wykorzystane jako dowód
2017	9876	142	9734	9	9725	1525	98,47 %	99,91 %	15,68 %
2018	8451	205	8246	8	8238	1730	97,48 %	99,90 %	21 %
2019	8196	116	8080	15	8065	1303	97,48 %	99,81 %	16,15 %
2020	10115	150	10005	21	9984	1471	99,79 %	99,79 %	14,73 %
2021	11074	155	10919	7	10912	1672	99,93 %	99,93 %	15,32 %

85. Z informacji przedstawionych przez rząd, które nie zostały zakwestionowane przez skarżących, wynika, że w latach 2017–2021 Policja stosowała kontrolę operacyjną głównie w celu zapobiegania lub wykrywania przestępstw przeciwko porządkowi publicznemu, życiu i zdrowiu, bezpieczeństwu i wolności osobistej, przestępstw przeciwko mieniu, instytucjom państwowym i samorządowym, obrotowi pieniędzmi i finansowymi papierami wartościowymi, transakcjom handlowym oraz przestępstwom z ustawy o przeciwdziałaniu narkomanii.

86. Coroczne informacje opracowywane przez ministra sprawiedliwości dla Sejmu i Senatu pokazują, ile razy odpowiednie służby państwowe gromadziły dane dotyczące komunikacji. Wynika z niego również, że spośród 107, 163 i 136 kontroli stosowania przedmiotowego środka nadzoru przeprowadzonych przez sądy w latach 2019–2021 tylko odpowiednio jedna i dwie zakończyły się negatywną oceną służb państwowych, których dotyczyły przedmiotowe kontrole.

Rok	Dane dotyczące telekomunikacji	Dane dotyczące komunikacji pocztowej	Dane dotyczące komunikacji elektronicznej
2021	1 820 630	16 764	20 107
2020	1 546 326	13 309	24 959
2019	1 345 207	8 595	19 526
2018	1 325 241	8 601	22 933
2017	1 227 314	13 630	23 913

II. ODPOWIEDNIE TEKSTY MIĘDZYNARODOWE

A. Organizacja Narodów Zjednoczonych

Rezolucja nr 68/167 w sprawie prawa do prywatności w erze cyfrowej

87. Rezolucja nr 68/167 w sprawie prawa do prywatności w erze cyfrowej, przyjęta przez Zgromadzenie Ogólne 18 grudnia 2013 brzmi we fragmentach istotnych dla niniejszej sprawy następująco:

„Walne Zgromadzenie,

(...)

4. Zaprasza wszystkie państwa:

(...)

(c) Do dokonania przeglądu swoich procedur, praktyk i przepisów dotyczących nadzoru i przechwytywania komunikacji oraz gromadzenia danych osobowych, szczególnie na dużą skalę, w celu ochrony prawa do prywatności, zapewniając pełną zgodność ze wszystkimi zobowiązaniami wynikającymi z prawa międzynarodowego;

d) Do ustanowienie lub utrzymania, w przypadku gdy już istnieją, skutecznych niezależnych krajowych mechanizmów nadzorczych zdolnych do zapewnienia przejrzystości nadzoru i przechwytywania komunikacji oraz gromadzenia danych osobowych, które są przez nie przeprowadzane, w stosownych przypadkach, oraz do ich przestrzegania; (...)

B. Rada Europy

1. Konwencja Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (1981)

88. Konwencja o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych określa standardy ochrony danych w zakresie automatycznego przetwarzania danych osobowych w sektorze publicznym i prywatnym. We właściwych zapisach stanowi ona, co następuje:

Preambuła

Państwa członkowskie Rady Europy, sygnatariusze niniejszej Konwencji;

Zważywszy, że celem Rady Europy jest osiągnięcie większej jedności jej członków, w poszanowaniu zwłaszcza zasady rządów prawa oraz praw człowieka i podstawowych wolności;

Zważywszy, że pożądane jest rozszerzenie zakresu ochrony praw i podstawowych wolności każdego człowieka, w szczególności prawa do poszanowania prywatności, biorąc pod uwagę zwiększający się przepływ przez granice danych osobowych przetwarzanych automatycznie;

Potwierdzając jednocześnie swoje zaangażowanie na rzecz swobodnego

przepływu informacji bez względu na istniejące granice;

Uznając konieczność pogodzenia podstawowych wartości takich, jak poszanowanie prywatności ze swobodnym obiegiem informacji między narodami;

Uzgodniły co następuje:

Artykuł 1 – Postanowienia ogólne

Niniejsza Konwencja ma na celu zagwarantowanie, na terytorium każdej ze Stron, każdej osobie fizycznej, niezależnie od jej narodowości i miejsca zamieszkania, poszanowanie jej praw i podstawowych wolności, w szczególności prawa do prywatności, w związku z automatycznym przetwarzaniem dotyczących jej danych osobowych ('ochrona danych').
(...)"

Artykuł 8 – Gwarancje dodatkowe dla podmiotu danych

Każda osoba jest upoważniona do:

a. ustalenia informacji o istnieniu zautomatyzowanego zbioru danych osobowych, o jego zasadniczych celach oraz o tożsamości i miejscu zamieszkania lub siedzibie kontrolera zbioru;

b. otrzymywania w rozsądnych odstępach czasu, bez nadmiernej zwłoki i nadmiernych kosztów, potwierdzenia, że w danym zautomatyzowanym zbiorze znajdują się lub nie znajdują jej dane osobowe, oraz uzyskiwania tych danych w czytelnej formie;

c. uzyskania, w razie potrzeby, sprostowania lub usunięcia tych danych, jeśli zostały przetworzone z naruszeniem przepisów prawa wewnętrznego wprowadzających w życie zasady wymienione w art. 5 i 6 niniejszej Konwencji;

d. ustalenia formy zadośćuczynienia w razie nieuwzględnienia jej prośby o potwierdzenie albo udostępnienie, sprostowanie lub usunięcie danych w myśl pkt. b) i c) niniejszego artykułu.

Artykuł 9 – Wyjątki i ograniczenia

1. Wyjątki od przepisów art. 5, 6 i 8 niniejszej Konwencji dopuszczalne są jedynie w granicach określonych w niniejszym artykule.

2. Odstąpienie od stosowania art. 5, 6 i 8 niniejszej Konwencji jest dozwolone, jeśli przewidywane jest ustawowo przez Stronę, jako środek konieczny w społeczeństwie demokratycznym w interesie:

a. ochrony Państwa, bezpieczeństwa publicznego, interesów walutowych państwa lub zwalczania przestępczości;

b. ochrony podmiotu danych oraz praw i wolności innych osób.

(...)”

Artykuł 10 – Sanckje i odszkodowania

Każda ze Stron zobowiązuje się do wprowadzania odpowiednich sankcji i odszkodowań w przypadku naruszeń przepisów prawa wewnętrznego wprowadzających w życie podstawowe zasady ochrony danych, wymienione w niniejszym rozdziale”.

89. W sprawozdaniu wyjaśniającym dotyczącym powyższej konwencji przedstawiono następujące punkty:

Artykuł 9 – Wyjątki i ograniczenia

55. Wyjątki od podstawowych zasad ochrony danych są ograniczone do tych, które są niezbędne do ochrony podstawowych wartości w demokratycznym społeczeństwie. Tekst ustępu drugiego tego artykułu został zainspirowany tekstem ustępów drugich artykułów 6, 8, 10 i 11 Europejskiej Konwencji Praw Człowieka. Z decyzji Komisji i Trybunału Praw Człowieka dotyczących pojęcia „niezbędnego środka” jasno wynika, że kryteria takiego pojęcia nie mogą być ustalone dla wszystkich krajów i wszystkich czasów, ale muszą być rozpatrywane w odniesieniu do danej sytuacji w każdym kraju.

56. Ustęp 2(a) wymienia główne interesy państwa, które mogą wymagać wyjątków. Wyjątki te zostały sformułowane bardzo precyzyjnie, aby zapewnić, że państwa nie będą miały zbyt dużej swobody w ogólnym stosowaniu Konwencji.

Zgodnie z art. 16 państwa zachowują prawo do odmowy stosowania Konwencji w indywidualnych przypadkach z istotnych powodów, w tym wymienionych w art. 9.

Pojęcie „bezpieczeństwa państwa” należy rozumieć w tradycyjnym sensie ochrony suwerenności narodowej przed zagrożeniami wewnętrznymi i zewnętrznymi, w tym ochrony stosunków międzynarodowych państwa”.

2. Protokół dodatkowy do Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych dotyczący organów nadzoru i transgranicznych przepływów danych (8 listopada 2001, STCE nr 181)

90. Odpowiednie zapisy Protokołu dodatkowego z 8 listopada 2001 brzmią następująco:

Artykuł 1 – Organy nadzoru

1. Każda Strona ustanowi jeden lub większą liczbę organów odpowiedzialnych za zapewnienie zgodnej ze środkami swego prawa krajowego realizacji zasad określonych w rozdziałach II i III konwencji i w niniejszym protokole.

2. a. W tym celu organy te powinny posiadać, w szczególności, uprawnienia dochodzeniowe i interwencyjne, jak również prawo do angażowania się w postępowania prawne lub informowania właściwych organów sądowych o naruszeniach przepisów prawa krajowego, realizując zasady określone w artykule 1 ustęp 1 niniejszego protokołu.

b. Każdy organ nadzoru rozpatruje skargi wnoszone przez jakąkolwiek osobę dotyczące ochrony jej praw i podstawowych wolności w związku z przetwarzaniem danych osobowych, w zakresie swej kompetencji.

3. Organy nadzoru wykonują swe funkcje całkowicie niezależnie.

4. Od decyzji organu nadzoru, która daje podstawy do zaskarżenia, przysługuje odwołanie do sądu.

(...)

3. Zalecenie Komitetu Ministrów dla państw członkowskich o ochronie danych osobowych w sferze usług telekomunikacyjnych ze szczególnym uwzględnieniem usług telefonicznych

91. Rekomendacja R (95) 4 Komitetu Ministrów, przyjęta w dniu 7 lutego 1995, stwierdza w stosownych fragmentach, co następuje:

2.4. Władze publiczne nie mogą ingerować w treść komunikacji, w tym korzystać ze podsłuchów lub innych środków monitorowania lub przechwytywania komunikacji, chyba że taka ingerencja jest przewidziana przez prawo i stanowi niezbędny środek w demokratycznym społeczeństwie:

a. ochrony Państwa, bezpieczeństwa publicznego, interesów walutowych państwa lub zwalczania przestępczości;

b. ochrony podmiotu danych oraz praw i wolności innych osób.

2.5. W przypadku, gdy władze publiczne ingerują w treść komunikacji, prawo krajowe powinno regulować kwestię:

a. wykonywania praw dostępu i korygowania danych przez osobę, której dane dotyczą;

b. warunków, na jakich właściwe organy publiczne będą uprawnione do odmowy udzielenia informacji zainteresowanej osobie lub do odroczenia udzielenia takich informacji;

c. przechowywania lub niszczenia takich danych.

W przypadku gdy operator sieci lub dostawca usług otrzymuje od organu publicznego zlecenie przeprowadzenia ingerencji, zgromadzone dane powinny być ujawniane wyłącznie organowi wyznaczonemu w zezwoleniu na taką ingerencję”.

4. Sprawozdanie Europejskiej Komisji na rzecz Demokracji przez Prawo („Komisji Weneckiej”) w sprawie ustawy z 15 stycznia 2016 o zmianie ustawy o Policji oraz niektórych innych ustaw

92. Odpowiednie fragmenty opinii na temat projektu ustawy z 15 stycznia 2016 o zmianie ustawy o Policji oraz niektórych innych ustaw, przyjętej przez Komisję Wenecką na 107 sesji plenarnej (Wenecja, 10–11 czerwca 2016, CDL-AD (2016)012) brzmią następująco:

II. Zakres analizy

5. Poprawki z 2016 miały na celu skodyfikowanie metod niejawnego nadzoru stosowanego przez Policję i służby wywiadowcze. Organy państwowe mogą pozyskiwać informacje na wiele sposobów: od świadków lub informatorów, poprzez przeszukania pomieszczeń, „klasyczny” nadzór (śledzenie) itp. Jednak największą uwagę i krytykę opinii publicznej przyciągnęło uprawnienie organów państwowych do pozyskiwania informacji poprzez nadzór środków komunikacji i innych urządzeń lub kanałów: komputerów, telefonów, baz danych, poczty elektronicznej, sieci społecznościowych itp. Dlatego też analiza Komisji Weneckiej koncentruje się na przepisach prawa odnoszących się do tych metod nadzoru.

6. Opinia ta uwzględnia „normalne” działania organów ścigania, tj. nadzór prowadzony w celu zwalczania przestępczości w kraju. Komisja Wenecka nie analizuje tutaj działań w zakresie nadzoru zagranicznych służb wywiadowczych, wojskowych służb kontrwywiadowczych itp. Niemniej jednak zdaje sobie sprawę, że rozróżnienie między normalnym nadzorem prowadzonym w celu egzekwowania prawa a wywiadem prowadzonym w celach bezpieczeństwa narodowego jest nieostre. Wywiad jest jednak niezwykle złożonym i delikatnym obszarem, który zasługuje na osobną analizę.

7. Poprawki z 2016 roku dotyczyły kilku ustaw związanych z działalnością Policji i służb wywiadowczych. Ostatecznie wszystkie te teksty przewidują ten sam model nadzoru (z kilkoma drobnymi wyjątkami). Komisja Wenecka koncentruje się tutaj na ustawie o Policji, która może służyć jako przykład *mutatis mutandis* dla standardów odnoszących się do innych organów”.

III. Kontekst zmian dokonanych w ustawie o Policji oraz innych tekstach

10. Zmiany miały na celu dostosowanie polskiego systemu prawnego do wyroku Trybunału Konstytucyjnego z 30 lipca 2014, sygn. akt K 23/11 (...)

11. Chcąc uniknąć próżni prawnej, Trybunał Konstytucyjny dał ustawodawcy 18 miesięcy (tj. do 7 lutego 2016) na zmianę przedmiotowych tekstów. Ponieważ jednak niezbędne zmiany nie mogły zostać wprowadzone podczas poprzedniej kadencji, nowy parlament utworzony w listopadzie 2015 miał niewiele czasu na wdrożenie

orzeczenia z 30 lipca 2014. Poprawki zostały ostatecznie przyjęte w ramach procedury przyspieszonej”.

IV. Krótki opis ustawy o Policji

12. Poniższe punkty krótko podsumowują odpowiednie przepisy znowelizowanej ustawy o Policji. Komisja Wenecka skupi się na dwóch z nich: art. 19 (dotyczącym „klasycznego” nadzoru) i art. 20c (dotyczącym gromadzenia metadanych – których znaczenie wyjaśniono w pkt 15).

13. Artykuł 19 zawiera zasady dotyczące niejawnego nadzoru (znanego w oficjalnym angielskim tłumaczeniu ustawy o Policji jako ‘operational control’) zarządzanego w ramach wstępnego dochodzenia w sprawie dotyczącej (potencjalnych) przestępstw wymienionych w ust. 1 pkt 1–8. Sprawozdawcom Komisji Weneckiej wyjaśniono w Warszawie, że nadzór niejawny przewidziany w art. 19 nie podlega formalnym zasadom gromadzenia dowodów określonym w Kodeksie postępowania karnego: oznaczałoby to, że istnieją dwa odrębne systemy prawne. Nadzór niejawny często poprzedza wszczęcie dochodzenia w celu jego uzasadnienia. Jednak nie każdy nadzór niejawny prowadzi do postępowania karnego. Z drugiej strony, informacje uzyskane w wyniku niejawnego nadzoru mogą zostać przedstawione jako dowód w postępowaniu karnym. Nadzór niejawny jest zarządzany na okres maksymalnie trzech miesięcy (ust. 8), ale może zostać przedłużony na okres do 18 miesięcy (ust. 9).

14. Ustęp 6 art. 19 definiuje nadzór niejawny jako obejmujący takie środki, jak podsłuch, nagrywanie treści rozmów telefonicznych i korespondencji za pośrednictwem sieci telekomunikacyjnych (e-maile, komunikatory itp.), a także przechwytywanie korespondencji pocztowej, nagrywanie rozmów na żywo za pomocą odpowiednich urządzeń itp. Oznacza to, że „klasyczny” nadzór niejawny przewidziany w art. 19 umożliwia Policji poznanie treści komunikacji, którą rozmówcy uważali za poufną.

15. Artykuł 20c ustawy o Policji dotyczy metadanych. Mówiąc prościej, obejmuje to wszystkie dane związane z komunikacją i telekomunikacją. Mogą one obejmować informacje o wykonanych lub odebranych połączeniach telefonicznych, wybieranych numerach, czasie trwania połączeń, położeniu geograficznym urządzeń mobilnych w danym momencie, odwiedzanych stronach internetowych, połączeniach z witrynami, parametrach osobistych, adresach e-mail itp. Dostęp do metadanych nie ujawnia treści prywatnych komunikatów (art. 20c ust. 1), przynajmniej nie w taki sam sposób, jak „tradycyjny” nadzór na mocy art. 19. Jak jednak zobaczymy poniżej, rozróżnienie między treścią a formą nie jest już tak wyraźne, a metadane mogą przekazywać istotne informacje o życiu prywatnym danej osoby. Znaczenie tego terminu jest dalej zdefiniowane w odpowiednich przepisach (prawa telekomunikacyjnego, ustawa o świadczeniu usług elektronicznych i prawa pocztowego).

16. Nadzór niejawnny na mocy art. 19 i gromadzenie metadanych na mocy art. 20c różnią się pod względem podstaw, na jakich są zarządzane, oraz procedur. Jeśli chodzi o podstawy, art. 19 zawiera wyczerpującą listę przestępstw uzasadniających nadzór. Artykuł 20c zapewnia znacznie szersze ramy prawne dla gromadzenia metadanych, które są wymagane w celu zapobiegania lub wykrywania przestępstw, ratowania życia i zdrowia ludzkiego lub wspierania operacji poszukiwawczych i ratowniczych. Zasadniczo Policja może gromadzić metadane w dowolnym celu przydatnym dla jej szeroko rozumianej misji utrzymania porządku i pokoju.

17. Pod względem proceduralnym, nadzór niejawnny podlegający art. 19 zasadniczo wymaga uprzedniej zgody sądu rejonowego (ust. 1 i 2). Jednakże w wyjątkowo pilnych przypadkach, w których jakkolwiek zwłoka mogłaby skutkować utratą informacji lub zniszczeniem bądź zaginięciem dowodów przestępstwa, Policja może rozpocząć nadzór bez uprzedniej zgody sądu, a jedynie za zgodą prokuratora. Jeśli zezwolenie nie zostanie udzielone w ciągu pięciu dni, nadzór musi zostać zawieszony, a zebrane informacje zniszczone (ust. 3).

18. Z drugiej strony, art. 20c zezwala na pozyskiwanie metadanych bez uprzedniej zgody sądu. Artykuł 20ca przewiduje jedynie system kontroli a posteriori: co sześć miesięcy Policja jest zobowiązana do przedkładania właściwemu sądowi ogólnego sprawozdania z gromadzenia metadanych (ust. 2). Wreszcie, art. 20cb zawiera zasady przetwarzania i uzyskiwania określonych danych niepodlegających jakiejkolwiek kontroli, nawet a posteriori. Ostatecznie ustawa o Policji wprowadza dwa zasadniczo różne systemy prawne: jeden dla „klasycznego” nadzoru niejawnego komunikacji, a drugi dla gromadzenia metadanych.

19. Wydaje się, że gromadzenie metadanych na podstawie art. 20c jest szeroko stosowaną techniką dochodzeniową, podczas gdy „klasyczny” nadzór niejawnny jest znacznie rzadszy. Ministerstwo Spraw Wewnętrznych informuje, że w 2015 Policja prowadziła dochodzenia w 833 361 sprawach, z których 215 561 dotyczyło przestępstw wymienionych w art. 19 ust. 1. W tej grupie niejawnny nadzór zarządzono 8000 razy (tj. w 0,9% całkowitej liczby spraw w toku i w 3,7% spraw wymienionych w art. 19 ust. 1). Prokurator odmówił nadzoru policyjnego w 178 przypadkach, a sądy w 19.

20. Jeśli chodzi o gromadzenie metadanych, organy ścigania złożyły w 2015 roku 1 497 174 wniosków, z czego 1,3 miliona dotyczyło danych telekomunikacyjnych, a 0,2 miliona danych internetowych. W tym ostatnim przypadku żądania dotyczyły w szczególności adresów stron internetowych (902 razy), a także adresów e-mail, narzędzi komunikacji internetowej, blogów i czatów (4913 razy). Szczegółowe bilingi (zawierające informacje o wybieranych numerach wraz z datą, godziną i czasem trwania połączenia) są najczęściej żądanymi informacjami (703 819 razy w 2015). Około 330 000 wniosków dotyczyło mniej wrażliwych danych (nazwa i adres użytkownika przypisanego do urządzenia komunikacyjnego). Komisja Wenecka zwraca uwagę, że Polska liczy ponad 38 milionów mieszkańców.

21. (...) Komisja Wenecka podkreśla, że zmiany z 2016 wprowadzają kilka ulepszeń do systemu. Ustawa określa na przykład obecnie środki niejawnego nadzoru (art. 19 ust. 6), obejmuje interwencje techniczne i określa maksymalny czas trwania niejawnego nadzoru w przypadku jego przedłużenia (art. 19 ust. 9); ustawa o Policji nakłada na Policję obowiązek rejestrowania operacji niejawnego nadzoru (art. 19 ust. 16a i 16b); ustanawia procedurę kontroli sądowej gromadzenia metadanych a posteriori (art. 20ca); przewiduje zniszczenie lub ograniczenia w wykorzystywaniu informacji objętych tajemnicą zawodową i uzyskanych w drodze nadzoru (ust. 15 i nast. art. 19); zawiera bardziej szczegółowy opis uprawnień służb związanych z gromadzeniem metadanych internetowych (art. 20c i nast.) oraz nakłada obowiązek niszczenia nieistotnych danych (ust. 7 art. 20c).

31. (...) Komisja Wenecka zauważa, że dane gromadzone na podstawie art. 20c ustawy mogą ujawniać relacje społeczne, nawyki, preferencje i zainteresowania danej osoby. Połączona analiza różnych rodzajów metadanych (która nie jest zabroniona przez prawo) i przetwarzanie dużej ilości informacji uzyskanych w ten sposób może stanowić jeszcze głębszą ingerencję i ujawnić intymne aspekty życia prywatnego danej osoby. Dane te, zebrane potajemnie przez organy ścigania, mogą zostać wykorzystane w postępowaniu karnym przeciwko tej samej osobie lub innym osobom. Oznaczałoby to, że polski ustawodawca przyjął bardziej wiarygodne założenie, zakładając, że gromadzenie większości rodzajów metadanych na podstawie art. 20c ustawy stanowi ingerencję w życie prywatne osoby, której dane dotyczą.
(...)”

1. Merytoryczne powody wdrożenia nadzoru na mocy artykuł 19

a. Przestępstwa, które uzasadniają nadzór niejawny i zasada proporcjonalności w tym kontekście

39. Artykuł 19 ustawy zawiera wyczerpującą listę przestępstw, które mogą stanowić podstawę niejawnego nadzoru, co wyjaśnia zakres przedmiotowy tego przepisu. Lista w ust. 1 jest jednak bardzo obszerna. Komisja Wenecka przypomina, że (...) ze względu na ingerencję, jaką stanowi, niejawny nadzór nad treścią prywatnych komunikatów jest uzasadniony tylko w przypadku poważnych przestępstw. W odniesieniu do ustawy o Policji Komisja Wenecka ma na przykład wątpliwości, czy podsłuch telefoniczny jest konieczny w niektórych przypadkach nielegalnego posiadania substancji psychotropowych (art. 19 ust. 1 pkt 5), gdy od początku jest oczywiste, że chodzi o bardzo małe ilości na własny użytek.

40. Komisja Wenecka powtarza, że niektóre środki nadzoru przewidziane w art. 19 ust. 6 stanowią nie tylko ingerencję w poufność komunikacji prywatnej, ale także ingerencję w poszanowanie domu (prawo zezwala na podsłuchiwanie biur lub lokali mieszkalnych). Ten rodzaj nadzoru musi być bardzo dobrze uzasadniony i dopuszczalny tylko w dochodzeniach dotyczących najgroźniejszych przestępstw (...)

41. Komisja Wenecka przyznaje również, że polskie władze mają szeroki margines swobody w zakresie wyboru przestępstw, które powinny znaleźć się na liście, ponieważ jest to w dużej mierze kwestia priorytetów krajowej polityki karnej.

42. Co najważniejsze, prawo powinno wyraźnie wspominać o zasadzie proporcjonalności. Na przykład art. 19 definiuje środki nadzoru jako pomocnicze narzędzie dochodzeniowe (zob. ust. 46). Zawiera również wyczerpującą listę przestępstw, które mogą stanowić podstawę nadzoru. Ale proporcjonalności nie da się sprowadzić tylko do tego. Wszystkie zaangażowane strony – zarówno Policja, jak i sądy – powinny być zobowiązane do oceny, czy waga przestępstwa (nawet jeśli jest ono wymienione w art. 19 ust. 1) i złożoność dochodzenia wymagają jakiegokolwiek formy nadzoru. Odpowiedź może być oczywista w przypadku najpoważniejszych przestępstw, ale nie wszystkie z nich automatycznie wymagałyby nadzoru (zwłaszcza jeśli wiąże się to z ingerencją w poszanowanie domu), a tekst ustawy powinien to jasno określać”.

b. Konieczność realnego uzasadnienia

43. Lista w art. 19 ust. 1 określa rodzaje przestępstw, które Policja może badać za pomocą niejawnego nadzoru. Kryterium to jest jednak czysto formalne, ponieważ opiera się na sposobie, w jaki Policja charakteryzuje konkretną sytuację wymagającą dochodzenia. Policja może jednak popełnić błąd w ocenie faktów lub celowo nadać im etykietę prawną, która wprowadza je w zakres art. 19 (...). W związku z tym, oprócz upewnienia się, że przestępstwo, w związku z którym Policja ubiega się o zezwolenie na podstawie art. 19 ust. 2, znajduje się na liście z art. 19 ust. 1, sąd powinien również wziąć pod uwagę już zebrane dowody faktyczne i na tej podstawie zdecydować, czy niejawny nadzór jest uzasadniony.

(...)

44. (...) Niemniej jednak, prawo powinno jasno określać, że w celu przeprowadzenia nadzoru, Policja i prokurator muszą mieć przynajmniej pewne dowody *prima facie* działalności przestępczej, na podstawie których sąd zdecyduje, czy zezwolić na nadzór.

c. Prawdopodobieństwo uzyskania ważnych informacji poprzez nadzór

45. Policja powinna mieć wystarczający powód, aby przypuszczać, że nadzór danej osoby lub grupy dostarczy informacji przydatnych w śledztwie (...) takie przypuszczenie musi być poparte pewnymi faktami i dowodami.

(...)

e. Wartość dowodowa informacji

47. (...) ustawa o Policji nie mówi nic o wartości dowodowej informacji uzyskanych w wyniku tajnej nadzoru, który okazał się zarządzony bez

wystarczającego uzasadnienia. Nie jest jasne, czy nagrania, obrazy itp. zebrane w ten sposób mogą być wykorzystane w postępowaniu karnym (...)

48. Nie jest jasne (...), w jakim zakresie informacje te mogą być wykorzystywane, gdy uzyskano zezwolenie, ale na niewystarczających podstawach. Komisja Wenecka wskazuje, że w większości przypadków procedura wydawania zezwoleń będzie odbywać się przy drzwiach zamkniętych, a ani opinia publiczna, ani osoba zainteresowana nie będą wiedzieć, czy sąd odpowiedzialny za wydanie decyzji należycie uwzględnił potrzebę ochrony prywatności. W takich przypadkach sąd rozpatrujący meritum sprawy powinien mieć możliwość wyłączenia dowodów uzyskanych z niejawnego nadzoru przedstawionych przez prokuraturę, jeżeli doszło do poważnego i rażącego naruszenia prawa, w interesie zwalczania nadużyć nadzoru.”

2. Merytoryczne powody gromadzenia metadanych na mocy art.

20c ustawy o Policji

a. Przestępstwa uzasadniające gromadzenie metadanych

49. Policja ma znacznie szerszą swobodę w zakresie gromadzenia metadanych, co jest dopuszczalne, jeżeli służy to zapobieganiu lub wykrywaniu przestępstw, ratowaniu życia ludzkiego lub ochronie zdrowia albo prowadzeniu działań poszukiwawczych lub ratowniczych (ust. 1 art. 20c ustawy o Policji) (...)

53. (...) Artykuł 20c ustawy o Policji (...) zezwala na gromadzenie metadanych w dochodzeniach dotyczących wszystkich przestępstw. Rozsądne jest również założenie, że gromadzenie danych dozwolone na mocy art. 20c ustawy może czasami skutkować poważniejszymi naruszeniami prywatności niż monitorowanie GPS ruchów samochodu w stosunkowo krótkim okresie czasu – na przykład w przypadku analizy metadanych związanych z treścią (takich jak rejestrowanie stron internetowych).

54. (...) Nie wydaje się, aby szerokie sformułowanie art. 20c (tj., że Policja może wykorzystywać gromadzenie metadanych w celu zapobiegania przestępstwom lub ich wykrywania) spełniało wymóg przewidywalności określony w art. 8 EKPC. Jednym ze sposobów ograniczenia potencjalnych nadużyć tej metody dochodzenia byłoby stwierdzenie, że gromadzenie metadanych jest dopuszczalne tylko w dochodzeniach dotyczących przestępstw zagrożonych określonym minimalnym wymiarem kary. Przepis ten mógłby zostać uzupełniony o krótszą listę przestępstw niepodlegających zasadzie minimalnego wymiaru kary, ale w przypadku których gromadzenie metadanych stanowi całość lub część istotnych dowodów oskarżenia, takich jak niektóre formy cyberprzestępczości. Istnieją zatem bardziej odpowiednie sposoby uniknięcia ryzyka związanego z bardzo szerokim brzmieniem przepisów. Komisja Wenecka zachęca polskiego ustawodawcę do rozważenia ograniczenia zakresu zasady określonej obecnie w art. 20c ustawy”.

b. Prawdopodobieństwo uzyskania ważnych informacji przez gromadzenie metadanych

(...)

56. Artykuł 20c nie określa żadnych kryteriów prawdopodobieństwa, które Policja musi spełnić w celu gromadzenia metadanych. Komisja Wenecka uważa, że Policja powinna mieć konkretne podstawy do oceniania:

- że popełniono przestępstwo lub że działalność przestępcza jest w toku lub w przygotowaniu;
- oraz że nadzór prawdopodobnie ujawni więcej informacji na ten temat.

Oznacza to, że Policja powinna być w stanie wyjaśnić, na podstawie faktów, w jaki sposób gromadzenie metadanych przyczyni się w dochodzeniu w sprawie danej działalności przestępczej”.

c. Pomocniczość

57. Komisja Wenecka zauważa, że w przeciwieństwie do przypadku niejawnego nadzoru przewidzianego w art. 19 ustawy, polskie prawo nie nadaje gromadzeniu metadanych dodatkowego statusu wśród metod poszukiwania informacji.

58. (...) Prawo nie wymaga, aby inne metody były wcześniej stosowane bez rezultatu lub okazały się nieprzydatne, co wzmacnia potrzebę wprowadzenia zabezpieczeń przed nadużywaniem tego instrumentu przez organy ścigania i służby bezpieczeństwa (...).

59. Prawo powinno również zawierać przepis wskazujący Policji, kiedy może użyć tej metody. (...) Policja powinna to robić tylko wtedy, gdy jest to należycie uzasadnione, nawet w przypadku najmniej wrażliwych metadanych. Istotne jest rozważenie standardu kontroli, który ma być stosowany przez sądy w celu ustalenia, czy Policja działała zgodnie z prawem i swoimi uprawnieniami. Kryterium to powinno być bardziej rygorystyczne w przypadku niejawnego monitorowania treści: Policja powinna być zobowiązana do wykazania, że uzyskanie informacji w inny sposób byłoby niemożliwe oraz że informacje, które mają zostać zebrane w ten sposób, są mają zasadnicze znaczenie. Z drugiej strony, jeśli chodzi o metadane, sąd może przyjąć, że jest to najłatwiejsza metoda uzyskania informacji w okolicznościach sprawy i że informacje te są racjonalnie istotne dla celów dochodzenia. Do polskiego ustawodawcy należy sformułowanie przepisu, który będzie różnicował kryterium prawdopodobieństwa w zależności od tego, czy chodzi o nadzór niejawny, czy gromadzenie metadanych.

d. Pojęcie metadanych w artykule 20c

60. Pozostaje pytanie o charakter informacji, które mogą być gromadzone na mocy art. 20c. Sama ustawa nie opisuje dokładnie, co należy rozumieć przez metadane, ale odnosi się do kilku innych tekstów

dotyczących telekomunikacji, Internetu i usług pocztowych (...). Do specjalistów w danych dziedzinach należy decyzja, czy użyte terminy techniczne opisują metadane z wystarczającą precyzją. (...)

61. Komisja Wenecka zaczyna od stwierdzenia, że metadane „nie stanowią przekazu telekomunikacyjnego” (Ustawa o Policji, art. 20c, ust. 1). Oznaczałoby to, że zgodnie z logiką tekstu metadane nie powinny ujawniać treści komunikacji w ścisłym tego słowa znaczeniu. Jednak podczas dyskusji w Warszawie sprawozdawcy otrzymali sprzeczne odpowiedzi na pytanie, czy zgodnie z polskim prawem metadane obejmują informacje odnoszące się do treści: rejestrowanie przeglądania stron internetowych, pliki cookie, treść wyszukiwania, nagłówki wiadomości e-mail itp. Komisja Wenecka uważa, że prawo powinno albo ustanowić związek między tego rodzaju metadanymi a treścią komunikacji, do której dostęp reguluje art. 19, albo wyraźnie wyłączyć je z metadanych. Ważne jest, aby dokonać tego rozróżnienia w celu określenia stopnia rygorystyki gwarancji proceduralnych i zasad materialnych mających zastosowanie do metadanych związanych z treścią komunikacji.

62. Po drugie, art. 180c ust. 2 ustawy Prawo telekomunikacyjne nakazuje właściwym ministrom, w tym ministrowi spraw wewnętrznych, określenie w drodze rozporządzenia szczegółowego wykazu danych, o których mowa w art. 180c ust. 1, które Policja może gromadzić na podstawie art. 20c. Bardzo ważne jest zapewnienie, żeby uprawnienie do regulowania tego obszaru w drodze rozporządzenia nie doprowadziło do niekontrolowanego rozszerzenia koncepcji metadanych. (...)

63. Po trzecie, art. 20c odsyła również do art. 180d ustawy Prawo telekomunikacyjne, który z kolei odsyła do art. 161 ust. 1 tej samej ustawy. Ten ostatni stanowi, że dostawca usług teleinformatycznych oferowanych publicznie może, za zgodą użytkownika w przypadku osoby fizycznej, przetwarzać inne dane (...) użytkownika związane ze świadczoną na jego rzecz usługą. Sformułowanie to wydaje się sugerować, że metadane mogą obejmować wszystkie informacje, które abonent powszechnej usługi ICT zgodził się udostępnić swojemu dostawcy usług. Wiemy jednak, że niewielu użytkowników czyta wszystkie klauzule umowy dostawy określające informacje, które ‘dobrowolnie’ udostępniają dostawcy w celu skorzystania z usługi. W połączeniu z art. 20c ustawy, przepis ten może zatem prowadzić do praktycznie niekontrolowanego rozszerzenia kategorii metadanych, które dostawcy usług ICT, a ostatecznie rząd, mogą gromadzić. Podejście to nie jest również zgodne z zasadą swobodnej dostępności danych, która jest integralną częścią prywatności (...).

(...)

65. W związku z tym Komisja Wenecka zaleca, aby polski ustawodawca zweryfikował, w razie potrzeby przy wsparciu specjalistów ICT i ekspertów prawnych w danych dziedzinach, czy opis metadanych w przepisach wystarczająco określa kategorie informacji, na których gromadzenie zezwala art. 20c. Szczególną uwagę należy zwrócić na dane

dotyczące treści komunikacji. W tym względzie Komisja Wenecka zaleca unikanie otwartych formuł lub tych, które odnoszą się do zasad określonych przez władzę wykonawczą lub do polityk danych dostawców usług ICT”.

C. Osoby poddane nadzorowi a gromadzenie metadanych

1. Liczne grupy

(...)

69. Jeśli chodzi o gromadzenie metadanych (art. 20c), (...) wydaje się, że w prawie nie ma nic, co uniemożliwiłoby Policji gromadzenie metadanych bez ukierunkowania (...)

70. (...) Zdaniem Komisji Weneckiej nadzór tego rodzaju jest dopuszczalny bez nakazu sądowego, jeśli prawo zawiera wystarczające gwarancje ochrony przed masowym przechwytywaniem dużych ilości komunikatów. Aby zmniejszyć to ryzyko, prawo powinno opisywać sytuacje, w których szeroko ukierunkowany nadzór jest dozwolony, oraz określać kategorie osób, których komunikacja może być monitorowana. Wymogi dotyczące zatwierdzania tego rodzaju nadzoru powinny być rygorystyczne (na przykład dochodzenia w sprawie konkretnych poważnych przestępstw, które zostały już popełnione). W wyjątkowych przypadkach możliwe jest zapobieganie konkretnym przyszłym zagrożeniom, takim jak zagrożenia terrorystyczne.

71. Jeśli zezwolenie zostanie wydane, ważne jest, aby kontrole były bardzo solidne. Należy wprowadzić skuteczny system nadzorowania tych środków i powierzyć go niezależnemu organowi (lub organom) spoza Policji. Organ ten powinien mieć dostęp do dokumentów uzasadniających monitorowanie oraz do jego wyników. W szczególności powinien on mieć za zadanie zapewnienie, że szeroko ukierunkowany nadzór jest odpowiednio proporcjonalny do potrzeb konkretnego dochodzenia, bez dyskryminujących motywów (nie może być skierowany do grup ludności często podejrzewanych o popełnienie pewnych przestępstw), że nigdy nie jest wykorzystywany do celów wykraczających poza zakres kompetencji Policji lub organów ścigania, a wszystkie informacje, które nie są wymagane do danego dochodzenia, są systematycznie niszczone.”

2. Niepodejrzane osoby

72. Prawo nie precyzuje dokładnie, kto może podlegać ‘klasycznemu’ niejawnemu nadzorowi lub gromadzeniu metadanych. Może to być, jak się zdaje, dowolna osoba lub grupa (przyjaciele, krewni itp. osoby będącej celem nadzoru), o ile jest prawdopodobne, że w ten sposób można uzyskać informacje, które umożliwią osiągnięcie celów określonych w art. 29 w odniesieniu do nadzoru i art. 20c w odniesieniu do gromadzenia danych.

73. Komisja Wenecka uważa, że zasada przewidywalności wymaga, aby prawo bardziej precyzyjnie określało charakter zaangażowania danych

osób lub grup w bezprawną działalność będącą przedmiotem dochodzenia. Chodzi oczywiście przede wszystkim osoby, które są bezpośrednio podejrzane. Ale prawo może również stanowić, że inne osoby mające kontakt z podejrzanym mogą, w niektórych przypadkach, podlegać nadzorowi. (...) Bardzo ważne jest, aby prawo opisywało sytuacje, w których osoby, których nie można racjonalnie uznać za bezpośrednio związane z działalnością przestępczą, mogą być celem nadzoru. Mogłoby na przykład dopuszczać tego typu środki tylko w przypadku szczególnie poważnych przestępstw (terroryzm, handel narkotykami na dużą skalę, rozprzestrzenianie broni masowego rażenia itp.) i wymagać większego uzasadnienia (większe prawdopodobieństwo uzyskania istotnych informacji w ten sposób) oraz bardziej rygorystycznych gwarancji proceduralnych (takich jak zaangażowanie ‘advokata prywatności’).

74. Podczas wizyty w Warszawie sprawozdawcy dowiedzieli się, że Kodeks postępowania karnego został znowelizowany w kwietniu 2016, a art. 19 ust. 15a-15e ustawy o Policji został uchylony. Poprawki te dałyby prokuratorowi swobodę decydowania o tym, czy informacje uzyskane przypadkowo na temat osoby nieobjętej nadzorem mogą zostać wykorzystane w postępowaniu karnym przeciwko tej osobie. Komisja Wenecka uważa, że wykorzystanie uzyskanych w ten sposób informacji o osobie trzeciej jako dowodu obciążającego powinno być dopuszczalne tylko w wyjątkowych przypadkach i tylko na mocy nakazu sądowego. Nie powinno natomiast raczej być dopuszczane w przypadku ścigania za stosunkowo drobne przestępstwa. Komisja Wenecka uważa również, że prawo musi jasno określać przypadki, w których takie informacje nie mogą być wykorzystane jako dowód – na przykład, jeśli przypadkowo przechwycone i nagrane rozmowy są objęte tajemnicą zawodową.”

3. Prawnicy, księża i inne osoby korzystające z wszystkim osoby ochrony tajemnicy zawodowej

(...)

77. Komisja Wenecka zidentyfikowała dwa główne niedociągnięcia w przepisach regulujących nadzór komunikacji objętej tajemnicą zawodową. Pierwsza z nich dotyczy poufności komunikacji między adwokatami oraz ich klientami. Prawo przewiduje, co należy zrobić z informacjami objętymi tajemnicą zawodową, które zostały już uzyskane w wyniku niejawnego nadzoru, ale nie wydaje się, aby zakazywało nadzoru nad komunikacją adwokatów per se. Nic nie stoi na przeszkodzie, aby Policja potajemnie podsłuchiwała rozmowy między adwokatem a jego klientem. Jest to nie do przyjęcia dla Komisji Weneckiej z powodów wyjaśnionych poniżej.

78. Zakaz wykorzystywania jako dowodów przeciwko podejrzanemu w postępowaniu karnym informacji uzyskanych z naruszeniem tajemnicy zawodowej oraz obowiązek ich zniszczenia (art. 15f) nie są wystarczające. Podsłuchując rozmowy między adwokatem a jego klientem, Policja może uzyskać ważne informacje, które doprowadzą ją do innych obciążających dowodów, które może ona następnie

przedstawić w postępowaniu karnym. Mimo że w polskiej procedurze karnej dowody tego typu, jako uzyskane w nieuprawniony sposób, nie są dopuszczalne, podsłuchiwanie rozmów między adwokatem a jego klientem daje Policji przewagę taktyczną i podważa zaufanie, jakie powinno istnieć między obrońcą a oskarżonym.

79. Według Komisji Weneckiej prawo powinno rozróżniać celowe naruszenia tajemnicy (które powinno być zasadniczo zabronione) i przypadkowe jej naruszenia. W pewnych oczywistych sytuacjach Policja powinna założyć, że rozmowa jest objęta tajemnicą zawodową (rozmowy między adwokatem a jego klientem w więzieniu lub na sali sądowej, konsultacje telefoniczne itp.) Podsłuchiwanie tej komunikacji powinno być zasadniczo zabronione (...)

80. Powyższe domniemanie nie ma charakteru absolutnego. (...) Odstępstwo jest jednak możliwe tylko w wyjątkowych przypadkach, na przykład jeśli istnieją wiarygodne przesłanki, że adwokat jest osobiście i świadomie powiązany ze szczególnie poważnym przestępstwem, a podsłuchiwanie jego rozmów z klientem jest jedyną możliwą metodą dochodzenia w dalszym toku śledztwa. Odstępstwu temu powinny towarzyszyć wzmocnione gwarancje proceduralne (np. podsłuch zostanie powierzony niezależnemu sędziemu, który nie będzie miał związku z dochodzeniem i będzie zobowiązany do zachowania w tajemnicy nieistotnych informacji, które uzyska w ten sposób).

81. Druga luka dotyczy przechwytywania komunikacji od przedstawicieli innych grup zawodowych, którzy również są zobowiązani do zachowania tajemnicy w komunikacji z klientami (takich jak lekarze i mediatorzy). Komisja Wenecka zauważa, że podobnie jak w przypadku adwokatów i księży, w polskim prawie nie ma nic, co uniemożliwiłoby Policji podsłuchiwanie ich rozmów, nawet jeśli nagranie nie może być następnie wykorzystane jako dowód. Ustęp 15h artykułu 19 wymaga również, aby sąd dopuścił te nagrania jako dowód, 'jeśli jest to niezbędne z punktu widzenia systemu sądowego' i jeśli nie było innych środków ustalenia faktów.

82. Druga część wymogu pomocniczości jest rozsądna; ale pierwsza część ('konieczność' dla systemu sądowego) jest problematyczna. Każda informacja, która rzuca światło na sprawę, może być uznana za 'niezbędną z punktu widzenia systemu sądowego'. Jeśli użyteczność jest jedynym kryterium dopuszczalności przechwyconej rozmowy jako dowodu, tajemnica zawodowa traci wszelkie znaczenie.

(...)

84. Komisja Wenecka uważa, że oprócz zapobiegania ukierunkowanemu przechwytywaniu komunikacji objętej tajemnicą zawodową, prawo powinno wprowadzać gwarancje wzmacniające ochronę komunikacji tego rodzaju, nawet jeśli została ona przechwycona przypadkowo (...)

85. (...) Komisja Wenecka zaleca, aby polski ustawodawca rozważył bardziej rygorystyczne przepisy, które przy poszanowaniu

międzynarodowych standardów praw człowieka opisywałyby przypadki, w których komunikacja objęta tajemnicą zawodową może być potajemnie nagrywana, a następnie wykorzystywana jako dowód.”

D. Zabezpieczenia proceduralne

1. Czas trwania nadzoru i gromadzenia metadanych

87. Prawo zezwala na wdrożenie nadzoru na okres nieprzekraczający trzech miesięcy (art. 19 ust. 8); możliwe jest przedłużenie, z zastrzeżeniem nakazu sądowego złożonego przez odpowiednie służby za pisemną zgodą prokuratora, na kolejny okres do trzech miesięcy, jeśli pierwotne powody wdrożenia nadzoru są nadal aktualne. W należycie uzasadnionych przypadkach (jeżeli nowe fakty powodują konieczność zapobieżenia lub wykrycia działalności przestępczej lub znalezienia sprawców i uzyskania dowodów) nadzór może zostać przedłużony przez sąd wyższej instancji na kilka kolejnych okresów określonych przez ten sąd, łącznie na okres do 12 miesięcy (art. 19 ust. 9). Nadzór nie powinien trwać dłużej niż łącznie 18 miesięcy.

88. Komisja Wenecka zauważa, że maksymalny okres nadzoru przewidziany w ustawie jest sam w sobie dość długi. Jednak najbardziej wrażliwym punktem jest możliwość gromadzenia metadanych przez czas nieokreślony (art. 20ca). Prawo nie mówi nic o ilości danych historycznych, które Policja może uzyskać od dostawców usług ICT, ale zazwyczaj praktycznym ograniczeniem będzie tu 12-miesięczny okres ich przechowywania. Prawo nie określa również, jak długo Policja może przechwytywać strumień metadanych na żywo. Zasada proporcjonalności wymagałaby sprecyzowania tej kwestii. Niemniej jednak, Komisja Wenecka przyznaje, że okres przechowywania danych historycznych oraz okresy ciągłego przechwytywania wymiany metadanych (szczególnie w kontekście nadzoru strategicznego) mogą być stosunkowo długie.”

2. Uprzednia i wsteczna kontrola sądowa, systemy rozpatrywania skarg i kontrola przez niezależny organ

(...)

a. Autoryzacja i kontrola nadzoru wprowadzonego na mocy artykuł 19

i. Autoryzacja

91. Artykuł 19 wymaga uprzedniej zgody sądu rejonowego na nadzór. Wyjątkowo, w bardzo pilnych przypadkach, Policja może prowadzić nadzór bez takiego zezwolenia, jednak musi on zostać przerwany, jeśli zezwolenie nie zostanie uzyskane w ciągu pięciu dni, a wszystkie zebrane informacje muszą zostać zniszczone (ust. 3).

92. (...) pożądane byłoby rozszerzenie wymogu uprzedniego zezwolenia sądowego na gromadzenie metadanych związanych z treścią, które mają bardzo podobny charakter do przechwytywania komunikacji objętego art. 19 (...).

93. (...) w Polsce odstępstwo [przewidziane w art. 19 ust. 3 dla przypadków niecierpiących zwłoki] nie jest uzasadnione powagą lub charakterem przestępstwa, a jedynie ryzykiem utraty dowodów. Nie jest również jasne, co się stanie, jeśli Policja zawiesi ‘pilne’ przechwytywanie przed upływem pięciodniowego okresu; przepis ten, interpretowany elastycznie, pozwoliłby Policji na przeprowadzanie przechwytywania o stosunkowo krótkim czasie trwania bez kontroli sądowej. (...)

95. Po drugie, nie występuje postępowanie kontradiktoryjne. Zgodnie z prawem sąd rozpatruje wniosek Policji ex parte, bez udziału osoby, której dotyczy nadzór. (...) Tymczasem bez kontradiktoryjnej konfrontacji sędziego będzie mniej krytyczny wobec stanowiska Policji. Ponadto ryzyko odwołania istnieje tylko, jeśli sędzia odrzuci wniosek, ale nie, jeśli go zaakceptuje i zarządzi nadzór. W takich warunkach uprzednia zgoda sądu na nadzór może stać się zwykłą formalnością.

96. Prawo słusznie angażuje prokuratora w proces wydawania zgody na nadzór. Biorąc jednak pod uwagę bliskie powiązania między prokuratorem a Policją w polskim systemie, nie wydaje się, aby stanowiło to wystarczającą gwarancję proceduralną.

97. Aby zwiększyć skuteczność uprzedniej kontroli sądowej, kontrola ex parte powinna zostać uzupełniona poprzez zaangażowanie w postępowanie ‘adwokata prywatności’: niezależnego prawnika posiadającego niezbędne umiejętności techniczne i poświadczenie bezpieczeństwa, który nie jest instytucjonalnie związany ani z Policją, ani z prokuraturą. Jego zadaniem byłaby obrona interesów osoby, której dotyczy nadzór.

ii. Kontrola wsteczna

98. (...) Informacje uzyskane w wyniku nadzoru mogą niekiedy zostać wykorzystane jako dowód w postępowaniu karnym, w którym to przypadku rozpatrzenie sprawy co do istoty dałoby oskarżonemu, przynajmniej teoretycznie, możliwość zakwestionowania legalności nadzoru. (...)

100. (...) W Polsce informacje dotyczące ‘kontroli operacyjnej’ są na ogół utajnione. Istnieje zatem ryzyko, że sąd weryfikujący nakaz nadzoru w postępowaniu co do istoty sprawy odmówi ujawnienia obronie informacji dotyczących zezwolenia na podsłuch. Wykluczenie tych informacji z kontradiktoryjnego badania może znacząco zaszkodzić obronie w stosunku do oskarżenia, a zatem być niezgodne z wymogiem rzetelnego procesu.

101. (...) takie odwołanie byłoby możliwe tylko w bardzo niewielkim odsetku przypadków i tylko wtedy, gdy istnienie nadzoru zostało wspomniane w postępowaniu karnym. W zdecydowanej większości przypadków nadzór pozostałby ‘niejawny’.

102. W takich przypadkach prawo mogłoby uprawniać osobę objętą nadzorem do złożenia skargi z mocą wsteczną. Jednakże, aby skorzystać z tego prawa, musi ona posiadać wiedzę na temat nadzoru. (...) Komisja Wenecka zauważa, że prawo nie wydaje się zawierać żadnego wymogu powiadamiania osoby, której nadzór dotyczy, nawet po upływie określonego czasu. 103. Komisja Wenecka rozumie, że powiadomienie może narazić na szwank poufne metody lub bieżące operacje. (...) Niemniej jednak ważne jest, żeby prawo nakładało na zainteresowane służby ogólny obowiązek powiadamiania o nadzorze po fakcie, z zastrzeżeniem odstępstw. Gdy dana osoba dowiaduje się, że była inwigilowana, procedura *ex parte* może zostać uzupełniona o w pełni kontryktoryjną procedurę, w której sąd bada *de novo* legalność nadzoru. Istniałaby również możliwość stworzenia stałego mechanizmu pozasądowego, do którego mogłyby odwoływać się osoby zaniepokojone możliwym nadzorem.

104. Pożądane byłoby również wyraźne upoważnienie sędziego, który wydał zezwolenie na nadzór, do regularnego przeglądu informacji uzyskanych przez Policję w ten sposób. Umożliwiłoby mu to sprawdzenie, czy Policja nie przekracza upoważnienia, które początkowo sędzia podpisał na mocy art. 19 ust. 1, a także lepsze zrozumienie przydatności tego rodzaju środka oraz ingerencji, jaką stanowi. Wydaje się, że prawo zezwala sędziemu jedynie na żądanie informacji uzyskanych w wyniku nadzoru w przypadku przedłużenia nakazu podsłuchu lub w przypadku wstecznego zezwolenia na ‘pilny’ nadzór przeprowadzony bez uprzedniej zgody (art. 19 ust. 3, 9 i 10).

105. Innym rozwiązaniem byłoby ustanowienie systemu kontroli wstecznej przez niezależny organ działający z własnej inicjatywy. Komisja Wenecka zauważa, że art. 19 ustawy nakłada na Ministerstwo Spraw Wewnętrznych obowiązek przedkładania Sejmowi i Senatowi rocznego sprawozdania na temat nadzoru prowadzonego przez Policję. Artykuł 19 stanowi, że Ministerstwo musi jedynie przedstawić ogólny przegląd działań tego typu, bez uzasadniania potrzeby samych operacji. System ten nie może zatem zastąpić monitorowania konkretnych operacji nadzoru przez niezależny organ, który jest zaznajomiony z praktykami nadzoru i przechwytywania i nie jest instytucjonalnie związany z Policją lub zbyt blisko związany z władzą wykonawczą i organami ścigania lub służbami wywiadowczymi.

106. Komisja Wenecka podkreśla, że ten niezależny organ powinien być uprawniony do monitorowania wszystkich aspektów operacji (z zastrzeżeniem rozsądnej swobody operacyjnej ze strony zainteresowanych służb), do zapoznawania się ze wszystkimi informacjami (nawet niejawnymi) oraz do podejmowania wszelkich działań regresowych właściwych dla danej sprawy.

107. Komisja Wenecka podkreśla, że zezwolenie sądowe na nadzór przewidziane obecnie w art. 19 jest sercem systemu gwarantującego poszanowanie prywatności i innych praw podstawowych osób, których nadzór dotyczy. Powinien on jednak zostać uzupełniony o inne

gwarancje proceduralne, w szczególności możliwość weryfikacji legalności i konieczności nadzoru w trakcie późniejszego postępowania karnego lub złożenia skargi i wystąpienia o kontrolę sądową, jeśli nadzór nie doprowadził do wszczęcia postępowania karnego. Niezależny organ nadzorczy może interweniować, gdy nie toczy się postępowanie karne i gdy nie jest możliwe uruchomienie mechanizmu składania skarg, ponieważ osoba będąca celem nadzoru nie została powiadomiona, z ważnych powodów, o nadzorze. Niezależny organ kontrolny powinien być uprawniony do badania takich przypadków oraz przedstawiania zaleceń i sprawozdań. Nie jest jednak konieczne, aby działał on jako sąd odwoławczy w odniesieniu do sądu, od którego pochodziło pierwotne zezwolenie na nadzór.

108. Komisja Wenecka zdaje sobie sprawę, że stworzenie zupełnie nowego organu w Polsce i określenie jego uprawnień w stosunku do uprawnień Policji, prokuratury i sądów będzie wymagało czasu. Biorąc pod uwagę, że polski ustawodawca musiał działać szybko, nie jest zaskakujące, że organ tego typu nie został utworzony do grudnia 2015. Jednak obecna konstrukcja systemu przechwytywania metadanych przewidzianego w art. 20c (zob. pkt 110 i nast.) oraz słabość ogólnego nadzoru nad najbardziej inwazyjnymi formami niejawnego nadzoru (art. 19) wymagałyby utworzenia takiego organu.

109. (...) zezwolenie sądowe wymagane na mocy art. 19 jest bardzo użytecznym zabezpieczeniem proceduralnym, ale samo w sobie nie wystarcza do zagwarantowania przejrzystości działań Policji w zakresie niejawnego nadzoru (lub innych organów ścigania, które również mogą być zaangażowane). Polskie władze mają swobodę kształtowania modelu gwarantującego skuteczne monitorowanie operacji nadzoru, pod warunkiem, że będzie on oparty na niezależnym organie (lub organach) prowadzącym skuteczne monitorowanie określonych operacji oraz że będzie dysponował instrumentami prawnymi niezbędnymi do wykrywania i zwalczania nadużyć. Osoby objęte nadzorem powinny być następnie powiadamiane, aby mogły uczestniczyć w przeglądzie; jeśli nie jest to możliwe, inne mechanizmy powinny umożliwić zbadanie sprawy z perspektywy ochrony prywatności osób objętych nadzorem lub umożliwić przeprowadzenie skutecznego przeglądu legalności i zasadności tych środków.

**b. Zatwierdzanie i kontrola gromadzenia metadanych
przewidziane w artykule 20ca i.
Zatwierdzanie**

110. Ustawa nie uzależnia nadzoru nad metadanymi przewidzianego w art. 20c od zatwierdzenia sądowego: w logice polskiego prawa gromadzenie metadanych jest uważane za mniejszą ingerencję, a zatem nie wymaga tak rygorystycznych gwarancji proceduralnych, jak 'klasyczny' nadzór z art. 19. Komisja Wenecka przyznaje, że chociaż byłoby pożądaną, aby każde gromadzenie metadanych było wcześniej zatwierdzane przez sądy, procedura ta może czasami okazać się zbyt uciążliwa dla Policji. (...) Wystarczające byłoby powiadomienie sądu (lub niezależnego organu nadzorczego [...]) w późniejszym terminie

111. Metadane związane z treścią stanowią główny wyjątek od tej zasady: Komisja Wenecka zaleca, aby polskie władze rozważyły objęcie ich zakresem art. 19 (jeśli jeszcze tego nie zrobiły), z zastrzeżeniem wszystkich zabezpieczeń proceduralnych (w szczególności uprzedniego zatwierdzenia przez sąd). Możliwe byłoby również uzależnienie gromadzenia metadanych na dużą skalę od uprzedniego zatwierdzenia (jeśli celem jest cały obszar geograficzny w danym czasie). Wsteczna kontrola określonych operacji powinna jednak stanowić wystarczającą gwarancję przed nadużyciami w przypadku większości typów metadanych.”

ii. Kontrola wsteczna

112. Artykuł 20ca nakłada na Policję obowiązek przedkładania właściwemu sądowi okręgowemu półrocznego sprawozdania zawierającego ogólne informacje na temat monitorowania metadanych w minionym okresie.

113. Komisja Wenecka uważa, że obowiązek składania sprawozdań nie jest wystarczający do zapewnienia przejrzystości działań Policji w zakresie gromadzenia metadanych. Dokumenty te zawierają jedynie podsumowanie informacji, ale nie zawierają szczegółów na temat każdej operacji. Trudno sobie wyobrazić, jakie wnioski mógłby wyciągnąć sędzia z takiej lektury. Co prawda sędzia może z własnej inicjatywy poprosić Policję o informacje, które uzasadniały przekazanie metadanych Policji (art. 20ca ust. 3); nie jest jednak jasne, co miałyby go skłaniać do przeprowadzenia zindywidualizowanej analizy tego typu. W mało prawdopodobnym przypadku, gdy aktywnie bada informacje dotyczące sprawy i wykrywa nieprawidłowości, jego ustalenia mogą prowadzić do postępowania karnego lub dyscyplinarnego przeciwko danym funkcjonariuszom Policji.

114. Powstaje zatem pytanie, czy kontrola wsteczna powinna zostać powierzona sądowi czy niezależnemu organowi. (...)

115. Jednym z rozwiązań mogłoby być większe zaangażowanie sądów w monitorowanie operacji nadzoru metadanych, pod warunkiem, że dysponują one wystarczającymi zasobami (czas, dostęp do umiejętności technicznych, specjalne umiejętności itp.) Kwestia przechwytywania metadanych jest jednak trudna do oddzielenia od innych aspektów dochodzeń policyjnych. Sądy powszechne mogą mieć trudności z ciągłym sprawowaniem swego rodzaju funkcji nadzorczej nad Policją.

116. Lepszym rozwiązaniem byłoby wykorzystanie organów złożonych z ekspertów w celu uzupełnienia lub zastąpienia kontroli sądowej (...)

117. W każdym razie każdy system kontroli wstecznej powinien opierać się na prawdziwie niezależnym organie posiadającym niezbędne umiejętności i uprawnienia do prawidłowego monitorowania metadanych. Podobnie jak w przypadku niejawnego nadzoru (art. 19), polskie władze mają bardzo szeroką swobodę w opracowaniu systemu

wspieranego przez niezależny organ, który wymagałby od Policji przekonania niezależnego obserwatora spoza jej szeregów o potrzebie zastosowania tego środka. Prawo powinno uczynić taki organ kontrolny odpowiedzialnym za bieżące proaktywne monitorowanie wszystkich operacji i nadać mu niezbędne uprawnienia w stosunku do Policji i prokuratorów. Mogłaby również wprowadzić obowiązek kwalifikowanego powiadamiania i mechanizm składania skarg (do sądu lub niezależnego organu kontrolnego).

(...)

119. Aby uprościć zadanie Policji i odciążyć sądy, polski ustawodawca mógłby nawet wyłączyć z zakresu kontroli wstecznej zapoznanie się przez Policję z danymi dotyczącymi abonamentów. Jeśli zdecyduje się to zrobić, operacje tego typu nie będą regularnie sprawdzane przez sądy (ani żaden inny niezależny organ), ale należy wprowadzić system rejestrowania, z pewną formą weryfikacji wstecznej ważności operacji na podstawie próbek. W każdym razie, poza najmniej inwazyjnymi metadanymi, wszystkie operacje policyjne powinny podlegać skutecznej i pełnej kontroli wstecznej.}

c. Bezpośredni dostęp do metadanych

120. Art. 20c ust. 3 zezwala Policji na bezpośredni dostęp do metadanych bez udziału personelu dostawców usług ICT, pod warunkiem, że jest to przewidziane w umowie między Policją, jej dowództwem wysokiego szczebla i dostawcą. Oznacza to, że Policja może mieć bezpośredni i stały dostęp do metadanych.

122. (...) władze zapewniły sprawozdawców (...), że tylko niektórzy wyznaczeni funkcjonariusze Policji mieli bezpośredni dostęp do metadanych u dostawców usług ICT¹¹⁰ oraz że Policja rejestruje wszystkie ich połączenia. Są to minimalne gwarancje, które powinny zostać utrzymane. Tymczasem w Polsce organy ścigania mają dostęp do danych bez wiedzy operatorów telekomunikacyjnych, w nieograniczonych ilościach i po bardzo niskich kosztach (...), co znacznie zwiększa ryzyko nadużyć. Ci specjalnie wyznaczeni funkcjonariusze, choć są specjalistami, nie wydają się pełnić funkcji eliminowania nieuzasadnionych wniosków (...), ale po prostu ułatwiania (tj. działania jako kanał komunikacji). Ustęp 4 art. 20c wymaga jednak pełnej identyfikacji funkcjonariuszy Policji, którzy zapoznają się z metadanymi, co jest dobrym rozwiązaniem.

123. Komisja Wenecka zauważa, że w obecnym kształcie prawo nie powierza kontroli nad gromadzeniem metadanych niezależnemu organowi odpowiedzialnemu za weryfikację, czy Policja rozsądnie wykorzystuje swoje uprawnienia, zgodnie z dobrą praktyką dochodzeniową (...).

124. Sprawozdawcom wydaje się również, że w przypadku bezpośrednich konsultacji w czasie rzeczywistym trudne może być techniczne oddzielenie treści i metadanych. Konieczne byłoby zatem wprowadzenie do systemu modułów zapewniających wyraźne

oddzielenie treści od metadanych, a Policja miałaby dostęp tylko do tych innych.

(...)”

VII. Wnioski

(...)

133. Komisja Wenecka zaleca ulepszenie prawa poprzez wprowadzenie następujących istotnych zmian (jak również innych zaleceń przedstawionych w tekście niniejszej opinii):

- wzmocnienie zasady proporcjonalności poprzez rozszerzenie kryteriów niejawnego nadzoru (art. 19), a także dodanie nowych kryteriów gromadzenia metadanych (art. 20c), tak aby nadzór niejawny i gromadzenie metadanych były zarządzane tylko w najpoważniejszych przypadkach, zwłaszcza w przypadku procedury nadzwyczajnej (art. 19 ust. 3);

- ustawowe zakazanie nadzoru nad komunikacją a priori objętej tajemnicą adwokacką, precyzyjne określenie możliwych wyjątków od tej zasady i zrobienie tego samo w odniesieniu do innej komunikacji objętej tajemnicą zawodową;

- ograniczenie czasu trwania nadzoru metadanych, wymaganie od Policji prowadzenia rejestrów umożliwiających skuteczne kontrolę wsteczną operacji nadzoru, zwłaszcza w przypadku ‘bezpośredniego dostępu’;

- uzupełnienie systemu uprzedniego zezwolenia sądowego na tradycyjny nadzór, o którym mowa w art. 19, o inne gwarancje proceduralne (‘adwokata prywatności’, mechanizm składania skarg, system automatycznej kontroli wstecznej tych operacji przez niezależny organ itp.)

- w odniesieniu do gromadzenia metadanych (art. 20c), wprowadzenie skutecznego systemu monitorowania tego typu operacji przez niezależny organ, posiadający niezbędne uprawnienia dochodzeniowe i kompetencyjne oraz prawo do podejmowania odpowiednich kroków prawnych.

(...)”

III. UNIA EUROPEJSKA

A. Karta praw podstawowych Unii Europejskiej

93. Artykuły 7, 8 i 11 Karty mają następujące brzmienie:

Artykuł 7 – Poszanowanie życia prywatnego i rodzinnego

Każdy ma prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się.

Artykuł 8 – Ochrona danych osobowych

1. Każdy ma prawo do ochrony danych osobowych, które go dotyczą.
2. Dane te muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Każdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania.
3. Przestrzeganie tych zasad podlega kontroli niezależnego organu.

Artykuł 11 – Wolność wypowiedzi i informacji

1. Każdy ma prawo do wolności wypowiedzi. Prawo to obejmuje wolność posiadania poglądów oraz otrzymywania i przekazywania informacji i idei bez ingerencji władz publicznych i bez względu na granice państwowe.
2. Szanuje się wolność i pluralizm mediów.

B. Dyrektywy i rozporządzenia Unii Europejskiej odnoszące się do ochrony i przetwarzania danych osobowych

1. Dyrektywa 95/46/WE z 24 października 1995 w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych („dyrektywa o ochronie danych osobowych”)

94. Przez wiele lat dyrektywa o ochronie danych osobowych regulowała ochronę i przetwarzanie danych osobowych w Unii Europejskiej. Nie miał on jednak zastosowania do działań państw członkowskich związanych z bezpieczeństwem publicznym, obronnością i bezpieczeństwem narodowym, które nie wchodzą w zakres prawa wspólnotowego (art. 3 ust. 2).

2. *Dyrektywa 2002/58/WE z 12 lipca 2002 dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)*

95. Motywy 2 i 11 dyrektywy o prywatności i łączności elektronicznej stanowią, co następuje:

- 2) Niniejsza dyrektywa dąży do poszanowania fundamentalnych praw i jest zgodna z zasadami uznanymi w szczególności przez Kartę Praw Podstawowych Unii Europejskiej. W szczególności niniejsza dyrektywa zmierza do zapewnienia pełnego poszanowania praw określonych w art. 7 i 8 tej Karty.

(...)

11) Niniejsza dyrektywa, podobnie jak dyrektywa 95/46/WE, nie odnosi się do kwestii ochrony podstawowych praw i wolności związanych z działalnością, która nie jest regulowana prawem wspólnotowym. Dyrektywa nie zmienia zatem istniejącej równowagi między prawem do prywatności osoby fizycznej a możliwością Państw Członkowskich do podejmowania środków, określonych w art. 15 ust. 1 niniejszej dyrektywy, niezbędnych do ochrony bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (włączając gospodarczy dobrobyt państwa, gdy działania dotyczą zagadnień bezpieczeństwa państwa) i wykonywania prawa karnego. Wskutek tego, niniejsza dyrektywa nie wpływa na możliwości Państw Członkowskich do zgodnego z prawem przejmowania danych w łączności elektronicznej lub podejmowania innych środków, jeżeli jest to konieczne dla któregośkolwiek z tych celów i zgodne z Europejską Konwencją o Ochronie Praw Człowieka i Podstawowych Wolności, dla której wykładnię stanowi orzecznictwo Europejskiego Trybunału Praw Człowieka. Środki tego rodzaju muszą być właściwe, współmierne do zamierzonego celu i niezbędne w ramach społeczeństwa demokratycznego oraz powinny podlegać stosownym zabezpieczeniom zgodnie z Europejską Konwencją o Ochronie Praw Człowieka i Podstawowych Wolności”.

96. Odpowiednie zapisy tej dyrektywy brzmią następująco:

Artykuł 1 – Zakres i cel

1. Niniejsza dyrektywa przewiduje harmonizację przepisów krajowych wymaganych do zapewnienia równoważnego poziomu ochrony podstawowych praw i wolności, w szczególności prawa do prywatności i poufności, w odniesieniu do przetwarzania danych osobowych w sektorze łączności elektronicznej oraz w celu zapewnienia swobodnego przepływu we Wspólnocie tego typu danych oraz urządzeń i usług łączności elektronicznej.

2. Przepisy niniejszej dyrektywy dookreślają i uzupełniają dyrektywę 95/46/WE zgodnie z celami przedstawionymi w ust. 1. Ponadto zapewniają ochronę uzasadnionych interesów abonentów będących osobami prawnymi.

3. Niniejsza dyrektywa nie ma zastosowania do działalności, która wykracza poza zakres Traktatu ustanawiającego Wspólnotę Europejską, takiej jak działalność określona w tytułach V i VI Traktatu o Unii Europejskiej, ani w żadnym wypadku do działalności dotyczącej bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (włączając dobrobyt gospodarczy państwa, gdy działalność odnosi się do spraw bezpieczeństwa państwa) i działalności państwa w dziedzinie prawa karnego”.

Artykuł 15 – Stosowanie niektórych przepisów dyrektywy 95/46/WE

1. Państwa Członkowskie mogą uchwalić środki ustawodawcze w celu

ograniczenia zakresu praw i obowiązków przewidzianych w art. 5, 6, art. 8 ust. 1-4, i art. 9 tej dyrektywy, gdy takie ograniczenia stanowią środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego (i.e. bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej, jak określono w art. 13 ust. 1 dyrektywy 95/46/WE. W tym celu, Państwa Członkowskie mogą, między innymi, uchwalić środki ustawodawcze przewidujące przechowywanie danych przez określony czas uzasadnione na podstawie zasad ustanowionych w niniejszym ustępie. Wszystkie środki określone w niniejszym ustępie są zgodne z ogólnymi zasadami prawa wspólnotowego, w tym zasadami określonymi w art. 6 ust. 1 i 2 Traktatu o Unii Europejskiej”.

3. Dyrektywa 2006/24/WE w sprawie zatrzymywania danych

97. Przed wyrokiem TSUE z 8 kwietnia 2014 stwierdzającym jej nieważność (pkt 104–108 poniżej) dyrektywa w sprawie zatrzymywania danych stanowiła między innymi, co następuje:

Artykuł 1 – Przedmiot i zakres zastosowania

1. Celem niniejszej dyrektywy jest zbliżenie przepisów państw członkowskich w zakresie obowiązków dostawców ogólnie dostępnych usług łączności elektronicznej lub publicznych sieci łączności w zakresie zatrzymywania pewnych danych przez nie generowanych lub przetwarzanych, aby zapewnić dostępność przedmiotowych danych do celu dochodzenia, wykrywania i ścigania poważnych przestępstw, określonych w ustawodawstwie każdego państwa członkowskiego.

2. Niniejsza dyrektywa stosuje się do danych o ruchu i lokalizacji, dotyczących zarówno osób fizycznych, jak i prawnych, oraz do powiązanych z nimi danych niezbędnych do identyfikacji abonenta lub zarejestrowanego użytkownika. Nie odnosi się ona natomiast do treści komunikatów elektronicznych, w tym informacji uzyskiwanych przy użyciu sieci łączności elektronicznej”.

Artykuł 3 – Obowiązek zatrzymywania danych

1. Na zasadzie odstępstwa od art. 5, 6 i 9 dyrektywy 2002/58/WE, państwa członkowskie przyjmują środki w celu zagwarantowania, że dane określone w art. 5 niniejszej dyrektywy są zatrzymywane zgodnie z jej przepisami w stopniu, w jakim są generowane lub przetwarzane na ich terenie przez dostawców ogólnie dostępnych usług łączności elektronicznej lub publicznej sieci łączności w trakcie świadczenia odnośnych usług łączności.”

4. Rozporządzenie (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO)

98. RODO weszło w życie 25 maja 2018, zastępując dyrektywę o ochronie danych. Rozporządzenie to ma bezpośrednie zastosowanie w państwach członkowskich i zawiera przepisy i gwarancje dotyczące przetwarzania w Unii Europejskiej informacji umożliwiających osobistą identyfikację zainteresowanych osób. Ma ono zastosowanie do „osób fizycznych” i nie obejmuje przetwarzania danych osobowych dotyczących osób prawnych (motyw 14). Zgodnie z art. 23 ust. 1 ustawodawstwo państw członkowskich może ograniczać zakres obowiązków i praw przewidzianych w art. 12–22 i art. 34, „jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym”, między innymi, bezpieczeństwu narodowemu, bezpieczeństwu publicznemu lub zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu lub ściganiu czynów zabronionych lub wykonywaniu kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom.

99. W szczególności takie przepisy muszą przewidywać prawo osób, których dane dotyczą, do bycia poinformowanym, w stosownych przypadkach, o wspomnianym ograniczeniu, chyba że byłoby to szkodliwe dla celu ograniczenia (art. 23 ust. 2 lit. h) RODO).

100. Każda osoba, której dane dotyczą, ma prawo wnieść skargę do organu nadzorczego, jeżeli sądzi, że przetwarzanie danych osobowych jej dotyczące stanowi naruszenie RODO (art. 77 ust. 1 RODO).

101. Każda osoba, której dane dotyczą, ma również prawo, w tych samych okolicznościach, do skutecznego sądowego środka ochrony prawnej (art. 79 ust. 1 RODO).

102. Każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia RODO, ma prawo do uzyskania od administratora lub podmiotu przetwarzającego odszkodowania za poniesioną szkodę (art. 82 ust. 1 RODO). Artykuł 82 ust. 2–4 reguluje sposób, w jaki można ubiegać się o takie odszkodowanie.

5. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych („Dyrektywa Policyjna”)

103. Dyrektywa Policyjna reguluje przetwarzanie przez właściwe organy danych osobowych osób fizycznych do celów „zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom” (art. 1 ust. 1 i art. 2 ust. 1). Zgodnie z art. 63 ust. 1 transpozycji należało dokonać najpóźniej do maja 2018. W Polsce ustawa z 14 grudnia 2018 o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości dokonała wymaganej transpozycji.

C. Właściwe orzecznictwo Trybunału Sprawiedliwości Unii (TSUE)

1. Digital Rights Ireland e.a. (C-293/12 i C-594/12, EU:C:2014:238)

104. W orzeczeniu z 8 kwietnia 2014 TSUE stwierdził nieważność dyrektywy 2006/24/WE w sprawie zatrzymywania danych, która zobowiązywała dostawców publicznie dostępnych usług łączności elektronicznej lub publicznych sieci łączności do zatrzymywania wszystkich danych o ruchu i lokalizacji przez okres od sześciu miesięcy do dwóch lat, tak aby takie dane były dostępne do celów prowadzenia dochodzeń, wykrywania i ścigania poważnych przestępstw określonych przez każde państwo członkowskie w jego prawie krajowym. Trybunał orzekł, że obowiązek zatrzymania tych danych stanowi ingerencję w prawo do poszanowania życia prywatnego i komunikowania się oraz w prawo do ochrony danych osobowych gwarantowane odpowiednio w art. 7 i art. 8 Karty praw podstawowych Unii Europejskiej.

105. Uznał również, że dostęp do danych przez właściwe organy krajowe stanowił dalszą ingerencję w to podstawowe prawo i że była ona „szczególnie poważna”. Uznał też, że fakt, iż dane były przechowywane, a następnie wykorzystywane bez informowania o tym abonenta lub zarejestrowanego użytkownika, mógł wywołać w umysłach osób, których dane dotyczyły, poczucie, że ich życie prywatne było pod stałym nadzorem. Stwierdził, że ingerencja spełniała cel interesu ogólnego, a mianowicie przyczyniała się do walki z poważną przestępczością i terroryzmem, a tym samym ostatecznie do bezpieczeństwa publicznego, ale nie była zgodna z zasadą proporcjonalności.

106. Po pierwsze, dyrektywa objęła wszystkie osoby i wszystkie środki komunikacji elektronicznej, jak również wszystkie dane o ruchu, bez jakiegokolwiek rozróżnienia, ograniczenia lub wyjątku na podstawie celu zwalczania poważnej przestępczości.

107. Po drugie, dyrektywa nie określiła materialnych i proceduralnych warunków regulujących dostęp właściwych organów krajowych do danych i ich późniejsze wykorzystanie, ani nie poddała takiego dostępu uprzedniej kontroli sądu lub niezależnego organu administracyjnego, którego decyzja miałaby na celu ograniczenie dostępu do danych i ich wykorzystania do tego, co jest ściśle niezbędne do osiągnięcia zamierzonego celu.

108. Po trzecie, dyrektywa wymagała, aby wszystkie dane były zatrzymywane przez okres co najmniej sześciu miesięcy, bez dokonywania rozróżnienia między kategoriami danych na podstawie ich potencjalnej przydatności do realizacji zamierzonego celu lub według osób, których dane dotyczą. Trybunał uznał również, że dyrektywa nie zawiera gwarancji zapewniających, za pomocą środków technicznych i organizacyjnych, skuteczną ochronę przechowywanych danych przed ryzykiem niewłaściwego użycia oraz bezprawnego dostępu i wykorzystania.

2. Tele2 Sverige (C-203/15 i C-698/15, EU:C:2016:970)

109. W wyroku wydanym w 21 grudnia 2016 r. na wniosek o wydanie orzeczenia w trybie prejudycjalnym złożony przez Administracyjny Sąd Apelacyjny w Sztokholmie oraz Sąd Apelacyjny Anglii i Walii, TSUE orzekł, że przepisy krajowe przewidujące ogólne zatrzymywanie wszystkich danych o ruchu i lokalizacji do celów zwalczania przestępczości są sprzeczne z art. 15 ust. 1 dyrektywy o prywatności i łączności elektronicznej. Orzekł, że przepis ten wyklucza również ustawodawstwo zezwalające władzom na dostęp do zatrzymanych danych, jeżeli taki dostęp (a) nie był ograniczony do

wyłączonego celu zwalczania poważnej przestępczości i (b) nie podlegał uprzedniej kontroli sądu lub niezależnego organu. TSUE oparł swoje wnioski m.in. na ogólnej strukturze dyrektywy o prywatności i łączności elektronicznej, w tym na ustanowionej w niej ogólnej zasadzie poufności komunikacji, a także na ścisłym wymogu konieczności określonym w prawie UE dla wszelkich ograniczeń ochrony danych osobowych. Wreszcie, TSUE odmówił odpowiedzi na pytanie, czy ochrona przyznana przez art. 7 i 8 Karty, zgodnie z jej wykładnią, była szersza niż ta przyznana przez art. 8 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności („Konwencji”). W szczególności zauważył, że prawo Unii Europejskiej może zapewniać szerszą ochronę niż ta gwarantowana przez Konwencję oraz że art. 8 Karty dotyczy prawa (ochrony danych osobowych), które nie ma odpowiednika w Konwencji.

3. *Ministerio Fiscal* (C-207/16, EU:C:2018:788)

110. W wyroku z 2 października 2018, wydanym w następstwie wniosku o wydanie orzeczenia w trybie prejudycjalnym złożonego przez Sąd Okręgowy w Tarragonie (Hiszpania), TSUE orzekł, że dostęp do przechowywanych nazwisk i adresów przekazanych organom publicznym w celu identyfikacji właścicieli kart SIM aktywowanych za pomocą skradzionego telefonu komórkowego stanowił ingerencję, która, choć nieuzasadniona potrzebą zwalczania „poważnych” przestępstw, nie była wystarczająco poważna, aby naruszyć art. 15 ust. 1 dyrektywy o prywatności i łączności elektronicznej.

4. *Privacy International* (C 623/17, EU:C:2020:790) i *La Quadrature du Net* (C-511/18, C-512/18 oraz C 520/18; EU:C:2020:791)

111. W wyroku wydanym w 6 października 2020 (*La Quadrature du Net* i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791) na wniosek o wydanie orzeczenia w trybie prejudycjalnym złożony przez francuski organ Conseil d’Etat (Radę Stanu) i belgijski Trybunał Konstytucyjny, TSUE potwierdził wniosek zawarty w wyżej wymienionej sprawie *Tele2 Sverige*, zgodnie z którym art. 15 ust. 1 dyrektywy o d’Etat prywatności i łączności elektronicznej sprzeciwia się ogólnemu zatrzymywaniu danych o ruchu i danych o lokalizacji do celów zwalczania poważnej przestępczości, i orzekł, że przepis ten zezwala jedynie na ukierunkowane zatrzymywanie takich danych, określone na podstawie obiektywnych i niedyskryminacyjnych czynników. Z drugiej strony, art. 15 ust. 1 nie wykluczał ogólnego zatrzymywania (a) adresów IP przypisanych do źródła połączenia internetowego oraz (b) danych dotyczących tożsamości cywilnej użytkowników systemów łączności. Uznał również, że ogólne zatrzymywanie danych o ruchu i lokalizacji – przez (odnawialny) okres ograniczony do tego, co jest absolutnie konieczne – było dopuszczalne, jeśli dane państwo stanęło w obliczu rzeczywistego i poważnego, obecnego lub przewidywalnego zagrożenia dla jego bezpieczeństwa narodowego. Określa jednak, że decyzja o wymogu ogólnego zatrzymywania danych z powodu takiego zagrożenia powinna podlegać skutecznej kontroli przez sąd albo przez niezależny organ administracyjny wydający wiążącą decyzję, oraz że kontrola ta powinna również obejmować zgodność z warunkami i gwarancjami wymaganymi na mocy art. 15 ust. 1.

112. W innym wyroku z 6 października 2020 (*Privacy International*, C-

623/17, EU:C:2020:790) TSUE, orzekając w sprawie pytania prejudycjalnego skierowanego przez Investigatory Powers Tribunal (brytyjski sąd mający uprawnienia śledcze), orzekł między innymi, że art. 15 ust. 1 dyrektywy o prywatności i łączności elektronicznej stoi na przeszkodzie przepisom umożliwiającym organowi wymaganie od dostawców usług łączności, w celu ochrony bezpieczeństwa narodowego, ogólnego przekazywania danych o ruchu i lokalizacji agencjom bezpieczeństwa i wywiadu.

5. Prokuratuur (Warunki dostępu do danych dotyczących łączności elektronicznej) (C-746/18, EU:C:2021:152)

113. W orzeczeniu wydanym w 2 marca 2021 w sprawie wniosku o wydanie orzeczenia w trybie prejudycjalnym złożonego przez estoński Sąd Najwyższy, TSUE przypomniał, że art. 15 ust. 1 dyrektywy o prywatności i łączności elektronicznej zezwala na dostęp, w celu zwalczania przestępczości, do przechowywanych danych o ruchu lub lokalizacji wyłącznie w przypadku poważnych przestępstw lub poważnych zagrożeń dla bezpieczeństwa publicznego, niezależnie od długości okresu, który miał obejmować wnioskowany dostęp, oraz ilości lub charakteru danych dostępnych w tym okresie. TSUE orzekł również, że rozpatrywanie wniosków o dostęp nie może zostać powierzone prokuraturze, ponieważ jej funkcje w zakresie kierowania postępowaniami przygotowawczymi i ścigania mają wpływ na jej niezależność od stron postępowania karnego.

6. Commissioner of An Garda Síochána e.a (C-140/20, EU:C:2022:258)

114. W orzeczeniu tym, wydanym 5 kwietnia 2022 na wniosek o wydanie orzeczenia w trybie prejudycjalnym złożony przez Sąd Najwyższy Irlandii, TSUE potwierdził swoje utrwalone orzecznictwo, zgodnie z którym prawo Unii stoi na przeszkodzie krajowym środkom ustawodawczym przewidującym ogólne i niezróżnicowane zatrzymywanie danych o ruchu i danych o lokalizacji związanych z łącznością elektroniczną w celu zwalczania poważnej przestępczości. TSUE odrzucił argument, że właściwe organy krajowe powinny mieć możliwość dostępu, w celu zwalczania poważnej przestępczości, do takich danych, które były przechowywane w sposób uogólniony i masowy w celu przeciwdziałania poważnemu zagrożeniu dla bezpieczeństwa narodowego, które było rzeczywiste i obecne lub przewidywalne. Zauważył, że zgodnie z tym argumentem dostęp mógłby być uzasadniony celem o mniejszym znaczeniu niż ten, który uzasadniał zabezpieczenie, a mianowicie ochroną bezpieczeństwa narodowego, co byłoby sprzeczne z hierarchią celów interesu publicznego, w kontekście których należy oceniać proporcjonalność środka zabezpieczającego. Uznał, że zezwolenie na taki dostęp groziłoby nieskutecznością zakazu ogólnego i niezróżnicowanego zatrzymywania danych do celów zwalczania poważnej przestępczości.

7. SpaceNet i Telekom Deutschland (C-793/19 oraz C-794/19, EU:C:2022:702)

115. W wyroku wydanym 20 września 2022 w sprawie wniosku o wydanie orzeczenia w trybie prejudycjalnym złożonego przez niemiecki Federalny

Sąd Administracyjny, TSUE potwierdził swoje orzecznictwo (wyroki w sprawach *La Quadrature du Net* i *Commissioner of An Garda Síochána*, pkt 111 i 114 powyżej) sprzeciwiające się powszechnemu i masowemu zatrzymywaniu danych w celu zwalczania poważnej przestępczości lub zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego, danych o ruchu i lokalizacji, uznając, że przedmiotowe przepisy krajowe nie są zgodne z prawem UE, pomimo istnienia przewidzianych w nich zabezpieczeń i krótszego okresu zatrzymywania (od 10 do 4 tygodni) niż w poprzednich sprawach. TSUE orzekł również, że zatrzymanie tych danych i dostęp do nich stanowią odrębne ingerencje w prawa podstawowe osób, których dane dotyczą, wymagające odrębnego uzasadnienia, a zatem przepisy krajowe zapewniające pełną zgodność z warunkami wynikającymi z orzecznictwa w sprawie dostępu do zatrzymanych danych nie mogą, ze względu na swój charakter, być w stanie ograniczyć ani nawet zaradzić poważnej ingerencji w prawa osób, których dane dotyczą, wynikającej z ogólnego zatrzymania tych danych.

8. *VD i SR (C-339/20 i C-397/20, EU:C:2022:703)*

116. W wyroku wydanym w 20 września 2022 na wniosek o wydanie orzeczenia w trybie prejudycjalnym złożony przez francuski sąd apelacyjny, TSUE orzekł, że dyrektywa w sprawie nadużyć na rynku i rozporządzenie w sprawie nadużyć na rynku w związku z dyrektywą o prywatności i łączności elektronicznej oraz w świetle Karty praw podstawowych Unii Europejskiej, nie zezwalały na ogólne i masowe zatrzymywanie danych dotyczących komunikacji przez operatorów usług łączności elektronicznej przez okres jednego roku od dnia, w którym zostały one zarejestrowane, do celów zwalczania przestępstw nadużyć na rynku.

9. *HYA i inni (Motywacja zezwoleń na podsłuchy telefoniczne) (C-349/21, EU:C:2023:102)*

117. W orzeczeniu wydanym w 16 lutego 2023 w sprawie wniosku o wydanie orzeczenia w trybie prejudycjalnym złożonego przez bułgarski wyspecjalizowany sąd karny, TSUE stwierdził, że decyzja zezwalająca na podsłuch telefoniczny może nie zawierać zindywidualizowanych uzasadnień. Stwierdził, że taka decyzja nie narusza obowiązku uzasadnienia, ponieważ opiera się na szczegółowym i dokładnym wniosku właściwego organu karnego, a powody wydania zezwolenia można łatwo i jednoznacznie wywnioskować z odniesienia między wnioskiem a zezwoleniem.

IV. ELEMENTY PRAWNOPORÓWNAWCZE

118. Trybunał przeprowadził analizę porównawczą prawa krajowego i praktyki trzydziestu pięciu państw będących stronami Konwencji⁷ w kwestii gwarancji przyznanych osobom prywatnym wobec organów prowadzących

⁷ Dotyczy to następujących krajów: Albania, Armenia, Azerbejdżan, Belgia, Bośnia i Hercegowina, Chorwacja, Czechy, Estonia, Francja, Gruzja, Grecja, Hiszpania, Holandia, Irlandia, Islandia, Liechtenstein, Litwa, Luksemburg, Łotwa, Mołdawia, Niemcy, Norwegia, Portugalia, Rumunia, San Marino, Serbia, Słowacja, Słowenia, Szwajcaria, Szwecja, Węgry, Wielka Brytania i Włochy

nadzór niejawny.

119. ⁸Informacje otrzymane od państw objętych badaniem pokazują, że w większości z nich (trzydzieści jeden państw) nadzór prowadzony w celu zwalczania przestępczości podlega uprzedniej kontroli organu sądowego. Ponadto wydaje się, że piętnaście z ww. państw wprowadziło, oprócz kontroli nadzoru a priori, także kontrolę a posteriori. Jest ona realizowana przez sądy (dziewięć państw)⁹, organy wykonawcze (jedno państwo)¹⁰, organy parlamentarne (dwa państwa)¹¹ lub organy hybrydowe (trzy państwa)¹². Ponadto niektóre z badanych państw wprowadziły przepisy dotyczące sytuacji nadzwyczajnych, w których prokurator może zezwolić na nadzór, ale musi on zostać przerwany, jeśli w krótkim czasie nie zostanie uzyskana zgoda sądu. W odniesieniu do nadzoru prowadzonego przez służby specjalne w celu zapobiegania niektórym poważnym przestępstwom lub ochrony bezpieczeństwa lub podstawowych interesów państwa, odpowiednie ustawodawstwo osiemnastu z tych państw¹³ uzależnia wprowadzenie przedmiotowego nadzoru od uprzedniego zezwolenia organu sądowego lub organu wykonawczego (trzy państwa)¹⁴ czy też organu mieszanego lub hybrydowego (sześć państw)¹⁵. Z drugiej strony, tylko pięć państw¹⁶ przewiduje kontrolę sądową środków nadzoru tego typu a posteriori, wyłącznie lub w uzupełnieniu innych mechanizmów kontroli. W szczególności we Francji kontrola, o której mowa, jest przeprowadzana przez organ zwany Conseil d'Etat (Radę Stanu), który, jeśli stwierdzi, że zastosowany środek nadzoru jest niezgodny z prawem, unieważnia odpowiednie zezwolenie, nakazuje zniszczenie danych zebranych w ramach nadzoru i informuje zainteresowaną osobę o jej statusie ofiary niezgodnego z prawem nadzoru. Podobnie w Wielkiej Brytanii, Investigatory Power Tribunal rozpatruje skargi osób fizycznych dotyczące prowadzonego wobec nich nadzoru. Wreszcie, w trzech państwach kontrola środków nadzoru a posteriori została powierzona organom podlegającym władzy wykonawczej. W trzynastu z tych państw¹⁷ kontrola przedmiotowego nadzoru a posteriori jest przeprowadzana przez parlamenty krajowe, komisje lub komitety parlamentarne, a w ośmiu innych państwach¹⁸ kontrola ta jest powierzona organom hybrydowym. Wreszcie, w trzech z ww. państw¹⁹ przedmiotowe służby państwowe są nadzorowane przez organy władzy wykonawczej.

120. Dwadzieścia jeden państw objętych badaniem nakłada na organy stosujące nadzór do celów zwalczania przestępczości obowiązek

⁸ Albania, Armenia, Azerbejdżan, Belgia, Bośnia i Hercegowina, Czechy, Estonia, Francja, Gruzja, Niemcy, Grecja, Węgry, Islandia, Irlandia, Włochy, Łotwa, Liechtenstein, Litwa, Luksemburg, Republika Mołdawii, Czarnogóra, Holandia, Macedonia Północna, Norwegia, Rumunia, San Marino, Serbia, Słowenia, Hiszpania i Szwecja

⁹ Belgia, Węgry, Luksemburg, Mołdawia, Czarnogóra, Serbia, Słowenia i Hiszpania

¹⁰ Estonia

¹¹ Czechy i Macedonia Północna

¹² Norwegia, Szwecja i Macedonia Północna

¹³ Albania, Armenia, Azerbejdżan, Chorwacja, Czechy, Estonia, Węgry, Irlandia, Łotwa, Litwa, Luksemburg, Macedonia Północna, Norwegia, Rumunia, Serbia, Słowacja, Słowenia i Szwajcaria

¹⁴ Grecja, Włochy i Liechtenstein.

¹⁵ Belgia, Francja, Niemcy, Luksemburg, Holandia i Wielka Brytania

¹⁶ Francja, Irlandia, Serbia, Słowenia i Wielka Brytania

¹⁷ Chorwacja, Czechy, Estonia, Niemcy, Włochy, Łotwa, Litwa, Luksemburg, Macedonia Północna, Norwegia, Rumunia, Słowacja i Słowenia

¹⁸ Belgia, Chorwacja, Czechy, Francja, Niemcy, Grecja, Holandia i Macedonia Północna

¹⁹ Chorwacja, Łotwa i Luksemburg

powiadomienia zainteresowanej osoby po przeprowadzeniu nadzoru. Osiem państw²⁰ wskazało, że ich ustawodawstwo przewiduje taki obowiązek w odniesieniu do nadzoru prowadzonego w celu ochrony bezpieczeństwa narodowego. Ponadto sześć innych krajów nie wprowadziło żadnych zobowiązań w tym obszarze. W niektórych z ośmiu państw, o których mowa powyżej, właściwy organ może sprzeciwić się takiemu powiadomieniu, jeśli istnieje zagrożenie dla bezpieczeństwa narodowego lub życia lub zdrowia osób prywatnych, lub jeśli istnieje ryzyko utrudnienia dochodzenia w sprawie karnej. W większości z trzydziestu pięciu państw objętych badaniem osoba fizyczna, która była przedmiotem nadzoru, może, w zależności od przypadku, albo zakwestionować go przed sądem powszechnym, składając odwołanie od decyzji zezwalającej na nadzór, albo zwrócić się do właściwego sądu o zbadanie legalności nadzoru i/lub zakwestionować legalność dowodów uzyskanych w wyniku nadzoru. Ponadto dziewięć zainteresowanych państw²¹ wprowadziło podobne środki zaradcze w odniesieniu do niejawnego nadzoru prowadzonego w celu ochrony bezpieczeństwa narodowego. W przypadku szkody wyrządzonej osobie fizycznej przez środek nadzoru zastosowany bez jej wiedzy, dana osoba może, w zależności od danego państwa, albo domagać się odszkodowania w formie powództwa o odszkodowanie, albo żądać wszczęcia postępowania przeciwko agentom właściwych służb państwowych, których uważa za odpowiedzialnych za nadużycia. Ponadto jedenaście państw wprowadziło specjalne środki odwoławcze w tym obszarze, zamiast lub oprócz odwołań sądowych. Rozpatrywanie odwołań złożonych w tym kontekście powierza się, w zależności od przypadku, organom hybrydowym podobnym do tych odpowiedzialnych za nadzór (siedem państw)²² lub organom parlamentarnym i/lub podlegającym władzy wykonawczej (cztery państwa)²³.

121. Oprócz tych środków odwoławczych, zainteresowane państwa wprowadziły dodatkowe zabezpieczenia w swoich odpowiednich przepisach, aby chronić osoby podlegające nadzorowi przed możliwymi nadużyciami ze strony organów prowadzących nadzór. Zabezpieczenia, o których mowa, obejmują m.in. wyczerpujący wykaz przestępstw, w odniesieniu do których można wydać zezwolenie na nadzór, obowiązek wydania wymaganego zezwolenia na piśmie lub uzasadnienia go, lub uzależnienia go od spełnienia istotnych warunków (konieczność, proporcjonalność, pomocniczość) dotyczących nadzoru, ograniczenie możliwości przedłużenia okresu obowiązywania środka, zobowiązanie właściwych organów do postępowania, zniszczenia dowodów uzyskanych w wyniku nadzoru po zakończeniu postępowania karnego, dla którego dowody te zostały zebrane, lub po upływie okresu biegnącego od momentu przeprowadzenia nadzoru, obowiązkowy udział w procedurze zatwierdzania środka nadzoru obrońcy interesów osoby, która jest przedmiotem nadzoru, i wreszcie szczegółowe uregulowanie kwestii związanych z dostępem, przekazywaniem i wykorzystywaniem informacji zebranych w wyniku nadzoru, a w szczególności tych, które są objęte tajemnicą zawodową. Ponadto w ośmiu krajach organy nadzorcze podlegają również nadzorowi organów ochrony danych osobowych, które posiadają rozległą wiedzę techniczną w kwestiach nadzoru.

²⁰ Estonia, Niemcy, Węgry, Liechtenstein, Holandia, Rumunia, Słowenia i Szwajcaria

²¹ Albania, Estonia, Gruzja, Węgry, Włochy, Lotwa, Luksemburg, Słowenia i Szwajcaria

²² Belgia, Francja, Grecja, Irlandia, Holandia, Szwecja i Wielka Brytania.

²³ Bośnia i Hercegowina, Chorwacja, Estonia i Litwa

122. Spośród wszystkich krajów uwzględnionych w badaniu dwadzieścia²⁴ wprowadziło przepisy regulujące zatrzymywanie i przetwarzanie danych dotyczących komunikacji przez Policję i służby wywiadowcze. W szesnastu państwach²⁵ ten rodzaj nadzoru podlega procedurze autoryzacji podobnej do tej mającej zastosowanie do monitoringu operacyjnego, a w trzech państwach²⁶ najwyraźniej nie podlega żadnej formie kontroli sądowej. Wreszcie, dziesięć państw nie dostarczyło Trybunałowi żadnych informacji na temat praktyki ich właściwych organów w odniesieniu do stosowania tego rodzaju nadzoru.

123. Dziewiętnaście państw²⁷ wprowadziło do swojego ustawodawstwa szczegółowe przepisy dotyczące nadzoru o charakterze „strategicznym”, a szesnaście państw²⁸ nie posiada żadnych regulacji w tym obszarze. W jedenastu z dziewiętnastu państw²⁹ dany środek nadzoru podlega kontroli a priori przez organy sądowe, a w dwóch państwach kontrola ta jest powierzona organom władzy wykonawczej³⁰. Większość zainteresowanych państw poddaje ten rodzaj nadzoru kontroli a posteriori, która jest sprawowana, w zależności od przypadku, przez organy parlamentarne (siedem państw)³¹, organy sądowe (cztery państwa)³², organy hybrydowe (sześć państw)³³ lub władzę wykonawczą (dwa państwa)³⁴. W pięciu państwach strategiczne środki nadzoru mogą być kwestionowane w postępowaniu sądowym, a jedenaście państw przewiduje, oprócz lub zamiast takiego postępowania sądowego³⁵, specjalną procedurę, w ramach której nadzór może być kwestionowany, w stosownych przypadkach, przed organem hybrydowym (siedem państw)³⁶ lub przed organem parlamentarnym lub wykonawczym (cztery państwa)³⁷. Wreszcie, pięć państw wprowadziło obowiązek powiadamiania zainteresowanych osób o tego rodzaju nadzorze.

PODSTAWA PRAWNA

I. ŁĄCZENIE SKARG

²⁴ Albania, Armenia, Belgia, Czechy, Estonia, Francja, Węgry, Irlandia, Liechtenstein, Litwa, Luksemburg, Mołdawia, Macedonia Północna, Norwegia, Serbia, Słowacja, Hiszpania, Szwecja, Szwajcaria i Wielka Brytania

²⁵ Albania, Czechy, Estonia, Francja, Węgry, Irlandia, Litwa, Luksemburg, Mołdawia, Norwegia, Serbia, Słowacja, Hiszpania, Szwecja, Szwajcaria i Wielka Brytania

²⁶ Armenia, Belgia i Macedonia Północna

²⁷ Belgia, Bośnia i Hercegowina, Estonia, Francja, Gruzja, Niemcy, Węgry, Irlandia, Łotwa, Liechtenstein, Mołdawia, Holandia, Macedonia Północna, Norwegia, Słowacja, Słowenia, Szwecja, Szwajcaria i Wielka Brytania

²⁸ W przeciwieństwie do nadzoru ukierunkowanego, nadzór strategiczny niekoniecznie jest wywoływany przez podejrzenie dotyczące jednej lub kilku konkretnych osób. Jego celem jest znalezienie lub zidentyfikowanie zagrożenia, a nie tylko zbadanie znanego zagrożenia.

²⁹ Bośnia i Hercegowina, Estonia, Gruzja, Węgry, Irlandia, Łotwa, Mołdawia, Macedonia Północna, Norwegia, Słowacja i Szwajcaria

³⁰ Belgia i Słowenia

³¹ Bośnia i Hercegowina, Estonia, Łotwa, Macedonia Północna, Norwegia, Słowacja i Słowenia

³² Francja, Irlandia, Mołdawia i Wielka Brytania

³³ Belgia, Francja, Liechtenstein, Holandia, Macedonia Północna i Szwecja

³⁴ Bośnia i Hercegowina oraz Łotwa

³⁵ Bośnia i Hercegowina, Estonia, Gruzja, Węgry i Irlandia

³⁶ Belgia, Francja, Grecja, Irlandia, Holandia, Szwecja i Wielka Brytania

³⁷ Bośnia i Hercegowina, Chorwacja, Estonia i Litwa

124. Biorąc pod uwagę podobieństwo przedmiotu skarg, Trybunał uznał za stosowne zbadanie ich łącznie w jednym wyroku.

II. ODNOŚNIE DO DOMNIEMANEGO NARUSZENIA ARTYKUŁU 8 KONWENCJI

125. Powołując się na art. 8 Konwencji, samodzielnie i w związku z art. 13, skarżący zaskarżają, po pierwsze, systemy niejawnego nadzoru oraz zatrzymywania i przetwarzania danych dotyczących komunikacji wprowadzone na mocy ustawy z dnia 15 stycznia 2016 i ustawy o działaniach antyterrorystycznych, uznając, że naruszają one ich prawo do poszanowania życia prywatnego. Następnie stwierdzają, że nie mają skutecznego środka prawnego, aby ustalić, czy sami byli przedmiotem niejawnej inwigilacji, a jeśli tak, to poddać taką inwigilacji kontroli pod kątem zgodności z prawem.

126. Rząd kwestionuje te zarzuty.

127. Zgodnie z zasadą *jura novit curia* Trybunał nie jest związany podstawami prawnymi przedstawionymi przez skarżących na podstawie Konwencji i jej Protokołów i może decydować o kwalifikacji prawnej faktów zawartych w skardze, badając je na podstawie artykułów lub postanowień Konwencji innych niż te, na które powołują się skarżący (*Radomilja i inni przeciwko Chorwacji* [GC], nr 37685/10 i 22768/12, ust. 126, 20 marca 2018). W niniejszej sprawie Trybunał zbada fakty w świetle odpowiednich postanowień art. 8 Konwencji, które brzmią następująco:

Artykuł 8

1. Każdy ma prawo do poszanowania swojego życia prywatnego (...)

2. Niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności osób”.

A. Odnośnie do dopuszczalności

Wstępne zarzuty zgłoszone przez Rząd dotyczące niezgodności ratione personae skargi z postanowieniami Konwencji oraz niewyczerpania krajowych środków odwoławczych

128. Rząd stwierdził, po pierwsze, że skarżący nie mogli twierdzić, że są ofiarami naruszenia ich prawa do poszanowania ich życia prywatnego, a po drugie, że nie wyczerpali krajowych środków odwoławczych. Skarżący, ze swojej strony, zakwestionowali argumenty przedstawione przez Rząd na poparcie tych wyjątków.

129. Trybunał uważa, że zarzuty podniesione przez Rząd są ściśle związane z istotą skarg skarżących i w związku z tym powinny zostać połączone z meritem sprawy (zob. *mutatis mutandis*, *Roman Zakharov przeciwko Rosji* [GC], nr 47143/06, ust. 150, 4 grudnia 2015).

130. Stwierdzając, że skargi wniesione na podstawie art. 8 nie były

oczywiście bezzasadne lub niedopuszczalne z jakiegokolwiek innego powodu na podstawie art. 35 Konwencji, Trybunał uznał je za dopuszczalne.

B. Odnosnie do tła

1. Odnosnie do statusu ofiar w przypadku skarżących oraz zaistnienia „ingerencji”

a) Argumenty stron

i. Rząd

131. Rząd uznaje, że skarżący nie mogli twierdzić, że są ofiarami naruszenia art. 8 Konwencji, a ich skargi miały charakter *actio popularis*. Jego zdaniem status skarżących jako ofiar zależał od warunków określonych w sprawie *Roman Zakharov* (wyrok cytowany powyżej), które nie zostały spełnione w niniejszej sprawie. W tym względzie Rząd stwierdza, że zainteresowane strony nie przedstawiły żadnych dowodów na poparcie swoich twierdzeń, że prowadzono wobec nich nadzór, a zatem twierdzenia te mają charakter spekulacyjny. A zatem skarżący kwestionują jedynie zgodność przedmiotowego ustawodawstwa z Konwencją. Rząd stwierdza ponadto, że skarżący, którzy są obywatelami polskimi, nie mogą skarżyć się na nadzór przewidziany w art. 9 ustawy o działaniach antyterrorystycznych, ponieważ przepis ten miał zastosowanie wyłącznie do cudzoziemców.

132. Uznaje również, że skarżący mieli do dyspozycji krajowe środki odwoławcze i krytykuje ich za nieskorzystanie z tych środków. Rząd argumentuje, iż po pierwsze skarżący mogli, na podstawie art. 2 ust. 1 ustawy o dostępie do informacji publicznej, zwrócić się do właściwych organów publicznych o ujawnienie im informacji rzekomo zebranych bez ich wiedzy w ramach niejawnego środka nadzoru, które to informacje zostały, jego zdaniem, zakwalifikowane jako „publiczne” przez Naczelny Sąd Administracyjny w jego odpowiednim orzecznictwie. Dodał, że gdyby wspomniane organy odmówiły uwzględnienia takiego wniosku, skarżący mogliby zaskarżyć decyzje odmowne do sądów administracyjnych dwóch szczebli. W tym zakresie wskazuje, że skarżący Wojciech Klicki i Katarzyna Szymielewicz, którzy wystąpili z takim wnioskiem do szefa ABW, nie skorzystali z przysługującego im środka zaskarżenia decyzji szefa ABW do sądu administracyjnego. Podnosi ponadto, że gdyby skarżący uważali, że przepisy art. 5 ust. 1 ustawy o dostępie do informacji publicznej w zakresie, w jakim nie zezwalają im na dostęp do informacji rzekomo uzyskanych bez ich wiedzy w drodze niejawnej inwigilacji naruszały ich prawo do poszanowania życia prywatnego, mogli oni – w przypadku bezskutecznego skorzystania z wyżej wymienionych środków odwoławczych przed sądami administracyjnymi – wnieść skargę do Trybunału Konstytucyjnego z powodu ich sprzeczności z art. 47, 49 i 51 ust. 3 Konstytucji. W opinii Rządu, gdyby Trybunał Konstytucyjny orzekł na korzyść skarżących, odpowiednie władze krajowe byłyby zobowiązane do zmiany odpowiednich przepisów, a skarżący mogliby wówczas wnieść powództwo o odszkodowanie przeciwko państwu na podstawie art. 417¹ KK. Ponadto Rząd uznaje, że środek odwoławczy przewidziany w art. 227 KPA był nieformalny i niewiążący dla ww. organów, a zatem skarżący skorzystali ze środka odwoławczego, który był nieskuteczny i nieodpowiedni w niniejszej sprawie. W tym względzie, choć

Rząd zgadza się, że przedmiotowa skarga miała charakter umożliwiający zainteresowanym stronom zwrócenie uwagi władz na ewentualne nieprawidłowości, wyjaśnia, że w żaden sposób nie mogła ona doprowadzić do jakiegokolwiek sądowego rozstrzygnięcia sporu zainteresowanych stron i stwierdza, że był to jedynie wybieg mający na celu wniesienie sprawy do Trybunału. Wreszcie, Rząd krytykuje skarżących za niepodniesienie przed władzami krajowymi, w odniesieniu do pierwszego skarżącego, zarzutów dotyczących naruszenia prawa do obrony jego klientów i prawa do rzetelnego procesu sądowego oraz, w odniesieniu do wszystkich skarżących, zarzutów dotyczących wprowadzenia, bez ich wiedzy, nadzoru nad nimi na podstawie ustawy o działaniach antyterrorystycznych.

ii. Skarżący

133. Skarżący odrzucają argumenty Rządu.

134. Uważają, że mają pełne prawo twierdzić, że są ofiarami naruszenia art. 8 Konwencji, zarówno ze względu na samo istnienie przepisów dotyczących niejawnego nadzoru, jak i ze względu na ich sytuację osobistą. Argumentują oni, że po pierwsze zakres przedmiotowych przepisów był szeroki, wyjaśniając, że miały one zastosowanie do każdej osoby podlegającej jurysdykcji państwa polskiego bez żadnych wyjątków dotyczących dziennikarzy, obrońców lub działaczy na rzecz praw człowieka. Dodają, że nadzór przewidziany w art. 9 ustawy o działaniach antyterrorystycznych dotyczy również osób, z którymi cudzoziemiec będący przedmiotem nadzoru pozostaje w kontakcie, nawet jeśli formalnie znajdują się one poza zakresem przedmiotowego przepisu. Następnie argumentują, że sami są narażeni na zwiększone ryzyko zastosowania wobec nich takiego nadzoru, biorąc pod uwagę ich sytuację osobistą i zawodową. Skarżący Mikołaj Pietrzak wskazuje na przykład, że jako prawnik występował w ważnych sprawach karnych, z których niektóre były politycznie wrażliwe, a także w sprawach dotyczących cudzoziemców, którzy w niektórych przypadkach podlegali niejawnemu nadzorowi. Pozostali skarżąc stwierdzają natomiast, że organizacje pozarządowe, w których pracują, zapewniają wsparcie prawne cudzoziemcom, w tym uchodźcom, oraz że pracują między innymi nad ochroną osób fizycznych przed służbami państwowymi, które prowadzą nadzór przy użyciu nowych technologii. Uważają oni, że dane szczególnie chronione będące w ich posiadaniu w związku z ich działalnością zawodową czynią ich głównymi celami dla organów nadzorczych, tym bardziej że nie istnieje żaden skuteczny mechanizm chroniący ich przed nadużyciami popełnianymi przez te organy. W szczególności Mikołaj Pietrzak podnosi, że środki techniczne, którymi dysponują zainteresowane służby państwowe, są niewątpliwie skuteczniejsze niż środki, które – jak twierdzi – podjął w celu zagwarantowania poufności swoich kontaktów zawodowych z klientami, a zatem środki te nie stanowią gwarancji bezpieczeństwa tych kontaktów w niniejszej sprawie. Ponadto, z odpowiednich danych statystycznych posiadanych przez Okręgową Radę Adwokacką w Warszawie wynika, że w okresie od czerwca 2016 do września 2022 adwokaci należący do Okręgowej Rady Adwokackiej w Warszawie zgłosili Okręgowej Radzie Adwokackiej w Warszawie około trzystu dwudziestu pięciu prób naruszenia tajemnicy ich komunikacji zawodowej.

135. Skarżący zgłosili również, po pierwsze, że prawo polskie nie przewiduje żadnego środka odwoławczego, który umożliwiłby im, w razie potrzeby,

ustalenie istnienia dotyczącego ich środka nadzoru i zbadanie jego zgodności z prawem, a po drugie, że obowiązujące ustawodawstwo nie nakłada na służby państwowe odpowiedzialne za te działania żadnego obowiązku powiadamiania zainteresowanych osób o środkach nadzoru, nawet w przypadku wyraźnego wniosku w tym zakresie z ich strony, co ich zdaniem uniemożliwia osobom objętym nadzorem zakwestionowanie zgodności z prawem takiego środka. Uznają, że skargi Rządu były pozbawione jakiegokolwiek użytecznego skutku, argumentując, że nie przedstawili żadnego przykładu decyzji krajowej, która mogłaby udowodnić coś przeciwnego. Wskazują również, że w niniejszej sprawie dwóch z nich bezskutecznie skorzystało z pierwszego ze środków odwoławczych wskazanych przez pozwane państwo. Ich zdaniem z przepisów prawa, na podstawie których szef ABW odrzucił ich wnioski, wynika, że informacje gromadzone w drodze niejawnego nadzoru mają charakter poufny, a zatem miał on obowiązek odmówić dostępu do nich każdemu, kto o to wnioskował. Dodają, że te zasady mają zastosowanie do wszystkich służb policyjnych i wywiadowczych, które korzystają z nadzoru. Jeśli chodzi o zaskarżenie decyzji szefa ABW do sądu administracyjnego, uznali oni, że jest ono skazane na niepowodzenie w świetle utrwalonego orzecznictwa Naczelnego Sądu Administracyjnego – tego samego orzecznictwa, do którego Rząd odniósł się w swoich uwagach; wyjaśnili, że sąd ten orzekł nie tylko, że informacje gromadzone przez Policję i służby wywiadowcze w drodze tajnej nadzoru są „publiczne”, ale także, że zgodnie z art. 5 ustawy o ochronie dostępu do informacji publicznej dostęp do takich informacji podlega ograniczeniom, w tym ograniczeniom określonym w ustawie o ochronie danych niejawnych. Podejście orzecznicze Naczelnego Sądu Administracyjnego w tej sprawie można zatem podsumować następująco: „Ograniczenia w dostępie do informacji publicznej związane z działalnością służb specjalnych, o ile wynikają z konieczności zapewnienia ochrony informacji niejawnych, są uzasadnione”.

136. Jeśli chodzi o skargę do Trybunału Konstytucyjnego, której wniesienie Rząd uznał za konieczne, jeśli środki odwoławcze, które skarżący wniesli do władz administracyjnych i sądów, nie przyniosły rezultatu, skarżący stwierdzili, że poza faktem, że środki te były w każdym razie nieskuteczne, nie można jej uznać za „środek odwoławczy, który należy wyczerpać” w rozumieniu orzecznictwa Trybunału z wielu powodów. Po pierwsze, stwierdzają oni, że aby skarga konstytucyjna była dopuszczalna, musi kwestionować przepis lub przepisy ustawowe, na których właściwy sąd lub organ władzy publicznej oparł decyzję zaskarżoną do Trybunału Konstytucyjnego. Wyjaśnili, że w niniejszej sprawie z decyzji szefa ABW dotyczących skarżącego Wojciecha Klickiego i skarżącej Katarzyny Szymielewicz wynika, że organ ten zastosował cały szereg przepisów prawa, a nie tylko art. 5 ustawy o dostępie do informacji publicznej. W związku z tym uznali, że wbrew temu, co Rząd twierdził w swoich uwagach, zaskarżenie przez nich samego art. 5 do Trybunału Konstytucyjnego byłoby niewystarczające w świetle surowych warunków dopuszczalności, które musiałaby spełniać skarga konstytucyjna. Po drugie, twierdzą oni, że taka skarga konstytucyjna doprowadziłaby do kontroli przez Trybunał Konstytucyjny jedynie przepisów regulujących funkcjonowanie ABW, a nie wszystkich odpowiednich przepisów, a zatem musieliby wszcząć kilka postępowań administracyjnych i złożyć skargę do Trybunału Konstytucyjnego w celu spełnienia wymogu wyczerpania krajowych

środków odwoławczych przed Trybunałem w Strasburgu. Po trzecie, wskazują oni, że korzystny dla nich wyrok Trybunału Konstytucyjnego nie unieważniłby automatycznie decyzji odmownych szefa ABW i sądów administracyjnych, a jedynie stanowiłby podstawę, pod pewnymi warunkami, do wznowienia stosownych postępowań, których przedmiot ograniczałby się zresztą, ich zdaniem, wyłącznie do kwestii dostępu do informacji niejawnych zgromadzonych przez ABW. Dodali również, że skarga konstytucyjna nie umożliwiłaby im ani zbadania legalności jakiegokolwiek nadzoru nad nimi, ani uzyskania odszkodowania w przypadku, gdyby był on niezgodny z prawem. Po czwarte, uważają, że skarga konstytucyjna nie spełnia wymogów skutecznego środka odwoławczego ze względu na kontrowersje, których przedmiotem jest obecnie Trybunał Konstytucyjny, a które stały się – jak podkreślają – podstawą wyroku w sprawie *Xero Flor (Xero Flor w Polsce sp. z o.o. przeciwko Polsce*, nr 4907/18, 7 maja 2021) prowadzonej przez Europejski Trybunał Praw Człowieka. Po piąte, powołując się na orzecznictwo Trybunału Konstytucyjnego (zob. pkt 70–73 powyżej), argumentowali, że Trybunał Konstytucyjny rozpatrywał już skargi podobne do tych rozpatrywanych w niniejszej sprawie, że przy tej okazji uznał, iż zaskarżone przepisy są niezgodne z konstytucją, a zatem wniesienie przez nich skargi do Trybunału Konstytucyjnego byłoby bezcelowe. Twierdzą oni ponadto, że ustawodawstwo, które miało na celu dostosowanie zaskarżonych przepisów do zasad określonych przez Trybunał Konstytucyjny, w rzeczywistości pogorszyło sytuację w tym zakresie, a w każdym razie obecny Trybunał Konstytucyjny stwierdził (zob. pkt 76 poniżej), że kontrola sądowa w odniesieniu do decyzji zezwalających na środki nadzoru nie jest wymagana. Po szóste, przypominając, że złożyli odwołanie na podstawie art. 227 KPA, twierdzili, że odwołanie to umożliwiło im potępienie wszystkich operacji nadzoru prowadzonych niejawnie przez zainteresowane służby państwowe i że dało tym służbom możliwość udzielenia odpowiedzi na wszystkie ich skargi dotyczące przedmiotowych operacji. Uznali również, że powództwo o odszkodowanie przeciwko państwu na podstawie art. 417¹ kodeksu cywilnego byłoby nieskuteczne, wyjaśniając, że takie powództwo wymagałoby wykazania bezprawnego charakteru dotyczącego ich nadzoru, a wymóg ten nie mógł zostać spełniony w przypadku braku jakiegokolwiek powiadomienia ich o przedmiotowym nadzorze. Wreszcie, w odpowiedzi na argument Rządu, że nie podnieśli przed władzami krajowymi niektórych ze swoich skarg dotyczących nadzoru prowadzonego na podstawie art. 9 ustawy o działaniach antyterrorystycznych, argumentowali, że w swoich odpowiednich skargach zakwestionowali możliwość korzystania przez służby państwowe z niejawnego nadzoru jako całości, a zatem ich skargi dotyczyły również nadzoru prowadzonego na podstawie przedmiotowego przepisu.

137. Skarżący stwierdzają, że nieadekwatność obowiązujących przepisów, w połączeniu z brakiem niezależnego mechanizmu kontroli i brakiem skutecznego środka odwoławczego w ich sprawie, daje im uzasadniony powód do obaw, że ich komunikacja jest objęta nadzorem.

b) Ocena Trybunał

i. Zasady ogólne

138. Trybunał stwierdził, że w niniejszej sprawie skarżący zarzucali

ingerencję w korzystanie z ich prawa chronionego na mocy art. 8 Konwencji, która miała wynikać nie z konkretnych środków nadzoru zastosowanych wobec nich, ale z samego istnienia przepisów zezwalających na niejawną nadzór nad ich komunikacją i ryzyka, że sami mogą podlegać takim środkom. 139. Trybunał pragnie wskazać, że ogólne zasady dotyczące tego, czy skarżący mogą twierdzić, że są „ofiarami” naruszenia art. 8 spowodowanego samym istnieniem ustawodawstwa krajowego lub praktyki zezwalającej na tajną nadzór, zostały określone w wyroku w sprawie *Roman Zakharov* (*Roman Zakharov*, cytowana powyżej, ust. 171), a następnie powtórzone w sprawie *Centrum för rättvisa przeciwko Szwecji* [GC], nr 35252/08, ust. 167, 25 maja 2021, oraz *Ekimdzhiev i inni przeciwko Bułgarii*, nr 70078/12, ust. 262, 11 stycznia 2022.

ii. Zastosowanie do niniejszej sprawy

140. W niniejszej sprawie Trybunał zauważa, że skarżący skarżą się na przepisy dotyczące niejawnego nadzoru, stosowane przez różne krajowe służby policyjne i wywiadowcze. Zauważa, po pierwsze, że system nadzoru prawnego składa się z kilku ustaw regulujących odpowiednie działania wspomnianych służb państwowych, a po drugie, że wszystkie odpowiednie teksty przewidują praktycznie identyczny model nadzoru. Zauważa również, że ustawa o Policji stanowi przykład *mutatis mutandis* dla innych organów.

141. Trybunał stwierdził, że w odniesieniu do niejawnego nadzoru ustawodawstwo krajowe ustanawia dwa różne systemy prawne, a mianowicie jeden odnoszący się do kontroli operacyjnej, a drugi odnoszący się do zatrzymywania i przetwarzania danych dotyczących komunikacji. Zauważa, że dwa rodzaje nadzoru, o których mowa, są regulowane odpowiednio przez art. 19 i art. 20 c ustawy o Policji. Zauważa ponadto, że pierwszy z tych przepisów włącza w zakres środków kontroli operacyjnej, które umożliwiają organom zapoznanie się z treścią komunikatów uzyskanych za pomocą środków takich jak, między innymi, podsłuch, nagrywanie rozmów telefonicznych, wiadomości e-mail lub wiadomości pozostawionych na poczcie głosowej, przechwytywanie korespondencji pocztowej lub nagrywanie rozmów na żywo przy użyciu odpowiednich urządzeń (zob. pkt 31 poniżej). Zdaniem Trybunału oczywiste jest, że takie środki nadzoru wiążą się z ingerencją w sferę prywatną osób, które są nimi objęte przez działania służb państwowych. Jeśli chodzi o dane dotyczące komunikacji, Trybunał zauważa, że obejmują one informacje dotyczące w szczególności wykonanych lub odebranych połączeń telefonicznych, wybieranych numerów, czasu trwania połączeń, położenia geograficznego urządzeń mobilnych, odwiedzanych stron internetowych, połączeń ze stronami internetowymi i adresów e-mail (pkt 46 poniżej). W tym względzie przypomina, że stwierdzał już, iż „o ile treść komunikacji, zaszyfrowana lub nie, może nie ujawniać nic użytecznego o jej nadawcy lub odbiorcy, to powiązane dane dotyczące komunikacji mogą ujawniać wiele informacji osobistych (...) [ponadto] wszelkie naruszenia spowodowane pozyskiwaniem powiązanych danych dotyczących komunikacji są z wielokrotnością przez masowe przechwytywanie, ponieważ dane te mogą [następnie] być analizowane i badane w celu stworzenia intymnego portretu danej osoby (...)” (*Big Brother Watch i inni przeciwko Zjednoczonemu Królestwu* [GC], nr 58170/13 i 2 inne, ust. 342, 25 maja 2021).

142. Trybunał zauważa, że art. 19 ust. 1 ustawy o Policji zezwala

funkcjonariuszom Policji na niejawnie prowadzenie czynności operacyjno-śledczych w celu zapobiegania lub wykrywania przestępstw, wykrywania sprawców takich przestępstw oraz zbierania i utrwalania dowodów. Zauważa, że katalog przestępstw, w odniesieniu do których przedmiotowe środki nadzoru mogą być stosowane przez dane organy państwowe, jest sformułowany w sposób szeroki, a ponadto zauważa, że kilka specjalnych służb państwowych może wprowadzić takie środki nadzoru w celach przydatnych do wykonywania ich odpowiednich obowiązków ustawowych. Odnosząc się do wniosków Trybunału Konstytucyjnego w wyroku K 23/11 (cytowanym powyżej), Trybunał uznaje również, że zakres *ratione personae* kontroli operacyjnej jest szeroki. Ponadto, odnosząc się do wyżej wspomnianej opinii Komisji Weneckiej (zob. pkt 92 powyżej), zauważa, że organ ten uznał, z jednej strony, że „cel nadzoru nie został jasno określony w ustawie o Policji”, a z drugiej strony, że „dowolna osoba lub grupa [mogła być celem nadzoru], o ile jest prawdopodobne, że w ten sposób można uzyskać informacje, które umożliwią osiągnięcie celów określonych dla nadzoru w art. 19 [ustawy o Policji] oraz w art. 20c [tej samej ustawy] w odniesieniu do gromadzenia metadanych”. Jeśli chodzi w szczególności o ten ostatni rodzaj nadzoru, Trybunał wziął pod uwagę fakt, że odpowiednie przepisy nie określają kategorii osób, których komunikacja może być nadzorowana. Zdaniem Trybunału sporne przepisy, jak wynika z przedstawionych powyżej wniosków opinii Komisji Weneckiej, ustanowiły system nadzoru, w ramach którego praktycznie każdy użytkownik usług telekomunikacyjnych i internetowych może mieć przechwyconą komunikację i nie zostać nigdy poinformowanym, że został objęty nadzorem. Jeśli chodzi o przepisy ustawy o działaniach antyterrorystycznych, Trybunał zauważa, podobnie jak skarżący, że chociaż zakres *ratione personae* przedmiotowej ustawy jest ograniczony do cudzoziemców podejrzanych o działalność terrorystyczną, każda osoba, która była z nimi w kontakcie, może pośrednio doświadczyć nadzoru swojej komunikacji, niezależnie od tego, czy została osobiście objęta nadzorem (zob. *mutatis mutandis Ekhimdzhiiev i inni*, cytowany powyżej, ust. 263).

143. Trybunał uważa również, że z powodów przedstawionych poniżej w paragrafach 241–245, polskie prawo nie przewiduje skutecznych środków odwoławczych dla osoby, która uważa, że została poddana tajnemu nadzorowi (zob. *mutatis mutandis, Roman Zakharov*, cytowany powyżej, ust. 176).

144. Uznał zatem, że w niniejszej sprawie skarżący nie musieli wykazywać, że byli narażeni na ryzyko poddania ich niejawnemu nadzorowi ze względu na ich sytuację osobistą (dla podobnego rozumowania, patrz *idem*, ust. 177 i *Ekhimdzhiiev i inni*, cytowany powyżej, ust. 276).

145. Biorąc pod uwagę niejawny charakter i szeroki zakres środków nadzoru przewidzianych w przepisach zaskarżonych przez skarżących oraz brak skutecznych krajowych środków odwoławczych, za pomocą których osoby, które uważałyby się za objęte nadzorem, mogłyby zakwestionować środki nadzoru rzekomo zastosowane wobec nich, Trybunał uważa, że uzasadnione jest zbadanie zaskarżonych przepisów *in abstracto* (*idem*, ust. 277).

146. W związku z tym uznał, że skarżący mogli twierdzić, że są ofiarami naruszenia Konwencji, mimo że nie mogli stwierdzić na poparcie swoich wniosków, że zostali poddani konkretnemu środkowi nadzoru. Z tych samych powodów uważa, że samo istnienie przedmiotowego ustawodawstwa stanowi samo w sobie ingerencję w korzystanie przez zainteresowane osoby z ich

praw wynikających z art. 8 Konwencji. W konsekwencji Trybunał odrzuca zarzut Rządu, że skarżący nie zasługują na status ofiary.

2. Odnosnie do uzasadnienia

ingerencji a) Argumenty stron

i. Dostępność prawa wewnętrznego

147. Skarżący uznali, że ustawodawstwo krajowe dotyczące tajnego nadzoru nie spełniało wymogów jakościowych, aby stanowić „prawo” w rozumieniu Konwencji, a zatem doszło w odniesieniu do nich do naruszenia art. 8 Konwencji. Wskazują oni, że chociaż ogólne uprawnienia służb państwowych odpowiedzialnych za prowadzenie nadzoru są regulowane przez przepisy regulujące działanie tych służb, różne środki przechwytywania podlegają szczegółowym przepisom, które mają charakter poufny. Stwierdzają oni, że regulacja ta jest konsekwencją ochrony przyznanej metodom działania służb specjalnych i stosowanym przez nie środkom. Wyjaśnili, że z jednej strony odpowiednie przepisy upoważniają szefów różnych zainteresowanych służb do regulowania wspomnianych metod i środków w drodze dekretów, a z drugiej strony dotychczasowe próby ustawodawcy uregulowania wszystkich powiązanych kwestii w jednej ustawie nie powiodły się.

148. Rząd utrzymuje, że przedmiotowe przepisy spełniają wymogi „dostępności” i „przewidywalności”. Argumentuje, że wszystkie odpowiednie przepisy krajowe zostały opublikowane w Dzienniku Ustaw, a zatem są „dostępne”. Dodaje, że przepisy wspomnianych ustaw są sformułowane wystarczająco precyzyjnie i w sposób umożliwiający każdej osobie – w razie potrzeby z odpowiednią poradą – dopasowanie swojego postępowania. Uważa, że przedmiotowe ustawodawstwo krajowe zapewnia obywatelom, w jasny i szczegółowy sposób, odpowiednie wskazanie okoliczności, w których władze publiczne są uprawnione do uciekania się do niejawnego nadzoru.

ii. Zakres stosowania środków nadzoru

149. Skarżący uważają, że zakres niejawnego nadzoru jest szeroki. Wyjaśniają w tym względzie, że kilka służb policyjnych i wywiadowczych może zastosować przedmiotowy środek i że mogą to zrobić w odniesieniu do dużej liczby przestępstw, z których niektóre, jak twierdzą, są stosunkowo drobne. Dodają, że właściwe służby policyjne i Żandarmeria Wojskowa mogą ponadto zatrzymywać dane dotyczące komunikacji do celów zapobiegania i wykrywania wszelkich przestępstw, z zastrzeżeniem jedynie, że przestępstwo jest karalne na mocy prawa krajowego. Argumentowali również, że przepisy określające listę przestępstw, w odniesieniu do których można prowadzić tajny nadzór, zostały zbadane przez Trybunał Konstytucyjny, który w sprawie K 23/11 (cytowanej powyżej) stwierdził, że niektóre z nich są niezgodne z Konstytucją.

150. Skarżący argumentowali również, że procedura „nadmierzająca” przewidziana w art. 19 ust. 3 ustawy o Policji (zob. pkt 35 powyżej), zgodnie z którą Policja może prowadzić nadzór bez zgody sędziego przez okres do pięciu dni, miała zastosowanie do wszystkich przestępstw, w przypadku których dozwolony był nadzór operacyjny, a nie tylko do najpoważniejszych przestępstw.

151. Skarżący uznają, że przepisy dotyczące tajnego nadzoru zawierały ogólne sformułowanie, argumentując, że zgodnie z art. 9 ustawy o działaniach antyterrorystycznych (zob. pkt 52–57 powyżej) ustawa zezwalała władzom na prowadzenie takiego nadzoru wobec „osoby niebędącej obywatelem Rzeczypospolitej Polskiej, w stosunku do której istnieje obawa co do możliwości prowadzenia przez nią działalności terrorystycznej”, a niejasność tego sformułowania może prowadzić do kwestionowania jego stosowania w praktyce przez służby państwowe odpowiedzialne za tę sprawę.

152. Wskazują również, że stopień precyzji przepisów regulujących uprawnienia do tajnego nadzoru różnych służb policyjnych i wywiadowczych różni się w zależności od danej służby. Powołując się na art. 6 ust. 8 ustawy o ABW, zarzucili, że zezwala on na stosowanie technik wywiadu elektronicznego, mimo że techniki te nie były, ich zdaniem, przedmiotem żadnej szczególnej regulacji w prawie krajowym.

153. Uważają również, że przepisy krajowe nie określają wystarczająco przestępstw, które mogą stanowić podstawę do zatrzymywania danych dotyczących komunikacji. Ich zdaniem z brzmienia przedmiotowych przepisów prawa wynika, że taki środek może być stosowany w każdym dochodzeniu i w odniesieniu do każdego przestępstwa. Uważają, że chociaż zatrzymywanie danych dotyczących komunikacji jest dozwolone w ramach odpowiednich kompetencji każdej z zainteresowanych służb państwowych, jego stosowanie nie jest wolne od nadużyć z ich strony, biorąc pod uwagę brak jakiegokolwiek niezależnego mechanizmu kontroli wobec przedmiotowych służb państwowych, który interweniowałby na etapie zatwierdzania wspomnianego środka. Odnosząc się do odpowiednich przepisów ustawy o CBA, dodają, że CBA może przechowywać dane dotyczące komunikacji do celów czysto analitycznych.

154. Argumentują, że ustawa o Policji i inne przepisy regulujące nadzór nie określają dokładnie, jakie dane dotyczące komunikacji mogą być gromadzone, ale odsyłają w tym zakresie do innych przepisów, w tym odpowiednio dotyczących telekomunikacji, Internetu i komunikacji pocztowej. Zwracają również uwagę, że odpowiednie przepisy wymagają, aby dane były przechowywane przez dostawców usług telekomunikacyjnych przez dwanaście miesięcy, co ich zdaniem oznacza, że ilość danych udostępnianych w ten sposób zainteresowanym organom jest bardzo duża.

155. W odniesieniu do kategorii osób, które mogą podlegać niejawnemu nadzorowi, skarżący wyjaśnili, że art. 19 ust. 5 ustawy o Policji stanowił, że taki środek może być stosowany w odniesieniu do podejrzanego „lub” oskarżonego, z czego wywnioskowali, że osoby, których komunikacja została przechwycona, niekoniecznie musiały być podejrzanе o popełnienie jakiegokolwiek przestępstwa. Powołując się na ustalenia zawarte w cytowanym powyżej wyroku Trybunału Konstytucyjnego K 23/11, argumentują, że zakres *ratione personae* nadzoru jest co do zasady nieograniczony; dodali, że przepisy dotyczące zatrzymywania danych telekomunikacyjnych nie zawierają z kolei żadnej specyfikacji co do ich zakresu *ratione personae*.

156. Wreszcie skarżący zauważają, że sporne przepisy nie przewidują żadnych odstępstw w odniesieniu do monitorowania komunikacji zawodowej przez prawników i dziennikarzy. Wyjaśniają po pierwsze, że choć ustawa o Policji nakłada na służby państwowe, które prowadziły nadzór, obowiązek zniszczenia zgromadzonych przez nie informacji tego typu, to nie przewiduje ona zewnętrznego i niezależnego mechanizmu kontroli w zakresie realizacji

przez te służby przedmiotowego obowiązku, a po drugie, że o usunięciu zgromadzonych informacji decydują wyłącznie przedstawiciele służb prowadzących nadzór na podstawie analizy ich treści. Argumentują oni, że dopiero gdy materiał objęty tajemnicą zawodową zostanie przekazany właściwemu sądowi do zbadania, sąd decyduje, czy wykorzystać ten materiał jako dowód w postępowaniu karnym. Uważają również, że ryzyko przejęcia przez władze treści komunikacji zawodowej prawników samo w sobie może zaszkodzić prawu do obrony ich klientów i prawidłowemu funkcjonowaniu wymiaru sprawiedliwości jako całości.

157. Rząd utrzymywał, że z odpowiednich przepisów ustaw regulujących działanie Policji i służb wywiadowczych wynikało, że służby te stosowały środki nadzoru wyłącznie w ramach swoich uprawnień oraz w celu zapobiegania i wykrywania najpoważniejszych przestępstw, jak wyraźnie określono w tych przepisach. Dodał, że w wyniku orzeczenia Trybunału Konstytucyjnego w sprawie K 23/11, przepisy ustaw skrytykowanych przez Trybunał zostały zmienione, tak że obowiązek niszczenia przedmiotów objętych tajemnicą obrony i spowiedzi zebranych w trakcie nadzoru ma teraz zastosowanie do wszystkich służb policyjnych i wywiadowczych prowadzących nadzór.

iii. Czas trwania nadzoru

158. Skarżący argumentują, że okres osiemnastu miesięcy, w którym można prowadzić niejawną nadzór, jest sam w sobie długi, a ponadto, ponieważ to służby ABW lub SKW mogą się do niego odwoływać, środek ten może być przedłużany w nieskończoność. Dodają, że w nagłych przypadkach środek nadzoru może być stosowany przez pięć dni bez uprzedniego zezwolenia lub kontroli sądowej. Wreszcie, wskazują oni, że ustawa o działaniach antyterrorystycznych pozwala władzom na stosowanie niejawnego nadzoru wobec cudzoziemca bez zgody sądu przez okres do trzech miesięcy.

159. Rząd stwierdza, że nadzór jest dozwolony na okres nieprzekraczający trzech miesięcy i że może zostać przedłużony tylko raz, za zgodą właściwego sądu okręgowego i na maksymalny okres trzech miesięcy, jeżeli nie ustały przyczyny, które uzasadniały jego wprowadzenie. Wyjaśnia, że jeśli pojawiają się nowe okoliczności uzasadniające kontynuowanie dochodzenia, właściwy sąd może nakazać kontynuowanie nadzoru przez kilka kolejnych okresów, których łączny czas nie może przekroczyć dwunastu miesięcy. Określa on, po pierwsze, że zasady te mają również zastosowanie w sytuacjach nadzwyczajnych, a po drugie, że nadzór zostaje przerwany, gdy tylko ustaną przyczyny, które uzasadniały jego zastosowanie, a najpóźniej z końcem okresu, na który został zatwierdzony.

iv. Zatwierdzanie środków nadzoru

160. Skarżący twierdzą, że odwołanie się do kontroli operacyjnej przez właściwe służby państwowe wymaga uprzedniej zgody sądu, z wyjątkiem sytuacji nadzwyczajnych, kiedy dany środek może zostać zastosowany bez zgody sądu na maksymalny okres pięciu dni. Wskazują również, że wymóg uprzedniej zgody sądu nie ma zastosowania do zatrzymywania danych dotyczących komunikacji, a ustawa antyterrorystyczna zezwala na

prorowadzenie niejawnego nadzoru przez trzy miesiące bez uprzedniej zgody sądu.

161. Skarżący uznają również, że procedura sądowego zatwierdzenia nadzoru ma wady, które ich zdaniem wynikają w szczególności z jej poufnego charakteru i braku udziału w niej osoby, która była przedmiotem przedmiotowego środka. Wyjaśniają w tym względzie, że decyzja wydana na koniec wspomnianej procedury jest poufna, nie jest uzasadniona i może zostać zaskarżona wyłącznie przez prokuratora, z wyłączeniem osoby podlegającej nadzorowi, dodając, że krajowe orzecznictwo dotyczące tajnej nadzoru jest niedostępne dla opinii publicznej, a sąd rozpatrujący wniosek o zezwolenie na nadzór podejmuje decyzję wyłącznie na podstawie informacji zawartych w aktach, które zainteresowane służby uznały za przydatne do przekazania mu na poparcie ich wniosku. Jednakże, według skarżących, odpowiednie statystyki pokazują, że odsetek wniosków o zezwolenie na nadzór rozpatrzonych pozytywnie przez sądy wynosi około dziewięćdziesiąt dziewięć procent wszystkich rozpatrzonych wniosków. Skarżący uważają, że w tych okolicznościach każdy powinien kwestionować zarówno stosowanie nadzoru przez Policję i służby wywiadowcze na zasadzie czysto pomocniczej, jak i skuteczność kontroli sądowej wspomnianego nadzoru. 162. Skarżący wskazują również, że zatrzymywanie danych dotyczących komunikacji przez odpowiednie służby państwowe nie podlega żadnemu uprzedniemu zezwoleniu sądowemu. Uważają one, że wykorzystanie tego środka persona przez służby nie ma charakteru pomocniczego, lecz pierwszorzędny i nie podlega żadnej skutecznej niezależnej kontroli. W tej kwestii utrzymują, że kontrola przeprowadzana przez sądy okręgowe na podstawie półrocznych sprawozdań przedkładanych im przez zainteresowane służby państwowe nie spełnia wymogów Konwencji w tym zakresie, ponieważ ich zdaniem jest fakultatywny i nie może prowadzić do właściwej oceny „konieczności” i „proporcjonalności” nadzoru. Dodają, że odpowiednie przepisy nie określają kryteriów, na podstawie których przeprowadzana jest ta kontrola, ani jej skutków w odniesieniu do gromadzonych danych i osób objętych tym środkiem. Stwierdzają, że zatrzymywanie danych dotyczących komunikacji nie podlega skutecznej kontroli niezależnego organu, który byłby w stanie zweryfikować, czy Policja wykorzystuje swoje uprawnienia w rozsądny sposób i zgodnie z dobrą praktyką dochodzeniową.

163. Skarżący zauważają również, że kontrola sprawowana przez prokuratorów nad służbami państwowymi stosującymi nadzór nie może być uznana za skuteczną ze względu na obecne podporządkowanie polskich prokuratorów ministrowi sprawiedliwości. Ich zdaniem podobne względy mają zastosowanie do komisji sejmowej nadzorującej działalność służb specjalnych. W tym punkcie argumentują, że chociaż komisja ta posiada rozległą wiedzę specjalistyczną w tej dziedzinie, składa się wyłącznie z polityków, z wyłączeniem jakichkolwiek ekspertów, a ponadto jej sprawozdania dla Sejmu i Senatu są poufne, a jej posiedzenia odbywają się za zamkniętymi drzwiami. Dodają, że Najwyższa Izba Kontroli (NIK) nie ma uprawnień do nadzorowania środków nadzoru wprowadzonych w odniesieniu do osób prywatnych.

164. Rząd wyjaśnia, że zgodnie z polskim prawem kontrola operacyjna podlega kontroli sądowej a priori zarówno w odniesieniu do jej zatwierdzenia, jak i rozszerzenia, a środek zatrzymywania danych dotyczących komunikacji podlega kontroli sądowej a posteriori. Twierdzi, że procedura zatwierdzania środków nadzoru jest szczegółowo uregulowana. W tym względzie wyjaśnia,

że środki, o których mowa, mogą zostać zatwierdzone przez właściwy sąd okręgowy na wniosek szefa jednej lub więcej zainteresowanych służb państwowych, jego zastępców lub innych urzędników wyraźnie upoważnionych na mocy odpowiednich przepisów, którzy muszą złożyć pisemny wniosek należycie uzasadniony i zatwierdzony z wyprzedzeniem przez prokuratora; wniosek ten musi również określać numer akt sprawy, przestępstwo, którego dotyczy i jego kwalifikację prawną, okoliczności uzasadniające zastosowanie nadzoru, dowody na to, że inne środki dochodzeniowe okazały się nieskuteczne lub bezużyteczne, dane osoby, której dotyczy wniosek, umożliwiające jej jednoznaczną identyfikację, miejsce, w którym ma być prowadzony nadzór oraz rodzaj, cel i czas trwania proponowanego środka nadzoru. Stwierdza również, że sąd powołany do orzekania w sprawie takiego wniosku sprawdza zgodność z prawem i proporcjonalność danego środka, podkreślając, że wszystkie czynności właściwego sądu są wykonywane zgodnie z przepisami regulującymi przekazywanie, przechowywanie i niszczenie informacji niejawnych. Dodaje, że odrzucenie przez sąd wniosku o zezwolenie może stanowić podstawę do wniesienia odwołania przez organ publiczny, który złożył wniosek. Wyjaśnia również, z jednej strony, że tylko wyjątkowo, w przypadkach wyjątkowo pilnych ze względu na ryzyko utraty lub zmiany dowodów popełnienia przestępstwa, szef danej służby państwowej może zarządzić zastosowanie środka nadzoru wyłącznie na podstawie uprzedniej zgody właściwego prokuratora oraz, po drugie, że jeżeli zezwolenie sądowe na wspomniany środek nie zostanie uzyskane w ciągu pięciu dni od rozpoczęcia jego stosowania, nadzór zostaje przerwany, a uzyskane w związku z nim informacje zostają niezwłocznie zniszczone.

165. Rząd wskazuje również, że art. 20 ca ustawy o Policji (pkt 49 powyżej) nakłada na Policję obowiązek przedkładania właściwemu sądowi okręgowemu półrocznego sprawozdania zawierającego następujące informacje dotyczące zatrzymywania i przetwarzania danych dotyczących komunikacji w okresie referencyjnym: liczbę przypadków zatrzymania danych, ze wskazaniem rodzaju danych, o których mowa; kwalifikacje prawne, w odniesieniu do których złożono wnioski o zatrzymanie danych dotyczących komunikacji, lub informacje dotyczące zatrzymania danych mających na celu ochronę życia i zdrowia ludzkiego lub wsparcie misji poszukiwawczych lub ratowniczych. Dodaje, że sąd nadzorujący stosowanie środka zatrzymywania danych z łączności przez właściwe służby państwowe może zapoznać się z treścią tych sprawozdań i że informuje Policję o swoich wnioskach w ciągu trzydziestu dni od zakończenia sprawozdania. Określa, że ten mechanizm monitorowania zatrzymywania danych dotyczących komunikacji został wprowadzony w następstwie orzeczenia Trybunału Konstytucyjnego K 23/11 i wejścia w życie, w następstwie tego orzeczenia, ustawy z 15 stycznia 2016.

166. Stwierdza również, że przechowywanie i przetwarzanie danych dotyczących komunikacji przez służby państwowe korzystające z tego środka nadzoru odbywa się pod nadzorem ich odpowiednich przełożonych na wszystkich etapach procesu. Wyjaśnia, że przedmiotowy środek nadzoru stanowi zarówno podstawowy, jak i pomocniczy środek dochodzeniowy dla zainteresowanych służb państwowych, precyzując, że w przypadku dochodzeń w sprawie niektórych przestępstw, takich jak stalking, oszustwa popełnione przez Internet lub rozpowszechnianie zdjęć pornograficznych, jest to w praktyce jedyny sposób na uzyskanie odpowiednich dowodów.

167. Argumentuje, że niejawni nadzoru jest gwarancją skuteczności dla stosujących ją służb państwowych, a w konsekwencji osoba jej poddana nie jest powiadamiana o danym środku.

168. Wreszcie wskazuje, że stosowanie środków nadzoru podlega nie tylko kontroli sądowej, ale jest również nadzorowane przez Sejm i Senat lub, w przypadku działań służb specjalnych, przez komisję parlamentarną, która, jak podkreśla, bada roczne sprawozdania przedkładane jej przez odpowiednich szefów zainteresowanych służb. Dodaje, że ci ostatni, o ile działają w ramach wykonywania obowiązków służbowych, również podlegają nadzorowi NIK z punktu widzenia legalności, skuteczności i staranności działania, a także z punktu widzenia ostrożności gospodarczej. Wyjaśnia również, że zgodnie z art. 231 ust. 1 i 2 kodeksu karnego, nadużycie władzy przez funkcjonariusza publicznego podczas wykonywania obowiązków służbowych podlega karze trzech lat pozbawienia wolności lub dziesięciu lat pozbawienia wolności, jeżeli dany funkcjonariusz działał z zamiarem uzyskania korzyści majątkowej lub osobistej, precyzując, że przepis ten ma zastosowanie do wszystkich funkcjonariuszy publicznych, którzy korzystają z nadzoru.

v. Procedura działania w przypadku zapoznawania się z treścią, używania, przechowywania i niszczenia przechwyconych danych

169. Skarżący utrzymują, że sądy krajowe nie są zaangażowane w procedurę niszczenia niejawnych materiałów pochodzących z nadzoru, które nie są przydatne w dochodzeniu karnym, oraz że przepisy regulujące niszczenie informacji objętych tajemnicą zawodową nie gwarantują, że Policja lub służby specjalne nie będą miały dostępu do takich informacji, które ich zdaniem wymagają większej ochrony. Twierdzą oni, że niszczenie przez Policję i służby wywiadowcze zatrzymanych danych dotyczących komunikacji nie podlega żadnej kontroli ze strony organu niezależnego od służb, które je zgromadziły, dodając, że odpowiednie przepisy nie określają, czy sąd sprawujący kontrolę nad zatrzymywaniem danych dotyczących komunikacji jest uprawniony do nakazania zniszczenia niepotrzebnych lub pozyskanych niezgodnie z prawem danych.

170. Zwracają również uwagę, że jeśli po zakończeniu niejawnego nadzoru właściwe służby państwowe nie zgromadziły żadnych dowodów popełnienia przestępstwa, osoba objęta środkiem nie jest o tym informowana i wskazują, że nie może ona w związku z tym poddać kontroli legalności środka nadzoru. Uznają oni, że taka sytuacja jest sprzeczna z wnioskami zarówno Trybunału Konstytucyjnego zawartymi w decyzji S 2/06 (pkt 72 powyżej), jak i Komisji Weneckiej (pkt 92 powyżej), które ich zdaniem nigdy nie zostały wdrożone przez polski rząd. Odnosząc się do odpowiednich danych statystycznych będących w ich posiadaniu, dodają, że liczba spraw karnych, w których informacje zebrane w ramach nadzoru zostały wykorzystane jako dowód, jest niewielka.

171. Skarżący stwierdzają również, że wszystkie wyrażone przez nich obawy dotyczące braku skutecznego monitorowania niejawnych środków nadzoru zostały potwierdzone przez niedawny skandal związany z

programem „Pegasus”³⁸ w przypadku stosowania którego żadna z domniemyanych ofiar nadzoru nie miała, ich zdaniem, żadnych możliwości sprawdzenia, czy nadzór miała miejsce i czy był zgodny z prawem. Uważają, że sytuacja ta jest kolejnym argumentem przemawiającym za wprowadzeniem obowiązku powiadamiania osoby objętej środkiem nadzoru o objęciu jej nadzorem.

172. Rząd ze swojej strony stwierdza, że elementy uzyskane w ramach operacyjnych środków dochodzeniowych, które nie doprowadziły do wszczęcia postępowania lub nie są istotne dla toczącego się postępowania, są niezwłocznie niszczone przez komisję protokolarną na podstawie decyzji podjętej przez organ Policji, który wystąpił o zezwolenie na zastosowanie przedmiotowych środków. Dodaje, że właściwe organy, a mianowicie komendant główny Policji krajowej i jego odpowiednicy w odpowiednich służbach specjalnych, powinny niezwłocznie zarządzić zniszczenie przez komisję protokolarną materiałów zebranych w drodze nadzoru, które zawierały informacje, o których mowa w art. 178 KPK (zob. pkt 58 powyżej). Zauważa również, że jeżeli służby prowadzące nadzór niejawni zgromadzą dowody uzasadniające wszczęcie postępowania karnego lub mające znaczenie dla toczącego się postępowania karnego, dowody te są przekazywane właściwemu prokuratorowi lub prokuratorowi regionalnemu wraz ze wszystkimi elementami pozyskanymi z operacyjnych czynności dochodzeniowych. Wyjaśnia on, że informacje objęte tajemnicą zawodową (zdefiniowaną w art. 178a KPK [*ibidem*]) są przekazywane prokuratorowi, a następnie sądowi, który zezwolił na nadzór, w celu podjęcia decyzji, co należy z nimi zrobić. Wyjaśnia, że w tej kwestii sąd, orzekając niezwłocznie, zezwala na wykorzystanie w postępowaniu karnym informacji objętych tajemnicą zawodową, jeżeli uzna, że „wymaga tego interes prawidłowego administrowania wymiarem sprawiedliwości” oraz że fakt mający znaczenie dla danego postępowania nie może zostać ustalony za pomocą innych dowodów, a także zarządza zniszczenie informacji, które nie mogą być wykorzystane w postępowaniu karnym lub które są zbędne dla takiego postępowania.

173. Rząd utrzymuje również, że zatrzymywanie danych dotyczących komunikacji przez Policję i służby wywiadowcze podlega ścisłym regulacjom na mocy odpowiednich przepisów.

Stwierdza, że co do zasady dostawcy usług ICT są zobowiązani do zapewnienia właściwym funkcjonariuszom Policji dostępu do tego typu danych. Wyjaśnia, że w celu zapewnienia wewnętrznej kontroli nad tym środkiem nadzoru, szefowie służb specjalnych oraz ich odpowiednicy w krajowych siłach policyjnych i innych agencjach upoważnionych do jego stosowania prowadzą poufne rejestry elektroniczne, w których rejestrowane są wszystkie wnioski o dostęp do danych dotyczących komunikacji. Dodaje, z jednej strony, że dane, o których mowa w art. 20 ca ustawy o Policji (pkt 49 powyżej), które mają znaczenie dla toczącego się postępowania karnego, są przekazywane przez upoważnionych funkcjonariuszy Policji właściwemu prokuratorowi, który decyduje, co należy z nimi zrobić, a z drugiej strony, że dane dotyczące komunikacji, które nie mają znaczenia dla postępowania karnego, są niezwłocznie niszczone przez komisję protokolarną. Przypomina,

³⁸ Organizacje pozarządowe posiadające rozległą wiedzę na temat technicznych aspektów nadzoru poinformowały wiele osób na całym świecie, w tym obywateli Polski, że są ofiarami wysoce inwazyjnego oprogramowania szpiegującego (cyberbroni).

że operatorzy usług ICT są zobowiązani do przechowywania zgromadzonych przez siebie danych dotyczących komunikacji przez okres dwunastu miesięcy.

b) Uwagi interwenientów ubocznych

i. Rzecznik Praw Obywatelskich Rzeczypospolitej Polskiej

174. Rzecznik Praw Obywatelskich (RPO) uważa, że chociaż operacje nadzoru muszą pozostać niejawne, nie powinny być przeprowadzane bez niezależnej kontroli zewnętrznej. Uważa on, że osoby podlegające nadzorowi powinny mieć możliwość kontroli legalności tej nadzoru przez organ niezależny od służb państwowych, które ją stosują, i utrzymuje, że zmiany legislacyjne, o których mowa w punkcie 9, które miały na celu dostosowanie odpowiednich przepisów do standardów określonych przez Trybunał Konstytucyjny, sprawiły, że obowiązujące przepisy jeszcze bardziej naruszają te standardy.

175. Przedstawiając główne elementy, które jego zdaniem budzą obawy co do przedmiotowych przepisów, RPO stwierdza, co następuje: po pierwsze, nie określa ono żadnych maksymalnych limitów czasowych dla dozwolonego nadzoru, a tam gdzie ma to miejsce, limity czasowe są zbyt długie; po drugie, lista przestępstw, w przypadku których można zezwolić na nadzór, jest zbyt szeroka; po trzecie, zasady regulujące wykorzystanie jako dowodów w postępowaniu karnym materiałów objętych tajemnicą zawodową, które zostały uzyskane za pomocą nadzoru, są nieprecyzyjne; po czwarte, służby państwa prowadzącego nadzór mają przez cały czas niemal nieograniczony dostęp do danych dotyczących komunikacji, które – zdaniem tego państwa – nie podlegają żadnej kontroli; po piąte, służby państwowe nie są związane żadnym obowiązkiem powiadamiania osoby objętej nadzorem o podjętym środku; po szóste, osoba objęta nadzorem nie dysponuje żadnymi środkami odwoławczymi, które umożliwiłyby jej, w razie potrzeby, ustalenie istnienia dotyczącej jej nadzoru i poddanie jej kontroli zgodności z prawem. Odnosząc się do odpowiednich statystyk będących w jego posiadaniu, RPO dodaje, że w Polsce liczba wniosków o zezwolenie na nadzór pozostaje wysoka, a odsetek odrzuconych wniosków jest niski. 176. Jest on szczególnie krytyczny wobec ustawy o działaniach antyterrorystycznych, twierdząc, że jest ona nieprecyzyjna i dyskryminuje obcokrajowców. Argumentuje, po pierwsze, że nadzór ustanowiony na mocy ustawy nie podlega żadnej zewnętrznej kontroli, a po drugie, że uprawnienia przyznane szefowi ABW do określenia w drodze poufnego zarządzenia katalogu danych, które nadzorowane przez niego służby mogą gromadzić w trakcie nadzoru, są szerokie. Wyraża zaniepokojenie brakiem środka odwoławczego, który pozwoliłby osobom podlegającym nadzorowi na dokonanie kontroli legalności nadzoru. Wyjaśnia również, że jeśli w następstwie środka nadzoru osoba, która jest przedmiotem nadzoru bez jej wiedzy, zostanie wpisana do rejestru osób podejrzanych o udział w działalności terrorystycznej, dana osoba nigdy nie jest o tym informowana, a zatem nie ma możliwości zażądania sprostowania lub usunięcia informacji zebranych bez jej wiedzy z tego rejestru.

177. Rzecznik Praw Obywatelskich wskazuje również, że art. 168a kodeksu postępowania karnego zezwala organom wszczynającym postępowanie karne na wykorzystanie dowodów zebranych w trakcie bezprawnej nadzoru osoby prywatnej.

ii. Fundacja ePaństwo

178. Interwenient uboczny oświadcza, że specjalizuje się w dziedzinie nowych technologii i działa na rzecz otwartości i przejrzystości danych cyfrowych oraz swobodnego dostępu do nich. W niniejszej sprawie wyraża swoje obawy co do nieadekwatności kontroli, której podlegają polska Policja i służby wywiadowcze, gdy stosują niejawną nadzór. Uważa, że zakres *ratione personae* tego nadzoru jest szeroki, ponieważ oprócz obywateli polskich może on być stosowany wobec cudzoziemców i każdej osoby, która ma z nimi kontakt. Dodaje też, że obecny polski rząd utrzymuje wrogię nastawienie do organizacji pozarządowych zaangażowanych w obronę praw człowieka, a zatem uważa, że są one narażone na większe ryzyko bycia obiektem niejawnego nadzoru.

iii. Fair Trials International

179. Interwenient uboczny Fair Trials International stwierdza, że władze prowadzące dochodzenia w sprawie przestępstw związanych z terroryzmem i niedawnym kryzysem Covid-19 często uciekały się do nadzoru osób pozbawionych wolności w sposób, który uznał za problematyczny w świetle wymogów art. 6 Konwencji. Domaga się on zakazu wykorzystywania przez wspomniane organy dowodów zebranych przez nie z naruszeniem prawa do prywatności osób oskarżonych o popełnienie przestępstwa, argumentując, że obecnie obowiązujące w Polsce przepisy nie zapewniają im wystarczających gwarancji ochrony w tym zakresie. Kładzie szczególny nacisk na potrzebę monitorowania nadzoru zarówno *a priori*, jak i *a posteriori*, biorąc pod uwagę jego inwazyjny charakter dla osób, które mu podlegają. Uważa, że kontrola środków nadzoru tego typu musi być szczególnie solidna i koniecznie sądowa, określając, że w tym względzie konieczne jest zarówno powiadomienie o tym osoby, która została poddana środkowi, jak i ustanowienie środka odwoławczego umożliwiającego tej osobie sprawdzenie legalności nadzoru. Dodaje, że w przypadku braku w prawie krajowym przepisów regulujących te kwestie, kontrola legalności i zgodności niejawnego nadzoru z zasadą rządów prawa w demokracji oraz z odpowiednimi standardami ochrony prywatności powinna zostać powierzona organowi niezależnemu od służb państwowych wdrażających dany środek.

180. Interwenient uboczny twierdzi również, że ramy prawne nadzoru muszą być jasne, przewidywalne i zapewniać konkretne zabezpieczenia w celu ochrony poufności komunikacji między adwokatami a ich klientami. Opierając się na wynikach swoich badań w tym obszarze, wskazuje, że większość pomocy prawnej dla osób oskarżonych o popełnienie przestępstwa, które są pozbawione wolności, jest obecnie świadczona za pomocą środków komunikacji elektronicznej, co jego zdaniem potwierdza argument, że istnieje potrzeba większej ochrony przed nadużyciami w zakresie przechwytywania tego typu komunikacji.

iv. Międzynarodowa Komisja Prawników (International Commission of Jurists, ICJ)

181. Odnosząc się do standardów dotyczących, odpowiednio, poufności wymiany informacji między prawnikami a ich klientami oraz niejawnego nadzoru osób prywatnych, wynikających z orzecznictwa Europejskiego

Trybunału Praw Człowieka i TSUE, a także z prac różnych organów międzynarodowych, w tym Wysokiego Komisarza ONZ ds. Praw Człowieka i specjalnego sprawozdawcy ds. wolności wypowiedzi Międzyamerykańskiej Komisji Praw Człowieka, interwenient uboczny uważa, że masowy nadzór stanowi obecnie najpoważniejsze zagrożenie, na jakie narażone są jednostki, tym bardziej, że jej zdaniem nie ma wystarczająco silnych zabezpieczeń chroniących jednostki przed niewłaściwym nadzorem. Dodaje, że wszelka komunikacja między adwokatami i ich klientami oraz między działaczami na rzecz praw człowieka powinna być objęta większą ochroną przed nadużywaniem środków nadzoru, biorąc pod uwagę znaczenie przedmiotowej komunikacji dla zainteresowanych osób i dla demokratycznego społeczeństwa jako całości.

v. Naczelna Rada Adwokacka („NRA”)

182. Interwenient uboczny stwierdza, że w wyniku wejścia w życie zmian w odpowiednich przepisach (zob. pkt 9 powyżej) komunikacja każdego adwokata w Polsce, bez wyjątku, może być przechwytywana przez odpowiednie służby państwowe bez żadnego nadzoru, bez wiedzy zainteresowanych stron i bez możliwości zgłaszania przez nie jakichkolwiek nadużyć ze strony tych służb państwowych. Jego zdaniem nie ma wątpliwości, że wysoka wydajność obecnych zasobów technicznych, jakimi dysponuje Policja oraz służby wywiadowcze umożliwia im uzyskiwanie praktycznie nieograniczonych ilości wszelkiego rodzaju informacji o osobach, w tym informacji o życiu prywatnym adwokatów.

183. Utrzymuje, że Policja i służby wywiadowcze przetwarzają informacje zebrane w trakcie nadzoru bez wiedzy osób, których one dotyczą, również w celach operacyjnych, które nie mają nic wspólnego z toczącym się postępowaniem. Wyjaśnia, że jeżeli dane służby państwowe gromadzą informacje objęte tajemnicą zawodową określoną w art. 178 KPK, to – przynajmniej teoretycznie – powinny one zostać przez nie niezwłocznie zniszczone. Jednak jego zdaniem jasne jest, że gdy zainteresowane służby państwowe dowiedzą się o ich treści, niechętnie pozbędą się ich całkowicie. Interwenient uboczny wyraża również zaniepokojenie faktem, że funkcjonariusz prowadzący nadzór jest jedyną osobą, która decyduje o zniszczeniu lub zachowaniu zebranych informacji, uznając, że taka sytuacja nieuchronnie rodzi pytania o poszanowanie poufności wymiany informacji między prawnikami a ich klientami przez odpowiednie służby państwowe.

184. Interwenient uboczny uważa również, że jakość przepisów dotyczących niejawnego nadzoru jest wątpliwa z następujących powodów. Po pierwsze, przedmiotowe przepisy dotyczą ponad pięćdziesięciu przestępstw karanych, w zależności od przypadku, przez polski kodeks karny lub jedną z siedmiu ustaw odnoszących się odpowiednio do właściwych służb policyjnych i wywiadowczych. Po drugie, osoba objęta środkiem nadzoru nie miałaby możliwości upewnienia się, że celem danego nadzoru była ochrona bezpieczeństwa publicznego. Po trzecie, przepisy zezwalające na nadzór osób prywatnych na podstawie „podejrzenia”, że popełniły one przestępstwo, byłyby nieprecyzyjne i zachęcałyby do arbitralnego stosowania takich środków przez właściwe organy. Po czwarte, przepisy określające prawo uprawnionych organów państwowych do prowadzenia nadzoru w sytuacji, gdy inne metody dochodzenia okazały się nieskuteczne z punktu widzenia realizowanego przez nie celu lub są bezużyteczne, również są na tyle

nieprecyzyjne, że dają tym organom praktycznie nieograniczoną swobodę w tym zakresie.

185. Wreszcie, interwenient uboczny uważa, że zakres uprawnień sądów w postępowaniach mających na celu kontrolę służb państwowych stosujących nadzór jest niewystarczający. Argumentuje on, że niszczenie danych zebranych w ramach nadzoru prowadzonego w zastosowaniu przepisów dotyczących sytuacji niecierpiących zwłoki nie podlega żadnej zewnętrznej kontroli ze strony zainteresowanych służb państwowych, dodając, że to samo dotyczy zebranych danych, które podlegają tajemnicy zawodowej adwokatów.

vi. Privacy International, Article 19 i Electronic Frontier Foundation

186. Organizacje będące interwenientami uważają, że dotychczasowe rozróżnienie między zatrzymywaniem danych dotyczących komunikacji, z jednej strony, a przechwytywaniem danych dotyczących treści komunikatów, z drugiej strony, w odniesieniu do stopnia ingerencji nadzoru w sferę prywatną docelowych osób, nie jest już istotne. Uważają one, że pierwsza z tych form nadzoru jest podobna do masowego nadzoru i dlatego powinna być zawsze otoczona wystarczająco solidnymi gwarancjami, aby chronić jednostki przed możliwymi nadużyciami. Ich zdaniem bezpośredni i nieograniczony dostęp do danych dotyczących komunikacji przez odpowiednie służby państwowe stanowi bardzo daleko idącą ingerencję w sferę prywatną osób objętych tym środkiem. Dlatego ich zdaniem konieczne jest zapewnienie, aby ta szczególna forma nadzoru była stosowana wyłącznie w sytuacjach wyraźnie przewidzianych przez prawo i z zastrzeżeniem uprzedniej zgody organu niezależnego od służb stosujących dany środek. Dodają, że minimalne zabezpieczenia przed możliwymi nadużyciami w tym obszarze powinny obejmować niezależny, bezstronny i dysponujący odpowiednimi zasobami mechanizm kontroli w celu zapewnienia przejrzystości wprowadzonego nadzoru oraz odpowiedzialności pracowników dopuszczających się nadużyć w stosownych przypadkach.

187. Interwenienci uboczni wskazują również, że w krajach demokratycznych istnieje rosnący konsensus co do wymogu powiadamiania osób podlegających nadzorowi o danym środku, aby mogły one zakwestionować jego zgodność z prawem. Uważają, że wymóg ten powinien podlegać wyjątkom tylko w przypadkach, w których powiadomienie mogłoby zagrozić celowi nadzoru lub zagrozić życiu innych osób. Ponadto, ich zdaniem, biorąc pod uwagę możliwy hamujący wpływ nadzoru na społeczeństwo obywatelskie, wszystkie organizacje pozarządowe bez wyjątku powinny korzystać z ochrony przed nadużyciami nadzoru podobnej do tej, z której korzystają adwokaci i dziennikarze.

vii. Specjalny sprawozdawcy ONZ ds. promowania i ochrony praw człowieka i podstawowych wolności podczas walki z terroryzmem („Specjalny sprawozdawca”)

188. Specjalny Sprawozdawca wyjaśnia, że w ramach swoich obowiązków prowadzi regularny dialog z agencjami wywiadowczymi i służbami bezpieczeństwa. Stwierdza, że przedłożył Radzie Praw Człowieka kilka

sprawozdań,³⁹ w tym zestawienie dobrych praktyk w zakresie monitorowania oraz ram i środków prawnych i instytucjonalnych, w tym nadzoru, które uważa za istotne dla zapewnienia poszanowania praw człowieka przez służby wywiadowcze w walce z terroryzmem⁴⁰.

189. Specjalny Sprawozdawca zauważa, że szybkie tempo rozwoju technologicznego, które umożliwia coraz większej liczbie ludzi na całym świecie korzystanie z nowych technologii informacyjnych i komunikacyjnych, ułatwia również władzom publicznym, firmom i osobom prywatnym monitorowanie, przechwytywanie i gromadzenie danych, co może prowadzić do naruszeń praw człowieka, w szczególności prawa do prywatności. Dodaje, że tendencja do „danyfikacji” (*datafication*), tj. powszechnego i zakrojonego na szeroką skalę wykorzystywania gromadzenia danych w ramach pracy służb wywiadowczych, stwarza wyraźne wyzwania w zakresie praw człowieka i praworządności.

190. Specjalny Sprawozdawca uważa, że ze względu na rosnące znaczenie wywiadu i niejawnego charakteru nadzoru, konieczne jest wprowadzenie mechanizmu kontroli obejmującego każdy etap procesu stosowania tego rodzaju środków, aby zapobiec możliwym naruszeniom praw człowieka. Uważa, że przedmiotowy mechanizm powinien być niezależny od organów odpowiedzialnych za prowadzenie nadzoru i że powinien obejmować sądowe zezwolenie na przedmiotowe środki, powiadomienie zainteresowanych osób a posteriori oraz środek zaradczy umożliwiający osobom, których prawa zostały naruszone w wyniku zastosowania środka, uzyskanie odszkodowania za poniesioną szkodę. Określa również, że środkiem nadzoru wprowadzonym w odniesieniu do przedstawicieli zawodów prawniczych lub organizacji społeczeństwa obywatelskiego i bez ich wiedzy powinny towarzyszyć szczególnie silne gwarancje ochrony przed możliwymi nadużyciami ze strony agencji wywiadowczych.

191. Wreszcie, Specjalny Sprawozdawca uważa, że powiadamianie a posteriori o środkach nadzoru osób, które są ich przedmiotem, jest najwłaściwszym sposobem zarówno umożliwienia danej osobie obrony przed organami, które je zastosowały, jak i umożliwienia organom nadzorującym te organy właściwego wykonywania ich obowiązków w tym obszarze. Odnosząc się w tym względzie do odpowiednich konkluzji Agencji Praw Podstawowych Unii Europejskiej,⁴¹ wskazuje, że w sześciu państwach członkowskich UE osoby objęte nadzorem są informowane o nadzorze a posteriori, a w dziewiętnastu innych państwach członkowskich obowiązek powiadomienia istnieje pod pewnymi warunkami, podobnie jak prawo osoby objętej nadzorem do dostępu do informacji zebranych bez jej wiedzy w ramach danego środka.

c) Ocena Trybunału

i. Kontrola operacyjna

³⁹ A/HRC/10/3

⁴⁰ A/HRC/14/46

⁴¹ „Inwigilacja prowadzona przez służby wywiadowcze: środki zabezpieczające prawa podstawowe oraz środki prawne dostępne w Unii Europejskiej” z 6 listopada 2015; „Inwigilacja prowadzona przez służby wywiadowcze: środki zabezpieczające prawa podstawowe oraz środki prawne dostępne w Unii Europejskiej – tom II: sytuacja w terenie i zmiany prawne” z 20 października 2017.

α) Zasady ogólne

192. Ogólne zasady dotyczące kwestii, kiedy niejawne środki nadzoru, w tym przechwytywanie komunikacji, mogą być uzasadnione na podstawie art. 8 ust. 2 Konwencji, zostały szczegółowo określone w wyroku w sprawie *Roman Zakharov* (cytowanym powyżej, ust. 227–34, 236, 243, 247, 250, 257–58, 275, 278 i 287–88). Wiele z tych zasad zostało niedawno powtórzonych – choć w nieco innym kontekście – w wyrokach *Centrum för rättvisa*, ust. 246–53, oraz *Big Brother Watch i Inni*, ust. 332–39, oba cytowane powyżej).

193. Chociaż nie jest konieczne powtarzanie ich wszystkich w tym miejscu, ważne jest, aby podkreślić, że nadrzędnym wymogiem w tym obszarze jest to, że system niejawnego nadzoru musi obejmować skuteczne zabezpieczenia – w szczególności mechanizmy przeglądu i kontroli – które chronią przed nieodłącznym ryzykiem nadużyć i które ograniczają ingerencję, jaką taki system pociąga za sobą w prawa chronione w art. 8 Konwencji, do tego, co jest „niezbędnym środkiem w demokratycznym społeczeństwie”. W takim przypadku, nawet jeśli obowiązujące ustawodawstwo zawiera przepisy ograniczające zakres uprawnień służb państwowych prowadzących niejawną nadzór, może to nie wystarczyć do ograniczenia ryzyka niewłaściwego wykorzystania tej metody dochodzenia przez dane służby państwowe. Z tego powodu istniejące mechanizmy monitorowania operacji nadzoru powinny zostać uzupełnione odpowiednimi mechanizmami zapewniającymi, że odpowiednie służby państwowe nie przekroczą swoich uprawnień w tym obszarze. Chociaż do Trybunału nie należy narzucanie Umawiającym się Państwom precyzyjnych rozwiązań w tej dziedzinie ani orzekanie o stosowności wybranych przez nie technik regulowania tych kwestii, to uważa on za właściwe wskazanie, iż mechanizm monitorowania operacji niejawnego nadzoru powinien opierać się na niezależnym organie monitorującym działającym z własnej inicjatywy i posiadającym niezbędne instrumenty prawne do wykrywania i zwalczania nadużyć. Pożądane byłoby, aby organ kontrolny, o którym mowa, był uprawniony do zapoznawania się ze wszystkimi informacjami, nawet niejawnymi, oraz aby miał uprawnienia dochodzeniowe i niezbędne uprawnienia, w szczególności do nakazania zaprzestania bezprawnego przechwytywania i zniszczenia przechwyconych materiałów uzyskanych lub przechowywanych niezgodnie z prawem (zob. *mutatis mutandis*, *Centrum för rättvisa*, cytowany powyżej, ust. 273).

194. W sprawach takich jak niniejsza, w których skarżący skarżą się abstrakcyjnie na system niejawnego nadzoru, a nie na konkretne przypadki jego stosowania, odpowiednie przepisy i praktyki krajowe muszą być badane w czasie, gdy Trybunał bada dopuszczalność skargi, a nie w czasie, gdy skarga została złożona. Co więcej, ocena tego, czy przedmiotowe przepisy zapewniają skuteczne zabezpieczenia, musi opierać się nie tylko na przepisach w ich obecnym brzmieniu, ale także na (a) faktycznym funkcjonowaniu systemu nadzoru oraz (b) istnieniu lub braku dowodów rzeczywistych nadużyć (zob. *idem*, ust. 151 i 274 oraz *Big Brother Watch i inni*, ust. 270 i 360, oba cytowane powyżej).

β) Zastosowanie do omawianego przypadku

195. Trybunał odwołuje się do swojego powyższego ustalenia (pkt 146), że samo istnienie ustawodawstwa skarżonego przez skarżących stanowi samo

w sobie ingerencję w wykonywanie przez zainteresowane osoby ich praw wynikających z art. 8 Konwencji. Zauważa, że w Polsce środki kontroli operacyjnej są regulowane przez szereg ustaw, w tym ustawę regulującą działalność Policji i innych służb specjalnych państwa. Zauważa, że strony nie kwestionują, że przedmiotowe środki nadzoru jako takie mają podstawę w prawie krajowym, ani że odpowiednie przepisy zostały oficjalnie opublikowane i są publicznie dostępne. Odnosząc, w związku z tym, argument przedstawiony przez skarżących dotyczący braku dostępności niektórych przepisów regulujących środki przechwytywania, Trybunał uważa, po pierwsze, że przedmiotowy argument jest niewystarczająco uzasadniony (zob. pkt 147 powyżej; dla rozumowania a contrario, zob. *Roman Zakharov*, cytowany powyżej, ust. 180 i 241–242), a po drugie, że nie ma potrzeby dalszego jego badania, ale że należy raczej skupić się na wymogach „przewidywalności” i „niezbędności”. Ponadto dla Trybunału jest jasne, że środki nadzoru dozwolone na mocy polskiego prawa służą uzasadnionym celom, takim jak między innymi zapobieganie przestępstwom, ochrona bezpieczeństwa narodowego, bezpieczeństwa publicznego i dobrobytu gospodarczego kraju. Pozostaje zatem sprawdzić, czy prawo krajowe zawiera wystarczające i skuteczne gwarancje i zabezpieczenia, aby spełnić wymogi „przewidywalności” i tego co „niezbędne w społeczeństwie demokratycznym”.

196. Trybunał oceni zatem kolejno zakres i czas trwania niejawnych środków nadzoru, procedury, których należy przestrzegać przy przechowywaniu, konsultowaniu, badaniu, wykorzystywaniu, przekazywaniu i niszczeniu przechwyconych danych, procedury wydawania zezwoleń, ustalenia dotyczące monitorowania stosowania niejawnych środków nadzoru, ewentualne istnienie mechanizmu powiadamiania oraz środki odwoławcze dostępne na mocy prawa krajowego (*Roman Zakharov*, cytowany powyżej, ust. 237–238).

– Zakres stosowania środków niejawnego nadzoru

▪ Zakres stosowania ratione materiae niejawnego nadzoru

197. Trybunał powtarza, że prawo krajowe musi określać zakres niejawnych środków nadzoru poprzez zapewnienie obywatelom odpowiednich wskazówek co do okoliczności, w których władze publiczne mogą odwołać się do takich środków – w szczególności poprzez zdefiniowanie kategorii osób, które mogą być podsłuchiwane oraz poprzez jasne określenie charakteru przestępstw, które mogą stanowić podstawę nakazu przechwytywania (*Roman Zakharov*, cytowany powyżej, ust. 243). Podkreśla, że kryterium przewidywalności nie wymaga jednak od państw wyczerpującej listy takich przestępstw. Z drugiej strony, muszą one dostarczyć wystarczających szczegółów co do ich charakteru (*Kennedy przeciwko Zjednoczonemu Królestwu*, [nr 26839/05, 18 maja 2010] ust. 159, *Zakharov*, ust. 244, cytowane powyżej).

198. W niniejszej sprawie Trybunał zauważył, że zakres ratione materiae tajnej nadzoru, określony w zaskarżonych przepisach, został ustalony odmiennie dla każdej ze służb państwowych odpowiedzialnych za prowadzenie tej nadzoru. Jak wynika z odpowiednich przepisów, zauważa, że zakres niejawnego nadzoru jest szeroki. Jeśli chodzi w szczególności o prawo dotyczące Policji krajowej, Trybunał zauważył, że przedmiotowe

prawo zawiera listę przestępstw, które mogą stanowić podstawę do tajnej nadzoru. Zauważa jednak, że ustawa zezwala na nadzór w przypadku bardzo szerokiego zakresu przestępstw, w tym stosunkowo drobnych przestępstw. Trybunał przypomina w tym kontekście, że monitorowanie treści komunikacji jest dopuszczalne tylko w odniesieniu do najpoważniejszych przestępstw (zob. *mutatis mutandis*, *Roman Zakharov*, ust. 245, *Ekimdzhiiev i inni*, ust. 299, *Kennedy* ust. 159 i *Klass i inni*, ust. 51, wszystkie cytowane powyżej). Odnosząc się do ustaleń zawartych we wspomnianej opinii Komisji Weneckiej, Trybunał zauważył, że organ ten doszedł do podobnych wniosków, wskazując władzom krajowym, że zakres *ratione materiae* nadzoru powinien być ograniczony do najgroźniejszych przestępstw.

199. Trybunał zauważył, że katalog przestępstw, w odniesieniu do których może być prowadzona kontrola operacyjna, został określony przez ustawodawcę za pomocą różnych technik legislacyjnych: poprzez wskazanie konkretnych fragmentów ustaw karnych, poprzez określenie typów przestępstw, których to dotyczy, a niekiedy poprzez odesłanie do całych rozdziałów lub ustaw szczególnych, w których przestępstwa te zostały określone. Uważa, że nie do niego należy stwierdzenie, która technika redagowania przepisów jest najbardziej odpowiednia do uregulowania przedmiotowych kwestii. Uważa, że najważniejsze jest, aby przepisy określające listę przestępstw, w przypadku których można wprowadzić niejawną nadzór, były wystarczająco przewidywalne w ich stosowaniu i sformułowane w taki sposób, aby władze krajowe mogły wszcząć przedmiotowy środek tylko w przypadku wystarczająco poważnych przestępstw. Jak wynika z konkluzji wyroku Trybunału Konstytucyjnego K 23/11 (cytowanego powyżej), Trybunał zauważył, że polski ustawodawca posługiwał się niekiedy bardzo ogólnymi sformułowaniami, do tego stopnia, że przypadki, w których władze mogłyby odwołać się do takiego środka w praktyce, mogłyby prowadzić do nieporozumień. Zauważa, że w wyniku ustaleń Trybunału Konstytucyjnego niektóre przepisy ustawy o ABW określające katalog przestępstw, w odniesieniu do których nadzór może być prowadzona przez przedmiotową agencję, zostały uchylone ze względu na brak jasności, a niektóre z podobnych przepisów ustaw odnoszących się do innych przedmiotowych służb państwowych zostały uznane za zgodne z Konstytucją, z zastrzeżeniem interpretacji zgodnie z wytycznymi określonymi przez Trybunał Konstytucyjny.

200. Trybunał stwierdził już, że brak precyzji co do sposobu interpretacji kluczowych pojęć przepisów dotyczących niejawnego nadzoru jest problematyczny (*ibidem*). Jednocześnie Trybunał przypomina, że orzekł, iż wymóg „przewidywalności” prawa nie idzie tak daleko, aby zobowiązywać państwa do przyjęcia przepisów prawnych szczegółowo wymieniających wszystkie sytuacje, które mogą prowadzić do podjęcia decyzji o ustanowieniu tajnej operacji nadzoru (*Szabó i Vissy przeciwko Węgrom*, nr 37138/14, ust. 64, 12 stycznia 2016).

▪ Zakres *ratione personae* niejawnego nadzoru

201. W odniesieniu do kwestii, kto może podlegać tajnemu nadzorowi, Trybunał zauważa, że z ustaleń poczynionych przez Trybunał Konstytucyjny w sprawie K 23/11 (cytowanej powyżej) jasno wynika, że zakres *ratione personae* nadzoru jest szeroki. Podobnie do opinii Komisji Weneckiej (cytowanej powyżej) Trybunał zwraca również uwagę, że kategorie osób,

które mogą być objęte kontrolą operacyjną, nie zostały określone w ustawie, a więc może to być każda osoba fizyczna lub grupa, pod warunkiem, że istnieje prawdopodobieństwo uzyskania w ten sposób informacji przydatnych dla celów nadzoru. W związku z tym Trybunał przypomina, że orzekł, iż środki przechwytywania skierowane do osoby niepodjętej o popełnienie przestępstwa, ale mogącej posiadać informacje o takim przestępstwie, mogą być uzasadnione na podstawie art. 8 Konwencji (zob. *Greuter przeciwko Holandii*, nr 40045/98, 19 marca 1998, oraz *Roman Zakharov*, cytowany powyżej, ust. 245). Zwraca uwagę, że zgodnie z polskim prawem wnioski o zezwolenie na prowadzenie kontroli operacyjnego muszą wyraźnie wskazywać osobę, której dotyczy dany nadzór, co oznacza, że nadzór tego typu jest zawsze ukierunkowany. W związku z tym Trybunał ma na uwadze, że obowiązujące przepisy nie wydają się nakładać żadnych obowiązków co do treści decyzji zezwalającej na nadzór. Uważa jednak, że krąg osób, które mogą podlegać niejawnemu nadzorowi, powinien zostać określony w przedmiotowej decyzji, a organ wydający zezwolenie powinien podać wystarczające uzasadnienie swojej decyzji w tej kwestii.

– *Czas trwania środków niejawnego nadzoru*

202. W niniejszej sprawie Trybunał zauważył, że zgodnie z odpowiednimi przepisami sędzia mógł zezwolić na zastosowanie środka przechwytywania na okres nieprzekraczający trzech miesięcy. Stwierdza również, że możliwe jest przedłużenie go na mocy postanowienia sądu na kolejny okres do trzech miesięcy, jeśli pierwotne powody nadzoru są nadal aktualne. Wskazuje również, że w należycie uzasadnionych przypadkach nadzór może zostać przedłużony przez sąd wyższej instancji na kilka kolejnych okresów, łącznie do dwunastu miesięcy. Ponadto nadzór nie może trwać łącznie dłużej niż osiemnaście miesięcy. Zauważa również, że kontrola operacyjna musi zostać zakończona, gdy tylko ustaną powody, które uzasadniały jej ustanowienie, a najpóźniej na koniec okresu, na który została zatwierdzona. W świetle wszystkich tych czynników Trybunał uważa, że prawo krajowe wyraźnie wskazuje maksymalny okres, po którym wygasa zezwolenie na przechwytywanie, oraz okoliczności, w których takie zezwolenie może zostać przedłużone. Zauważa, że czas trwania operacji przechwytywania może zależeć od szeregu czynników, w tym od powagi przestępstw, w związku z którymi podjęto środek, powagi podejrzeń dotyczących osoby objętej nadzorem oraz ingerencji, jaką dany nadzór pociąga za sobą w wykonywanie przez daną osobę jej praw w sferze chronionej przez art. 8. Uważa jednak, że w świetle niedociągnięć wskazanych poniżej w przedmiotowym modelu niejawnego nadzoru, nie ma potrzeby dalszego badania tej kwestii w niniejszej sprawie.

– *Zatwierdzanie przechwytywania*

203. W odniesieniu do procedur wydawania zezwoleń na nadzór, Trybunał powtarza, że muszą one być w stanie zagwarantować, że niejawny nadzór nie zostanie zarządzony przypadkowo, nieprawidłowo lub bez należytej i odpowiedniej kontroli (*Roman Zakharov*, cytowany powyżej, ust. 257). Rozważając tę kwestię, Trybunał weźmie pod uwagę szereg czynników, w tym w szczególności: służbę właściwą do wydania zezwolenia na nadzór, zakres nadzoru, który ta służba przeprowadza, oraz treść

zezwoleń na przechwytywanie (*idem*). Trybunał przypomina również, że udzielenie zezwolenia przez organ pozasądowy w celu przeprowadzenia podsłuchu telefonicznego może być zgodne z Konwencją (zob. na przykład *Weber i Saravia przeciwko Niemcom* [dec.], nr 54934/00, ust. 115, ECHR 2006-XI, *Klass i inni*, ust. 51, oraz *Kennedy*, ust. 31, wszystkie cytowane powyżej), pod warunkiem, że dany organ jest wystarczająco niezależny od władzy wykonawczej (*Dumitru Popescu przeciwko Rumunii* [nr 2], nr 71525/01, ust. 71, 26 kwietnia 2007). Co więcej, przedmiotowe procedury muszą być badane nie tylko tak, jak istnieją w teorii, ale także tak, jak funkcjonują w praktyce, o ile można to zweryfikować na podstawie wiarygodnych oficjalnych źródeł (*Ekimdzhiev i Inni*, cytowany powyżej, ust. 307).

204. W niniejszej sprawie Trybunał zauważył, że obowiązujące przepisy przewidują zabezpieczenia zapewniające, że niejawni nadzór jest stosowany tylko wtedy, gdy jest to rzeczywiście konieczne. Po pierwsze, tylko ograniczona liczba organów może żądać nadzoru w ramach swoich odpowiednich uprawnień (pkt 33 powyżej). Po drugie, prawo przewiduje formę kontroli wewnętrznej przed złożeniem wniosków o monitorowanie, które muszą pochodzić od szefa danego organu ścigania i zostać uprzednio zatwierdzone przez właściwego prokuratora (dla podobnego rozumowania, patrz *Ekimdzhiev i Inni*, cytowany powyżej, ust. 308). Po trzecie, prawo określa treść wniosku o zezwolenie na nadzór i wymaga podania uzasadnienia (pkt 34 powyżej). Po czwarte i najważniejsze, prawo wymaga, aby kontrola operacyjna została najpierw zatwierdzona przez sędziego. Wyjątkowo, w nagłych przypadkach, Policja może prowadzić nadzór bez takiego zezwolenia, ale będzie musiała go przerwać, jeśli nie uzyska takiego zezwolenia w ciągu pięciu dni od wdrożenia środka, a wszystkie informacje zebrane w tym kontekście będą musiały zostać zniszczone. Trybunał zauważa ponadto, że niektóre istotne aspekty procedury zatwierdzania niejawnego nadzoru zostały szczegółowo zbadane przez Trybunał Konstytucyjny, który stwierdził w tym względzie, że nie było żadnych elementów mogących poddać w wątpliwość skuteczność nadzoru nad tajnym nadzorem na etapie zatwierdzania przedmiotowego środka (zob. pkt 73 powyżej).

205. Trybunał zgadza się z ustaleniami Trybunału Konstytucyjnego, z których wynika, że wymóg uprzedniej zgody sądu na niejawni nadzór stanowi istotną gwarancję ochrony przed nadużyciami ze strony służb państwowych prowadzących przedmiotowy nadzór. Niemniej jednak odnotowano również szereg czynników, które wskazują, że krajowy system zezwalania na niejawni nadzór jest niezgodny z Konwencją.

206. Trybunał przypomina swój pogląd, zgodnie z którym uprawnienie do prowadzenia niejawnego nadzoru nad obywatelami jest dopuszczalne na mocy Konwencji tylko w zakresie ściśle niezbędnym do ochrony instytucji demokratycznych, a organ wydający zezwolenie musi być w stanie ustalić, czy istnieje uzasadnione podejrzenie co do danej osoby, w szczególności musi być w stanie ustalić, czy istnieją podstawy do podejrzenia danej osoby o planowanie, popełnianie lub popełnienie przestępstw lub innych czynów mogących stanowić podstawę do zastosowania środków niejawnego nadzoru, takich jak czyny zagrażające bezpieczeństwu narodowemu. Musi również upewnić się, że żądane przechwycenie spełnia kryterium „niezbędnego w społeczeństwie demokratycznym” określone w art. 8 ust. 2 Konwencji, w szczególności, że jest ono proporcjonalne do uzasadnionych celów, sprawdzając na przykład, czy możliwe jest osiągnięcie zamierzonych celów

za pomocą mniej restrykcyjnych środków (*Klass i Inni*, ust. 51, *Roman Zakharov*, ust. 260, *Stowarzyszenie Integracji Europejskiej i Praw Człowieka i Ekimdzhiev*, nr 62540/00, ust. 79–80, 28 czerwca 2007, oraz *Kennedy*, ust. 31–32, [cytowane powyżej]). Trybunał uważa, że w wyżej wymienionych okolicznościach właściwy organ, przed wydaniem zezwolenia na nadzór, musi zweryfikować istnienie „uzasadnionego podejrzenia” dotyczącego danej osoby, a w szczególności zbadać, czy istnieją przesłanki wskazujące na to, że planuje ona popełnić, popełnia lub popełniła czyny zabronione lub inne czyny mogące stanowić podstawę do zastosowania środków nadzoru. Z materiałów będących w posiadaniu Trybunału nie wynika jednak, by obowiązujące przepisy wymagały od sądu orzekającego w przedmiocie zezwolenia na nadzór weryfikacji istnienia tych elementów w odniesieniu do danej osoby, co zdaniem Trybunału stanowi istotny brak w tych przepisach.

207. Trybunał zauważa, że przepisy zaskarżone przez skarżących nie określają treści zezwolenia na przechwycenie ani nie wymagają od sądu wydającego takie zezwolenie uzasadnienia swojej decyzji, z wyjątkiem przypadków, gdy decyzja jest niekorzystna dla organu ścigania, który się o nią ubiegał (zob. *idem*, ust. 259 i *Ekimdzhiev i Inni*, ust. 309, oba cytowane powyżej, gdzie sądy wydające zezwolenie na stosowanie niejawnego nadzoru były związane, przynajmniej teoretycznie, obowiązkiem uzasadnienia swoich decyzji). Zauważa również, że procedura zatwierdzania niejawnego nadzoru nie jest kontradiktoryjna. W tym względzie Trybunał uznaje, że o ile jest oczywiste, iż charakter niejawnego nadzoru wymaga, aby procedura udzielania zezwolenia była przeprowadzana bez udziału osoby, która jest celem nadzoru, o tyle jedynym sposobem zapewnienia, że sędzia orzekający w przedmiocie wniosku o zezwolenie należycie zbadał zarówno wniosek, jak i dokumenty przedstawione na jego poparcie, oraz że rzeczywiście rozważył, czy przedmiotowy nadzór stanowiłby uzasadnioną i proporcjonalną ingerencję w korzystanie przez daną osobę lub osoby, w tym każdą osobę, na którą taka nadzór mogłaby mieć dodatkowy wpływ, z praw chronionych na mocy Artykułu 8 Konwencji (*Ekimdzhiev i Inni*, cytowany powyżej, ust. 313 i, *mutatis mutandis*, *Dragojević przeciwko Chorwacji*, nr 68995/11, ust. 91–92, 15 kwietnia 2015). Uważa on, że podczas gdy obowiązek ustalenia potrzeby przechwytywania spoczywa na organie wnioskującym, sędzia rozpatrujący wniosek o niejawną nadzór musi zweryfikować podstawy tego środka i udzielić zezwolenia tylko wtedy, gdy jest przekonany, że przechwytywanie jest zgodne z prawem, konieczne i uzasadnione, a ponadto musi to wyjaśnić w uzasadnieniu swojej decyzji. Co prawda, brak uzasadnienia nie może automatycznie prowadzić do wniosku, że sędziowie wydający nakazy nadzoru nieprawidłowo ocenili przedłożone im w tym celu wnioski. Trybunał bierze jednak pod uwagę fakt, że praktycznie wszystkie wnioski o zezwolenie na prowadzenie tajnego nadzoru są składane do Sądu Okręgowego w Warszawie, że większość agencji prowadzących nadzór podlega jurysdykcji tego sądu oraz że liczba wniosków o przechwytywanie zatwierdzonych przez sędziów jest wysoka (zob. pkt 84 powyżej). Uważa, że czynniki te, rozpatrywane w świetle niedociągnięć przedstawionych powyżej w odniesieniu do procedury wydawania zezwoleń na wprowadzenie tajnej nadzoru, mogą prowadzić do wątpliwości co do praktycznych zdolności sędziów do przeprowadzenia skutecznej kontroli sądowej przedmiotowego nadzoru (dla podobnego rozumowania, patrz *Ekimdzhiev i Inni*, cytowany powyżej, ust. 315–317).

208. Trybunał zauważył, że w pilnych przypadkach prokurator może

początkowo zezwolić na zastosowanie środków przechwytywania bez zgody sędziego, pod warunkiem, że sąd wyda zgodę w ciągu pięciu dni. Zauważa, że jeśli nie zostanie udzielone zezwolenie sądowe, nadzór musi zostać natychmiast przerwany, a zebrane materiały muszą zostać zniszczone. W tym względzie zauważa, że w Polsce zastosowanie trybu pilnego jest uzasadnione jedynie ryzykiem utraty dowodów, a nie powagą lub charakterem przestępstwa (zob. a contrario, *idem*, ust. 323, gdzie zastosowanie trybu pilnego było ograniczone do przypadków bezpośredniego niebezpieczeństwa popełnienia poważnego przestępstwa lub zagrożenia bezpieczeństwa narodowego). Zauważa, że obowiązujące przepisy dają władzom znaczną swobodę w określaniu sytuacji, w których uzasadnione jest skorzystanie z pozasądowej procedury nadzwyczajnej, co stwarza ryzyko nadużycia tej procedury i obejścia wymogu uprzedniej zgody. Uważa, że biorąc pod uwagę niebezpieczeństwa, jakie odwołanie się do takiej pozasądowej procedury nadzwyczajnej pociąga za sobą dla sfery prywatnej osoby podlegającej niejawnemu nadzorowi, obowiązujące przepisy powinny zawierać wystarczające zabezpieczenia, aby zapewnić, że jej stosowanie jest oszczędne i ograniczone do należycie uzasadnionych przypadków. Ponadto, chociaż zgodnie z prawem nadzór musi zostać zaprzestany w ciągu pięciu dni, jeśli nie zostanie udzielone zezwolenie sądowe, nie ustalono, czy obowiązujące prawo zawiera wystarczające zabezpieczenia przed wielokrotnym stosowaniem przedmiotowego środka.

209. Jeśli chodzi o zakres badania przeprowadzanego przez sąd wydający zezwolenie, Trybunał zauważył, że w Polsce sąd orzekający o zezwoleniu na wprowadzenie środka nadzoru ma przed sobą jedynie materiał, który służby państwowe ubiegające się o takie zezwolenie przedstawiły mu na poparcie swojego wniosku. W tym względzie wskazuje, że niedostarczenie sądom wszystkich istotnych informacji może pozbawić je uprawnień do ustalenia, czy istnieje wystarczająca podstawa faktyczna dla niejawnych środków nadzoru (zob. *mutatis mutandis*, *Ekhimdzhiiev i Inni*, cytowany powyżej, ust. 30). Jednocześnie powtarza on swój pogląd, że istnieją techniki, które pozwalają pogodzić, z jednej strony, uzasadnione obawy o bezpieczeństwo dotyczące charakteru i źródeł danych wywiadowczych, a z drugiej strony, potrzebę zapewnienia oskarżonemu wystarczających przywilejów wynikających z zasad postępowania (*Roman Zakharov*, cytowany powyżej, ust. 261). W niniejszej sprawie Trybunał zauważa, że sąd orzekający w sprawie zezwolenia na zastosowanie środka niejawnego nadzoru ma możliwość odrzucenia wniosku organu wnioskującego o zezwolenie na zastosowanie przedmiotowego środka, jeżeli uzna, że wniosek jest niewystarczająco uzasadniony. Zauważa również, że decyzja w tym zakresie wydana przez dany sąd nie pozbawia danego organu możliwości ponownego złożenia wniosku po sprawdzeniu, które z posiadanych przez niego informacji powinny lub mogą zostać przekazane sędziemu, aby mógł on ocenić potrzebę wprowadzenia środka nadzoru.

210. Mając na uwadze powyższe rozważania, Trybunał uznał, że procedury wydawania zezwoleń istniejące w prawie polskim, tak jak funkcjonują one w praktyce, są niewystarczające do zapewnienia, że niejawne środki nadzoru są stosowane wyłącznie w rzeczywiście uzasadnionych przypadkach.

– *Procedury przechowywania, zapoznawania się z treścią, sprawdzania, wykorzystywania, przekazywania i niszczenia*

przechwyconych danych

211. Trybunał stwierdza, że polski ustawodawca przewidział w każdej z ustaw regulujących wprowadzenie kontroli operacyjnej przez różne służby policyjne i wywiadowcze ramy zniszczenia informacji zebranych za pomocą tej kontroli, które okazały się zbędne dla osiągnięcia celów realizowanych przez daną służbę państwową. Zauważa, że różne przepisy mające zastosowanie w tym obszarze określają niemal identyczne zasady. W szczególności w odniesieniu do ustawy o Policji Trybunał zauważył, że zgodnie z odpowiednimi przepisami materiały zgromadzone w drodze niejawnego nadzoru, które są zbędne dla jego celu lub nieistotne dla postępowania karnego, muszą zostać niezwłocznie zniszczone przez komisję protokolarną. Zauważa, że podobny obowiązek niszczenia danych zgromadzonych w wyniku kontroli operacyjnego w przypadkach uznanych za pilne jest przewidziany w przypadku nieudzielenia zezwolenia na daną kontrolę. Ponadto Trybunał zauważa, że właściwi urzędnicy przekazują prokuratorowi wszelkie informacje umożliwiające wszczęcie postępowania karnego lub istotne dla toczącego się postępowania.

212. Z posiadanych informacji wynika również, że informacje gromadzone przez służby państwowe prowadzące kontrolę operacyjną są przekazywane właściwym prokuratorom i sądom z zachowaniem przepisów mających zastosowanie do informacji niejawnych. Trybunał zauważa również, że obowiązujące przepisy nakładają na służby państwowe prowadzące tajną nadzór obowiązek prowadzenia ewidencji w formie elektronicznej dokumentów dotyczących tej nadzoru.

213. Trybunał uznaje, że przepisy dotyczące przetwarzania i niszczenia informacji przechwyconych za pomocą kontroli operacyjnej ustanawiają gwarancje ochrony zgromadzonych w ten sposób danych. Zauważa jednak, po pierwsze, że zniszczenie zebranego materiału powierza się urzędnikom służb państwowych prowadzących nadzór, a po drugie, że stosowanie przedmiotowego środka nie podlega żadnej zewnętrznej kontroli niezależnej od zainteresowanych służb państwowych (dla podobnego rozumowania zob. *Association for European Integration and Human Rights i Ekimdjiev przeciwko Bułgarii*, cyt. powyżej, ust. 85, por. także *Klass i Inni*, cyt. powyżej, ust. 20 i 52, gdzie urzędnik posiadający kwalifikacje wymagane do dostępu do wymiaru sprawiedliwości badał zebrane informacje, które mogły zostać wykorzystane zgodnie z prawem przed przekazaniem ich zainteresowanym służbom państwowym, i przystępował do niszczenia wszelkich innych zebranych dokumentów).

– *Przepisy dotyczące monitorowania komunikacji objętej
tajemnicą zawodową*

214. Trybunał zauważa, że skarżący Pietrzak zarzuca, że obowiązujące ustawodawstwo nie zapewnia wystarczającej ochrony tajemnicy zawodowej adwokatów.

215. W tym względzie Trybunał wskazuje, że podczas gdy art. 8 chroni poufność wszelkiej „korespondencji” między osobami fizycznymi, zapewnia on większą ochronę wymianom między prawnikami a ich klientami. Jest to uzasadnione faktem, że prawnikom powierzono podstawową w każdym społeczeństwie misję, a mianowicie obronę stron procesowych. Jednakże prawnik nie może wykonywać tego podstawowego zadania, jeżeli nie jest w

stanie zagwarantować osobom, których broni, że ich wymiana informacji pozostanie poufna (*mutatis mutandis Michaud przeciwko Francji*, nr 12323/11, ust. 118, ECHR 2012, oraz *R.E. przeciwko Zjednoczonemu Królestwu*, nr 62498/11, ust. 131, 27 października 2015).

216. W swoim orzecznictwie Trybunał określił zatem szereg minimalnych gwarancji, które powinny zostać określone w prawie w celu uniknięcia nadużyć władzy w przypadkach, gdy materiały prawnie chronione tajemnicą zawodową zostały zebrane za pomocą niejawnych środków nadzoru (*Dudchenko przeciwko Rosji*, nr 37717/05, ust. 105, 7 listopada 2017).

217. Po pierwsze, prawo musi jasno definiować zakres tajemnicy adwokackiej oraz określać, w jaki sposób, na jakich warunkach i przez kogo należy dokonywać rozróżnienia między dokumentami chronionymi i niechronionymi. Biorąc pod uwagę, że poufne relacje między prawnikami a ich klientami są szczególnie wrażliwym obszarem, który bezpośrednio dotyczy prawa do obrony, niedopuszczalne jest powierzenie tego zadania członkowi władzy wykonawczej bez nadzoru niezawisłego sędziego (*Kopp przeciwko Szwajcarii*, 25 marca 1998, ust. 73 i 74, Zbiór Orzeczeń 1998 II).

218. Z drugiej strony, przepisy dotyczące badania, wykorzystywania i przechowywania zebranych materiałów, środki ostrożności, które należy podjąć przy przekazywaniu ich innym stronom oraz okoliczności, w których nagrania mogą lub muszą zostać usunięte lub zebrane materiały zniszczone, muszą zapewniać wystarczające gwarancje ochrony materiałów objętych tajemnicą zawodową (*R.E.*, cytowany powyżej, ust. 138–39).

219. W niniejszej sprawie Trybunał zauważył, że we wspomnianym wyżej wyroku Trybunału Konstytucyjnego K 23/11 stwierdzono, iż przepisy dotyczące kontroli operacyjnej, w brzmieniu obowiązującym w danym czasie, są sprzeczne z Konstytucją w zakresie, w jakim nie zapewniają żadnej gwarancji ochrony poufności wymiany informacji przez osoby, którym powierzono tajemnicę zawodową. Trybunał zauważył, że Trybunał Konstytucyjny orzekł również, z jednej strony, że nadzór nad komunikacją między prawnikami a ich klientami nie jest zakazany *per se* i że taki absolutny zakaz jest ponadto niepożądany, a z drugiej strony, że konieczne jest jednak, aby przedmiotowemu nadzorowi towarzyszyły odpowiednie zabezpieczenia w celu ochrony przed niewłaściwym wykorzystaniem lub niewłaściwym gromadzeniem przez służby państwowe prowadzące niejawną nadzór informacji objętych tajemnicą zawodową. Trybunał zauważył, że zdaniem Trybunału Konstytucyjnego gwarancje te powinny obejmować co najmniej mechanizm prewencyjnej kontroli sądowej treści potencjalnie objętych tajemnicą adwokacką, który jest w stanie zapewnić zniszczenie danych, które muszą pozostać poufne w tym zakresie.

220. Trybunał zauważył, że w przeciwieństwie do niektórych przepisów krajowych badanych przez niego w przeszłości (zob. na przykład *Dudchenko*, cytowany powyżej, ust. 108–110), polskie przepisy dotyczące niejawnego nadzoru przed lub poza postępowaniem karnym, w obecnym brzmieniu, określają zasady postępowania z informacjami objętymi tajemnicą zawodową. W szczególności w odniesieniu do ustawy o Policji Trybunał odniósł się do art. 19, który określa, co należy zrobić z informacjami wchodzącymi w zakres przedmiotowego przywileju. Jak wynika z brzmienia tego przepisu prawnego, Trybunał zauważył, że wprowadza on rozróżnienie między, z jednej strony, informacjami, które korzystają z ochrony bezwzględnej tajemnicy zawodowej, do której uprawnieni są obrońcy i duchowni, a z drugiej strony, informacjami, które korzystają z mniejszej ochrony przedmiotowej tajemnicy,

jak w przypadku notariuszy, adwokatów i radców prawnych (z wyjątkiem obrońców), mediatorów i dziennikarzy.

221. Trybunał zauważa, że warunki materialne, od których zależy możliwość prowadzenia przez Policję tajnego nadzoru komunikacji między prawnikami a ich klientami, są takie same jak te, które mają zastosowanie do tajnego nadzoru wszystkich osób fizycznych (dla podobnego rozumowania, patrz *Dudchenko*, ust. 108, oraz *Ekimdzhiiev i Inni*, ust. 333, oba cytowane powyżej). Zauważa, że obowiązujące przepisy nakładają na właściwych funkcjonariuszy Policji obowiązek niszczenia informacji chronionych bezwzględną tajemnicą zawodową. Jednocześnie wskazuje, że przedmiotowe przepisy nie zakazują tajnego nadzoru adwokatów. Przywołując ustalenia, podsumowane powyżej, dokonane przez Trybunał Konstytucyjny w wyroku K 23/11, Trybunał zauważa, że Konwencja nie wymagała od Umawiających się Państw zakazu wszelkiego nadzoru komunikacji między aresztowanym a jego adwokatem. Wskazuje jednak, że poufność takiej komunikacji jest podstawowym prawem jednostki i bezpośrednio wpływa na prawo do obrony. Dlatego odstępstwo od tej zasady może być dozwolone tylko w wyjątkowych przypadkach i musi być otoczone odpowiednimi zabezpieczeniami przed nadużyciami (zob. *mutatis mutandis*, *Erdem przeciwko Niemcom*, nr 38321/97, ust. 65, ETPC 2001 VII).

222. Trybunał uważa zatem, że co do zasady kontrola komunikacji objętej bezwzględną tajemnicą zawodową powinna być dozwolona tylko w wyjątkowych sytuacjach, takich jak te, w których istnieją wiarygodne przesłanki, że adwokat jest współsprawcą szczególnie poważnego przestępstwa lub wykroczenia, a podsłuchiwanie jego rozmów z klientem jest jedyną możliwą metodą dochodzenia w śledztwie (por. *Erdem*, cytowany powyżej, ust. 62, sprawa, w której odstępstwa od zasady poufności korespondencji między aresztowanym a jego obrońcą były dozwolone tylko w bardzo szczególnym kontekście zwalczania przestępstw terrorystycznych, *Mulders przeciwko Holandii* [dec.], nr 23231/94, 6 kwietnia 1995, w którym stosowanie niejawnych środków nadzoru wobec adwokatów było dozwolone tylko w nagłych przypadkach i gdy sam adwokat był podejrzany o współudział w przestępstwach, w przypadku których prawo zezwalało na zastosowanie tymczasowego aresztowania, albo wyrok w sprawie *R.E.*, cytowany powyżej, ust. 132, w którym uzyskanie przez policję informacji objętych tajemnicą zawodową adwokata było dozwolone tylko w przypadku zagrożenia życia i integralności fizycznej osób lub bezpieczeństwa narodowego oraz gdy nadzór mógł dostarczyć właściwym służbom państwowym informacji niezbędnych do zwalczania wspomnianych zagrożeń). Uważa również, że w takich okolicznościach nadzór nad komunikacją objętą bezwzględną tajemnicą zawodową powinien podlegać uprzedniemu zatwierdzeniu przez zewnętrzny organ niezależny od służb prowadzących dany nadzór, a najlepiej przez sąd.

223. Trybunał zauważa ponadto, że z przepisów art. 19 ust. 15 ustawy o Policji wynika, że decyzja o tym, co należy zrobić z informacjami zebranymi w trakcie niejawnych środków nadzoru, spoczywa przede wszystkim na właściwym funkcjonariuszu Policji. Zauważa w szczególności, że ten ostatni ocenia, czy zebrane w ten sposób informacje są objęte tajemnicą komunikacji między obrońcą a jego klientem i czy w związku z tym powinny zostać niezwłocznie zniszczone, czy też przekazane właściwemu sądowi w celu wydania orzeczenia w sprawach, w których przedmiotowe informacje korzystają z mniejszej ochrony tajemnicy zawodowej. W tym

względnie Trybunał przypomina, że orzekł, iż decyzja o tym, co stanie się z informacjami objętymi zakresem tajemnicy adwokackiej nie powinna, co do zasady, być pozostawiona uznaniu służb państwowych, które je gromadzą, ale powinna zostać powierzona organowi zewnętrznemu niezależnemu od zainteresowanych służb państwowych, najlepiej niezawisłemu sędziemu (w celu uzyskania podobnego rozumowania zob. *Kopp*, cytowany powyżej, ust. 73, gdzie pozostawiono wyspecjalizowanemu urzędnikowi w departamencie prawnym organu administracyjnego, bez jakiegokolwiek kontroli ze strony niezawisłego sędziego, ustalenie, co konkretnie wchodziło w zakres kompetencji prawnika, a co wiązało się z działalnością inną niż działalność doradcy, oraz, a contrario, *Erdem*, cytowany powyżej, ust. 67, gdzie stosowanie środka kontroli korespondencji aresztowanego i jego adwokata było nadzorowane przez niezawisłego sędziego, który nie miał żadnego związku ze śledztwem i który miał zachować w tajemnicy informacje, o których się dowiedział). Trybunał zauważa, że Rzecznik Praw Obywatelskich Rzeczypospolitej Polskiej wyraził podobne obawy w tym względzie, stwierdzając, że chociaż mechanizm selekcji treści objętych tajemnicą adwokacką mógł skutkować zniszczeniem poufnych informacji, nie uniemożliwiał służbom państwowym prowadzącym tajny nadzór zapoznania się z tymi chronionymi treściami (zob. pkt 74 powyżej).

224. Trybunał zauważył, że chronione informacje, które korzystają z mniejszej ochrony tajemnicy zawodowej, są przekazywane sądowi, aby mógł on zdecydować, co z nimi zrobić. Zauważa, że przepisy art. 19 ust. 15 ustawy o Policji również wymagały od sądu dopuszczenia takiego dowodu, jeżeli „jest to konieczne z punktu widzenia systemu sądowego” i jeżeli nie istniały żadne inne środki, za pomocą których można było ustalić fakty. Trybunał zauważa w tym względzie, że Komisja Wenecka w wyżej wymienionej opinii uznała, że pojęcie „konieczności z punktu widzenia systemu sądowego” użyte w przedmiotowych przepisach były na tyle niejasne, że umożliwiały interpretację tajemnicy zawodowej w sposób pozbawiający ją znaczenia. Zauważa, że w wyniku swoich ustaleń w tej kwestii wspomniany organ zalecił polskiemu ustawodawcy rozważenie bardziej rygorystycznych przepisów w tym zakresie. Trybunał wziął również pod uwagę fakt, że RPO wyraził swoje obawy w odniesieniu do tych samych kwestii. W niniejszej sprawie Rząd nie wskazał jednak, w jaki sposób sądy krajowe interpretowały termin „niezbędny z punktu widzenia systemu sądowego”. Trybunał przypomina, że orzekł, iż przepisy dotyczące niejawnych środków nadzoru, które mogą naruszać tajemnicę zawodową adwokatów, powinny spełniać szczególnie rygorystyczne warunki w zakresie jasności i precyzji, aby można je było uznać za „prawo” (por. *Erdem*, cytowany powyżej, ust. 67, gdzie przepisy regulujące kontrolę korespondencji aresztowanego z jego adwokatem zostały uznane za wystarczająco jasne i precyzyjne).

225. W tych okolicznościach Trybunał uznaje, że przepisy dotyczące ochrony tajemnicy zawodowej w operacjach niejawnego nadzoru nie spełniają kryterium przewidywalności prawa.

– Monitorowanie stosowania niejawnych środków nadzoru

226. Trybunał powtarza, że ocena kwestii, czy w prawie krajowym istnieją odpowiednie i skuteczne zabezpieczenia przed możliwymi nadużyciami ze strony organów prowadzących nadzór, zależy w szczególności od organów właściwych do monitorowania nadzoru oraz procedur monitorowania

inicjowania i wdrażania środków ograniczających (*Kennedy*, ust. 154 i *Roman Zakharov*, ust. 232, oba cytowane powyżej). Ponadto, jak Trybunał wskazywał w przeszłości, niejawni nadzór może zostać poddany kontroli na trzech etapach: w momencie jego zarządzenia, w trakcie jego prowadzenia lub po jego zakończeniu. Jeśli chodzi o pierwsze dwa etapy, sama natura i logika niejawnego nadzoru oznacza, że nie tylko nadzór jako taki, ale także kontrola, która mu towarzyszy, muszą być przeprowadzane bez wiedzy danej osoby. Ponieważ dana osoba nieuchronnie zostanie pozbawiona możliwości złożenia skutecznego odwołania lub wzięcia bezpośredniego udziału w jakiegokolwiek kontroli, istotne jest, aby istniejące procedury same w sobie zapewniały odpowiednie i równoważne gwarancje chroniące prawa jednostki. W obszarze, w którym nadużycia są potencjalnie tak łatwe w indywidualnych przypadkach i mogą mieć szkodliwe konsekwencje dla demokratycznego społeczeństwa jako całości, zasadniczo pożądane jest powierzenie funkcji nadzorczej sędziemu, chociaż nadzór przez organ niesądowy może być również uznany za zgodny z Konwencją, jeżeli organ ten jest niezależny od organów prowadzących nadzór i posiada wystarczające uprawnienia i obowiązki do sprawowania skutecznej i stałej kontroli (*Klass i Inni*, ust. 56 oraz *Roman Zakharov*, ust. 275, oba cytowane powyżej).

227. Trybunał przypomina, że w sprawie *Ekimdzhiiev i Inni* (cytowanej powyżej) przy badaniu skuteczności mechanizmu kontroli w odniesieniu do organów prowadzących niejawni nadzór wziął pod uwagę następujące elementy: (a) niezależność organu kontrolnego, jego kompetencje i uprawnienia w odniesieniu do naruszeń (prawo dostępu do wszystkich materiałów i podejmowania działań w celu zaradzenia naruszeniom, a w szczególności nakazania zniszczenia bezprawnie przechwyconych materiałów) oraz (b) otwartość działań organu prowadzącego nadzór na kontrolę publiczną (*ibidem*, ust. 334).

228. Odnosząc się bardziej szczegółowo do wymogu niezależności, Trybunał wziął w poprzednich sprawach pod uwagę sposób powoływania i status prawny członków organu nadzorczego. W szczególności orzekł, że organy składające się z członków Sejmu – zarówno strony rządzącej, jak i opozycji – lub osób posiadających kwalifikacje wymagane do powołania do sądownictwa i mianowanych przez parlament lub premiera są wystarczająco niezależne (zob. na przykład *Klass i inni*, cytowany powyżej, ust. 21 i 56, *Weber i Saravia*, decyzja cytowana powyżej, ust. 24–25 i 117, *Leander przeciwko Szwecji*, 26 marca 1987, Seria A, nr 116, *L. przeciwko Norwegii*, nr 13564/88, decyzja Komisji z 8 czerwca 1990 oraz *Kennedy*, cytowany powyżej, ust. 57 i 166). Z drugiej strony Trybunał stwierdził, że minister spraw wewnętrznych, który nie tylko był mianowany przez władze polityczne i był członkiem władzy wykonawczej, ale także był bezpośrednio zaangażowany w zamawianie specjalnych środków nadzoru, nie był wystarczająco niezależny (*Stowarzyszenie Integracji Europejskiej i Praw Człowieka i Ekimdjiev*, cytowany powyżej, ust. 85 i 87); doszedł do tego samego wniosku w odniesieniu do prokuratora i właściwych prokuratorów niższego szczebla (*Iordachi i Inni przeciwko Mołdawii*, nr 25198/02, ust. 47, 10 lutego 2009, oraz *Roman Zakharov*, cytowany powyżej, ust. 279–284), a także specjalnego organu, którego członkowie mieli kontrolować wnioski o specjalny nadzór pochodzące ze służby, która wcześniej ich zatwierdziła, a niektórzy z nich byli byłymi pracownikami danej służby (*Ekimdzhiiev i Inni*, cytowany powyżej, ust. 339–340).

229. W sprawie *Klass i Inni* (cytowanej powyżej) Trybunał uznał również

za zgodny z Konwencją system kontroli nadzoru składający się z urzędnika służby cywilnej posiadającego kwalifikacje wymagane przez organy sądowe, który przeprowadzał wstępną kontrolę na etapie wykonywania zarządzonych środków, parlamentarnej komisji nadzoru składającej się z pięciu członków parlamentu (w tym przedstawicieli opozycji), a wreszcie niezależnej komisji, która orzekała, z urzędu lub na skutek skargi osoby, która uważała, że jest objęta nadzorem, w sprawie legalności i konieczności środków, które miały zostać uchylone przez właściwego ministra, jeżeli komisja uznała je za niezgodne z prawem. Trybunał przypominał również, że w sprawie *Kennedy* (cytowanej powyżej) zatwierdził system kontroli nad tajną nadzorem, w którym niezależny organ, Investigatory Powers Tribunal, składający się z osób, które zajmowały lub zajmowały wysokie stanowiska sądowe i doświadczonych prawników, był uprawniony do anulowania nakazów przechwytywania, współpracując z Interception of Communication Commissionner, urzędnikiem, który również zajmował lub zajmował wysokie stanowisko sądowe, był uprawniony do anulowania nakazów przechwycenia i wniosków o takie nakazy.

230. W niniejszej sprawie Rząd utrzymuje, że wprowadzenie kontroli operacyjnej podlegało a priori kontroli sądowej w zakresie jej zatwierdzenia i ewentualnego późniejszego rozszerzenia, a ponadto działania służb państwowych prowadzących niejawną nadzór podlegały nadzorowi właściwych prokuratorów, niższej izby parlamentu (Sejmu), komisji sejmowej odpowiedzialnej za służby specjalne oraz NIK.

231. Trybunał zauważa jednak, że z posiadanych przez niego dowodów nie wynika, aby polskie sądy były właściwe do przeprowadzenia wystarczająco szerokiej kontroli przechwytywania. Zauważa w tym względzie, że kontrola sądów nad nadzorem jest ograniczona do początkowego etapu wydawania zezwolenia (dla podobnego rozumowania, patrz *Roman Zakharov*, ust. 274, *Stowarzyszenie Integracji Europejskiej i Praw Człowieka i Ekimdzhiev*, ust. 85 i *Ekimdzhiev i inni*, ust. 337, wszystkie cytowane powyżej). W szczególności wskazuje, że sąd wydający zezwolenie na nadzór nie ma jurysdykcji do ponownego rozpatrzenia wniosku, z wyjątkiem sytuacji, gdy orzeka w sprawie przedłużenia nakazu przechwycenia lub wniosku o zezwolenie z mocą wsteczną na „pilny” nadzór przeprowadzony bez uprzedniego zezwolenia. Zauważa również, że dany sąd nie jest informowany o wynikach przechwytywania, ani nie ma uprawnień do sprawdzenia, czy jakiegokolwiek warunki związane z decyzją o udzieleniu zezwolenia zostały spełnione.

232. Jeśli chodzi o prokuratorów, Trybunał zauważa, że są oni w pewnym stopniu zaangażowani w proces wstępnej kontroli nadzoru, że są informowani o wynikach przechwytywania i na ich wniosek, o jego postępach (zob. pkt 33 i 38 powyżej). Zgadza się zatem, że istnieją ramy prawne, które zapewniają, przynajmniej teoretycznie, pewien stopień kontroli nad środkami niejawnego nadzoru przez prokuratorów.

233. Jednocześnie zauważa, że w przeciwieństwie do organów nadzorczych, o których mowa w punkcie 229 powyżej, prokuratorzy w Polsce podlegają prokuratorowi generalnemu Prokuratury Krajowej, który jednocześnie pełni funkcje ministra sprawiedliwości (zob. pkt 64 powyżej). Już sam ten fakt może zagrozić ich zdolności do sprawowania niezależnej kontroli nad służbami państwowymi stosującymi środki niejawnego nadzoru.

234. Jeśli chodzi o uprawnienia i obowiązki prokuratorów, Trybunał zauważa, że zakres ich kontroli nad operacjami niejawnego nadzoru jest ograniczony.

Chociaż prokuratorzy nadzorujący przechwytywanie muszą być informowani o wynikach kontroli operacyjnej i mogą wymagać od służb prowadzących nadzór przedłożenia im wszelkich dokumentów związanych z danym nadzorem, nie mogą jednak nakazać zniszczenia nielegalnie przechwyconych materiałów (zob. a contrario, *Kennedy*, cytowany powyżej, ust. 168, gdzie wszystkie przechwycone materiały musiały zostać zniszczone, gdy tylko komisarz odpowiedzialny za przechwytywanie komunikacji odkrył, że przechwytywanie było niezgodne z prawem). 235. Jeśli chodzi o komisję sejmową nadzorującą działania służb specjalnych, Trybunał zauważa, że chociaż posiada ona rozległą wiedzę specjalistyczną w tej dziedzinie, jej rola ogranicza się do ogólnego nadzoru nad służbami państwowymi sprawującymi nadzór. W szczególności Trybunał zauważa, że komisja sejmowa nie ma uprawnień nadzorczych nad stosowaniem środków przechwytywania w określonych sytuacjach, ani nie jest uprawniona do podejmowania działań naprawczych, ponieważ nie może cofnąć zezwolenia na przechwytywanie, zatrzymać bezprawnego przechwytywania lub nakazać zniszczenia niewłaściwie zebranych danych (dla podobnego rozumowania, patrz *Ekimdzhiiev i Inni*, cytowany powyżej, ust. 345). Trybunał uznaje, że rozważania te odnoszą się również do kontroli sprawowanej przez Sejm i NIK nad służbami sprawującymi nadzór. W tej kwestii zgadza się z wnioskami Komisji Weneckiej zawartymi w wyżej wymienionej opinii, że system wymagający od Ministra Spraw Wewnętrznych przedkładania Sejmowi i Senatowi rocznego sprawozdania z nadzoru policyjnego nie może zastąpić monitorowania konkretnych operacji nadzoru przez niezależny organ, który jest zaznajomiony z praktykami nadzoru i przechwytywania i nie jest instytucjonalnie związany z policją lub zbyt blisko związany z władzą wykonawczą i organami ścigania lub służbami wywiadowczymi. Uważa, że to samo dotyczy rocznego sprawozdania sporządzanego przez szefa CBA i sprawozdania sporządzanego przez szefa KAS do wiadomości odpowiednio komisji sejmowej nadzorującej służby specjalne i Sejmu, które zawierają jedynie ogólny przegląd działań nadzorczych.

236. Trybunał powtarza, że do Rządu należy wykazanie, za pomocą odpowiednich przykładów, praktycznej skuteczności systemu nadzoru (*Roman Zakharov*, cytowany powyżej, ust. 284). W niniejszej sprawie Trybunał stwierdza, że pozwane państwo nie udowodniło swoich twierdzeń, że kontrola sprawowana przez wyżej wymienione organy nad służbami państwowymi stosującymi niejawnie środki nadzoru była skuteczna. W tym względzie Komisja Wenecka zaleciła Polsce uzupełnienie systemu sądowego zatwierdzania nadzoru o inne gwarancje proceduralne, opowiadając się za systemem automatycznej retrospektywnej kontroli tych operacji przez organ, który byłby niezależny od władzy wykonawczej i służb wywiadowczych. Trybunał uważa, podobnie jak Komisja Wenecka, że pożądane byłoby, aby niezależny organ nadzorczy, oprócz sądowej kontroli operacji nadzoru, był uprawniony do regularnego przeglądu z własnej inicjatywy wszystkich aspektów tych operacji, a w szczególności do weryfikacji legalności i konieczności danego nadzoru oraz zgodności z ograniczeniami określonymi w decyzji o zatwierdzeniu. Uważa również, że taki organ powinien mieć dostęp do wszystkich informacji, które uzna za niezbędne do wypełnienia swojego mandatu i być wyposażony w umiejętności wymagane do wykrywania i powstrzymywania nadużyć.

237. Trybunał uważa, że w przeciwieństwie do systemów monitorowania niejawnych operacji nadzoru rozważanych w pkt 229 powyżej, rozwiązania

obecnie obowiązujące w Polsce nie gwarantują skutecznego i niezależnego monitorowania służb państwowych prowadzących przedmiotowy nadzór. W świetle wskazanych powyżej niedociągnięć Trybunał uważa, że w obecnym kształcie kwestionowany mechanizm nadzoru stosowania środków kontroli operacyjnej nie jest w stanie zapewnić odpowiednich zabezpieczeń przed nadużyciami.

– *Powiadomienie o nadzorze komunikacji i dostępne środki odwoławcze*

238. Trybunał przejdzie teraz do kwestii powiadamiania o przechwytywaniu komunikacji, która jest nierozdzielnie związana ze skutecznością środków odwoławczych, a tym samym z istnieniem skutecznych zabezpieczeń przed nadużyciami uprawnień do nadzoru (*Roman Zakharov*, cytowany powyżej, ust. 234). Trybunał zauważa, że art. 19 ust. 16 ustawy o Policji wyraźnie stanowi, że informacje zebrane w trakcie kontroli operacyjnej przez służby policyjne prowadzące tajną nadzór nie są przekazywane osobie, która była przedmiotem danego nadzoru. Z posiadanych przez nią dowodów wynika również, że w Polsce osoba poddana tajnemu nadzorowi nie jest o nim informowana nawet po jego zakończeniu i nawet wtedy, gdy nadzór nie doprowadził do wszczęcia postępowania karnego. Tymczasem Trybunał wymaga, aby osoba objęta nadzorem została o tym poinformowana w późniejszym terminie, tak aby mogła być zaangażowana w monitorowanie środka. W ten sposób ustanowił on ogólny obowiązek powiadomienia z mocą wsteczną, z zastrzeżeniem odstępstw (*Roman Zakharov*, cytowany powyżej, ust. 288). Chociaż Trybunał przyznaje, że w praktyce nie jest możliwe wymaganie powiadomienia we wszystkich przypadkach, uważa jednak, że pożądane jest powiadomienie osoby, której dane dotyczą, po zniesieniu środków nadzoru i tak szybko, jak to możliwe bez narażania na szwank celu tych środków (*Klass i inni*, cytowany powyżej, ust. 58, *Weber i Saravia*, decyzja cytowana powyżej, ust. 135).

239. Trybunał zauważa, że w sprawie *Stowarzyszenie Integracji Europejskiej i Praw Człowieka i Ekimdjiev* (cytowanej powyżej) orzekł, że brak obowiązku powiadomienia osoby podsłuchiwanej o nadzorze na jakimkolwiek jej etapie był niezgodny z Konwencją, ponieważ pozbawiał zainteresowaną osobę jakiejkolwiek możliwości dochodzenia odszkodowania za bezprawną ingerencję w jej prawa wynikające z art. 8 i sprawiał, że środki odwoławcze dostępne w prawie krajowym były teoretyczne i iluzoryczne, a nie konkretne i skuteczne. Stwierdził zatem, że przedmiotowe ustawodawstwo nie zapewniało istotnego zabezpieczenia przed niewłaściwym stosowaniem specjalnych środków nadzoru (*Stowarzyszenie Integracji Europejskiej i Praw Człowieka i Ekimdjiev*, cytowane powyżej, ust. 90–91). Trybunał doszedł również do podobnego wniosku w odniesieniu do rosyjskiego ustawodawstwa dotyczącego przechwytywania komunikacji za pośrednictwem telefonów komórkowych, ponieważ osoby, których komunikacja została przechwycona, nie były powiadamiane o tym środku w żadnym momencie ani w żadnych okolicznościach, chyba że wszczęto przeciwko nim postępowanie karne lub doszło do niedyskrecji (*Roman Zakharov*, cytowany powyżej, ust. 289). Z drugiej strony, w sprawie *Kennedy* Trybunał orzekł, że brak obowiązku powiadomienia osoby zainteresowanej o środku przechwytywania na jakimkolwiek etapie jego stosowania był zgodny z Konwencją, biorąc pod uwagę fakt, że w Zjednoczonym Królestwie każda osoba, która podejrzała,

że jej komunikacja jest lub była przechwytywana, mogła skierować sprawę do Investigatory Powers Domyte, którego jurysdykcja nie była uzależniona od powiadomienia o przechwytywaniu (*Kennedy*, cytowany powyżej, ust. 167).

240. Trybunał zauważa, że polskie przepisy regulujące niejawną nadzór są podobne do przepisów bułgarskich i rosyjskich, o których mowa powyżej, ponieważ nie przewidują żadnego mechanizmu powiadamiania o takim nadzorze – czy to osoby podejrzanej o udział w nielegalnych działaniach, czy też osoby pośrednio objętej danym środkiem – chyba że przeciwko danej osobie wszczęto postępowanie karne, a przechwycone dane zostały wykorzystane jako dowód w tym postępowaniu. Zauważa, że Trybunał Konstytucyjny dwukrotnie zwracał uwagę ustawodawcy krajowemu na to, co uznał za lukę prawną stanowiącą w tym obszarze naruszenie praw określonych w art. 51 ust. 3 i 4 Konstytucji (gwarantujących prawo dostępu do urzędowych dokumentów i baz danych dotyczących jednostki oraz prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z prawem). Trybunałowi nie wydaje się, aby polski ustawodawca zastosował się do zaleceń skierowanych do niego w tej kwestii przez Trybunał Konstytucyjny, ani też, żeby rząd przedstawił jakiegokolwiek uzasadnienia dla bezczynności ustawodawcy. Ponadto Trybunał zauważa, że Komisja Wenecka w wyżej wymienionej opinii zaleciła Polsce wprowadzenie ogólnego obowiązku wstecznego powiadamiania, z odstępstwami, przez służby państwowe prowadzące nadzór.

241. Trybunał zauważa, że w przedmiotowej sprawie pozwany Rząd uznał, że skarżący – podobnie jak każda osoba, która uważała, że jest obiektem nadzoru – mogli, na podstawie art. 2 ustawy o dostępie do informacji publicznej (pkt 59 powyżej), zwrócić się do szefa lub szefów Policji i służb wywiadowczych o ujawnienie im informacji rzekomo zebranych bez ich wiedzy w trakcie niejawnego nadzoru oraz w przypadku negatywnej decyzji, zaskarżyć ją do sądu administracyjnego. Trybunał nie jest jednak przekonany argumentem Rządu dotyczącym skuteczności przedmiotowych środków odwoławczych. Zauważa, po pierwsze, że dwóch skarżących bezskutecznie skorzystało z pierwszego ze środków odwoławczych wskazanych przez Rząd, a po drugie, że zaskarżenie przedmiotowych decyzji szefów Policji i służb wywiadowczych byłoby prawdopodobnie skazane na niepowodzenie w świetle utrwalonego orzecznictwa Naczelnego Sądu Administracyjnego, zgodnie z którym informacje dotyczące czynności operacyjno-śledczych, zastosowanych metod, funkcjonariuszy, którzy podjęli interwencję oraz danych zgromadzonych za pomocą przedmiotowych czynności podlegają ochronie analogicznej do ochrony danych niejawnych, a zatem mogą zostać ujawnione wyłącznie osobom, które zostały do tego upoważnione.

242. Jeśli chodzi o skargę konstytucyjną, którą zdaniem Rządu skarżący powinni byli wnieść w przypadku, gdyby środki odwoławcze przed organami administracyjnymi i sądami okazały się nieskuteczne, Trybunał uważa za mało prawdopodobne, aby taka skarga okazała się skuteczna w przedmiotowym kontekście. Uznaje on, że nawet zakładając, że skarga konstytucyjna skarżących doprowadziłaby do stwierdzenia niekonstytucyjności przepisu cytowanego przez Rząd, nadal nie umożliwiłoby to zainteresowanym osobom zbadania legalności jakiegokolwiek nadzoru, który mógł ich obejmować.

243. Wreszcie, w zakresie, w jakim Rząd powołał się na możliwość wniesienia przez skarżących powództwa o odszkodowanie na podstawie art.

417¹ kodeksu cywilnego (zob. pkt 68 powyżej), Trybunał, mając na uwadze ustalenia, które poczynił powyżej w odniesieniu do skargi konstytucyjnej, uważa, że zarzuty Rządu dotyczące wspomnianego powództwa, którego wykonanie zależałoby od uprzedniego powodzenia przedmiotowej skargi konstytucyjnej, również mają charakter spekulacyjny.

244. W każdym razie Trybunał zauważa, że w niniejszej sprawie Rząd nie wykazał, za pomocą przykładów zaczerpniętych z orzecznictwa krajowego, że skorzystanie przez skarżących ze środków odwoławczych, na które powołuje się Rząd, umożliwiłoby im ustalenie, że prowadzono wobec nich nadzór, zbadanie zgodności z prawem tego nadzoru oraz uzyskanie odszkodowania w przypadku nadzoru niezgodnego z prawem.

245. Trybunał zauważa również, że Rząd nie wspomina o żadnym innym środku odwoławczym, który jego zdaniem byłby dostępny dla osoby chcącej złożyć skargę na niejawnny nadzór, co prowadzi do wniosku, że nie ma skutecznych środków odwoławczych w tym obszarze. W związku z tym uważa, że pozbawiając osobę, której dotyczy taki środek, skutecznej możliwości zakwestionowania go z mocą wsteczną, prawo krajowe nie zapewnia ważnego zabezpieczenia przed niewłaściwym wykorzystaniem niejawnego nadzoru.

– Wnioski

246. Podsumowując, Trybunał uznaje, że system kontroli operacyjnej w obecnym kształcie w Polsce nie zapewnia odpowiednich i skutecznych zabezpieczeń przed arbitralnością i ryzykiem nadużyć nieodłącznie związanych z każdym systemem nadzoru. W szczególności uważa, że zakres *ratione materiae* i *ratione personae* przepisów dotyczących przedmiotowego nadzoru nie jest określony z wystarczającą precyzją, że całkowity czas trwania nadzoru jest wątpliwy, a zasady dotyczące faktycznego uzasadnienia nadzoru nie są wystarczająco dopracowane. Choć przedmiotowemu systemowi nadzoru faktycznie towarzyszy mechanizm kontroli sądowej *a priori*, Trybunał nie jest przekonany, że procedura wydawania zezwoleń, stosowana w praktyce, jest w stanie zapewnić, że nadzór jest stosowany tylko wtedy, gdy taki środek jest „niezbędny w demokratycznym społeczeństwie”. W tym względzie zauważa w szczególności, że obowiązujące przepisy nie wymagają od sędziego orzekającego w sprawie zezwolenia na nadzór sprawdzenia istnienia „uzasadnionego podejrzenia” w odniesieniu do osoby, której dotyczy dany środek, a w szczególności zbadania, czy istnieją dowody pozwalające podejrzewać, że planuje ona popełnić lub popełniła czyny przestępcze lub inne czyny mogące stanowić podstawę do zastosowania niejawnych środków nadzoru, takie jak czyny zagrażające bezpieczeństwu narodowemu. Uważa, że byłoby pożądane, aby istniejąca procedura udzielania zezwoleń została uzupełniona o inne mechanizmy proceduralne kontroli *a posteriori*, takie jak, w przypadku gdy nadzór nie doprowadził do wszczęcia postępowania karnego, skarga otwarta dla osób zainteresowanych ewentualnym nadzorem, którym mogły być objęte, z możliwością złożenia wniosku o kontrolę sądową i audyt przeprowadzony przez niezależny organ. Zauważa, że w obecnej formie prawo nie wydaje się zawierać żadnych odpowiednich przepisów i zauważa, że prawo nie nakłada żadnego wymogu powiadamiania zainteresowanej osoby, nawet po pewnym czasie i nawet wtedy, gdy nie zagraża to celowi środka nadzoru. Wreszcie, Trybunał uważa, że sporne przepisy nie chronią odpowiednio komunikacji objętej tajemnicą

adwokacką. Wszystkie wyżej wymienione niedociągnięcia prowadzą Trybunał do wniosku, że prawo krajowe nie zapewnia wystarczających zabezpieczeń, aby zapobiec nadmiernemu stosowaniu nadzoru i nadmiernej ingerencji w życie prywatne osób fizycznych, których brak nie jest wystarczająco zrównoważony przez obecny mechanizm kontroli sądowej.

247. Z powodów przedstawionych powyżej Trybunał odrzuca zarzut Rządu dotyczący niewyczerpania krajowych środków odwoławczych i stwierdza, że krajowy system kontroli operacyjnej, jako całość, nie spełnia wymogów art. 8 Konwencji.

ii. Zatrzymywanie (retencja) danych dotyczących komunikacji w celu umożliwienia dostępu do nich przez odpowiednie władze krajowe

a) Zasady ogólne

248. Trybunał wskazał już, że dane abonenta telekomunikacyjnego, dane o ruchu i dane o lokalizacji, rozpatrywane osobno lub łącznie, mogą dotyczyć życia prywatnego zainteresowanych osób (*Ekimdzhiev i inni*, cytowany powyżej, ust. 372). Stwierdził też, że sam fakt przechowywania danych dotyczących życia prywatnego jednostki stanowił ingerencję w rozumieniu art. 8 (*Centrum för rättvisa*, cytowany powyżej, ust. 244). Ponadto Trybunał ustalił, że zatrzymywanie takich danych bez wiedzy osoby, której dane dotyczą, również stanowiło ingerencję w korzystanie przez osobę, której dane dotyczą, z prawa do poszanowania jej korespondencji (zob. cytowany powyżej *Ekimdzhiev i inni*, ust. 373 oraz *Ben Faiza przeciwko Francji*, nr 31446/12, ust. 66–67, 8 lutego 2018). Zauważył również, że późniejsze wykorzystanie przechowywanych informacji było nieistotne (*Amann przeciwko Szwajcarii* [GC], nr 27798/95, ust. 69, ETPC 2000-II). Wreszcie orzekł, że dostęp właściwych organów do przechowywanych w ten sposób danych stanowił dodatkową ingerencję w korzystanie przez osobę, której dane dotyczą, z jej praw chronionych na mocy art. 8 (*Ekimdzhiev i inni*, ust. 376 oraz, *mutatis mutandis*, *Centrum för rättvisa*, ust. 244, oba cytowane powyżej).

249. Trybunał podkreśla, że w wyniku postępu technologicznego w komunikacji elektronicznej w ciągu ostatnich dwóch dekad, taka komunikacja może obecnie ujawniać dużą ilość danych osobowych. Co więcej, każda ingerencja spowodowana pozyskaniem powiązanych danych dotyczących komunikacji jest zwielokrotniona przez masowe przechwytywanie, ponieważ takie dane mogą być teraz analizowane i przeszukiwane, umożliwiając stworzenie intymnego portretu osoby, której dane dotyczą, poprzez monitorowanie jej aktywności w sieciach społecznościowych, przemieszczania się, przeglądania Internetu i nawyków komunikacyjnych oraz poprzez poznanie jej kontaktów (*Centrum för rättvisa*, ust. 256, *Big Brother Watch i inni*, ust. 432, oraz *Ekimdzhiev i inni*, ust. 394, wszystkie cytowane powyżej). Pozyskiwanie powiązanych danych dotyczących komunikacji w kontekście masowego przechwytywania może być tak samo inwazyjne jak pozyskiwanie treści komunikatów, a zatem przechwytywanie i zatrzymywanie takich danych oraz przeprowadzane na nich wyszukiwania muszą być analizowane w świetle tych samych zabezpieczeń, które mają zastosowanie do treści komunikatów, bez konieczności, aby przepisy prawne regulujące przetwarzanie takich danych były identyczne pod każdym względem z przepisami regulującymi

przetwarzanie treści komunikatów (*Big Brother Watch i inni*, ust. 363 i 416, *Centrum för rättvisa*, ust. 277, oraz *Ekimdzhiev i inni*, ust. 394, wszystkie cytowane powyżej).

250. Trybunał powtarza, że w ten sam sposób, ogólnemu zatrzymywaniu danych dotyczących komunikacji przez dostawców usług komunikacyjnych i ich przetwarzaniu przez władze w indywidualnych przypadkach muszą towarzyszyć, *mutatis mutandis*, zabezpieczenia i gwarancje przed nadużyciami podobnymi do tych, które mają miejsce w przypadku niejawnego nadzoru (*Ekimdzhiev i inni*, cytowany powyżej, ust. 395).

251. Ponadto w cytowanym powyżej wyroku *Roman Zakharov*, który odnosił się do innych uzasadnionych celów, takich jak na przykład ochrona bezpieczeństwa narodowego, Trybunał określił mające zastosowanie gwarancje, koncentrując się na mechanizmach powiadamiania i środkach odwoławczych dostępnych na mocy prawa krajowego. Trybunał oparł swoją ocenę zgodności przedmiotowych środków przechwytywania z art. 8 na następujących kryteriach: dostępność prawa krajowego; zakres i czas trwania środków niejawnego nadzoru; procedury, których należy przestrzegać w celu przechowywania, sprawdzania, analizowania, wykorzystywania, przekazywania i niszczenia przechwyconych danych; procedury udzielania zezwoleń; ustalenia dotyczące kontroli stosowania środków niejawnego nadzoru; istnienie mechanizmu powiadamiania; oraz środki odwoławczych dostępne na mocy prawa krajowego (*ibidem*, ust. 238). Wreszcie, badając sprawy dotyczące systemów masowego przechwytywania komunikacji transgranicznej i otrzymywania danych wywiadowczych od zagranicznych służb wywiadowczych (*Big Brother Watch i inni* oraz *Centrum för rättvisa*, oba cytowane powyżej), Trybunał dodatkowo dostosował powyższe kryteria, w tym wymóg, aby prawo krajowe jasno określało podstawy, na których można zezwolić na masowe przechwytywanie, okoliczności, w których można przechwytywać komunikację danej osoby, oraz procedurę, której należy przestrzegać przy udzielaniu zezwolenia na niejawny nadzór.

β) Zastosowanie do omawianego przypadku

252. W niniejszej sprawie Trybunał zauważył, że skarżący zarzucają ustawodawstwu krajowemu, które wymaga od dostawców usług ICT zatrzymywania danych przetwarzanych przez nich w związku ze świadczonymi przez nich usługami telekomunikacyjnymi w celu ewentualnego dostępu do nich i ich przetwarzania przez właściwe służby Policyjne i wywiadowcze.

253. W tym względzie zauważa, że dane, które dostawcy usług ICT są zobowiązani przechowywać, obejmują informacje dotyczące w szczególności wykonanych lub odebranych połączeń telefonicznych, wybieranych numerów, czasu trwania połączeń, położenia geograficznego urządzeń mobilnych, odwiedzanych stron internetowych, połączeń ze stronami internetowymi i adresów e-mail (pkt 46 powyżej). Odwołuje się do swojej uwagi powyżej (pkt 141), że przedmiotowe dane, gdy są powiązane z nadawcą lub odbiorcą komunikacji, umożliwiają stworzenie intymnego portretu osoby, której dane dotyczą, poprzez monitorowanie jej aktywności w sieciach społecznościowych, jej ruchów, przeglądania Internetu i jej nawyków komunikacyjnych oraz poprzez poznanie jej kontaktów (zob. *mutatis mutandis*, *Ekimdzhiev i inni*, ust. 394 oraz *Big Brother Watch i inni*, ust. 342, oba cytowane powyżej). W tych okolicznościach Trybunał uznaje,

że przechowywanie przedmiotowych danych przez upoważnione organy wiąże się z ingerencją w sferę prywatną zainteresowanych osób.

254. Trybunał zauważa, że przedmiotowy środek, choć stosowany przez podmioty prywatne – dostawców usług łączności – został podjęty w ramach wykonania obowiązku ustawowego. W związku z tym Trybunał uznaje, że przedmiotową ingerencję można przypisać władzom krajowym (zob. *mutatis mutandis*, *Ekimdzhev i Inni*, cytowany powyżej, ust. 375).

255. Trybunał odwołuje się do swojej uwagi powyżej (pkt 248), że sam fakt przechowywania danych dotyczących życia prywatnego jednostki stanowi ingerencję w rozumieniu art. 8. Wskazuje również, że dostęp właściwych organów krajowych do takich danych stanowi dalszą ingerencję we wspomniane prawo podstawowe. Te dwa środki powinny być analizowane oddzielnie, ponieważ każdy z nich może wpływać na prawa gwarantowane przez Artykuł 8 Konwencji w różny sposób i w różnym stopniu (zob. *mutatis mutandis*, *Centrum för rättvisa*, ust. 244, *Big Brother Watch i Inni*, ust. 330, oraz *Ehimdzhev i Inni*, ust. 371, wszystkie cytowane powyżej).

256. W niniejszej sprawie Trybunał zauważa, że zgodnie z art. 20c ustawy o Policji, który stanowi przykład *mutatis mutandis* takiego środka dla innych organów, dostawcy usług teleinformatycznych są zobowiązani do przechowywania danych przetwarzanych przez nich w związku ze świadczonymi usługami przez okres dwunastu miesięcy w celu udostępnienia ich właściwym organom Policji do celów „zapobiegania lub wykrywania działalności przestępczej, ratowania życia ludzkiego lub ochrony zdrowia, lub prowadzenia akcji poszukiwawczych i ratowniczych”. Zauważa, że ustawa o Policji nie określa, jakie dane mogą być przechowywane, ale odsyła w tym względzie do innych tekstów dotyczących telekomunikacji, Internetu i usług pocztowych. Wskazuje, że art. 180c ust. 2 ustawy o telekomunikacji (zob. pkt 60 powyżej) wymaga również od właściwych ministrów wydania rozporządzeń określających szczegółowy wykaz danych, które dostawcy usług ICT muszą przechowywać zgodnie z art. 20c ustawy o Policji. Zauważa, że obowiązujące przepisy ustanowiły system nadzoru, w ramach którego wszyscy użytkownicy usług telekomunikacyjnych i internetowych są objęci środkiem zatrzymywania danych związanych z ich komunikacją bez informowania ich o tym. Zauważa, że przypadki, w których Policja i służby wywiadowcze mogą uzyskać dostęp do przechowywanych w ten sposób danych, są sformułowane w sposób ogólny, tak aby służby danego państwa mogły uzyskać dostęp do przedmiotowych danych i przetwarzać je w dowolnym celu przydatnym do wykonywania ich ustawowych obowiązków. Zauważa ponadto, że sporny mechanizm zatrzymywania danych dotyczących komunikacji umożliwia funkcjonariuszom właściwych służb państwowych bezpośredni dostęp do takich danych, bez udziału pracowników dostawców usług ICT, pod warunkiem, że taki dostęp jest przewidziany w poufnej umowie między Policją a dostawcą usług. Wskazuje, że w wyniku takich przepisów służby państwowe mają stały i bezpośredni dostęp do danych dotyczących komunikacji w nieograniczonym zakresie, bez wiedzy operatorów telekomunikacyjnych i bez jakiegokolwiek interwencji z ich strony.

257. W tych okolicznościach, zdaniem Trybunału, oczywiste jest, że ingerencja w korzystanie przez skarżących z prawa do poszanowania ich życia prywatnego, wynikająca z nałożonego na dostawców usług teleinformatycznych obowiązku zatrzymywania danych związanych z ich komunikacją, była poważna. Zauważa, że przedmiotowy środek może

słusznie wywoływać w umysłach zainteresowanych osób poczucie bezbronności i nadmiernego narażenia na osoby trzecie i może mieć negatywny wpływ na skuteczne korzystanie z ich praw podstawowych, w tym prawa do poszanowania ich życia prywatnego i korespondencji oraz prawa do nawiązywania relacji z innymi osobami. W tym względzie Trybunał odsyła do orzecznictwa TSUE przedstawionego w pkt 104–108 powyżej, z którego wynika, że TSUE uważa, iż dane o ruchu i lokalizacji dotyczące łączności elektronicznej, rozpatrywane jako całość, są w stanie umożliwić wyciągnięcie bardzo precyzyjnych wniosków na temat życia prywatnego osób, których dane zostały zgromadzone, oraz że zatrzymywanie takich danych do celów ewentualnego dostępu do nich przez właściwe organy krajowe stanowi ingerencję „o szczególnie poważnym i szerokim charakterze” w korzystanie przez zainteresowane osoby z ich praw podstawowych.

258. Trybunał wskazuje, że w przywoływanej powyżej sprawie *Ekimdzhiiev i Inni* (ust. 394–421), która dotyczyła systemu zatrzymywania danych dotyczących komunikacji podobnego do tego rozpatrywanego w niniejszej sprawie, Trybunał zbadał gwarancje dotyczące dostępu do gromadzonych danych i ich zatrzymywania; nie rozstrzygnął jednak, czy przedmiotowy system zatrzymywania danych jako taki był zgodny z wymogami art. 8. Zauważa jednak, że skarżący w niniejszej sprawie wyraźnie skarżyli się na mający do nich zastosowanie system zatrzymywania danych dotyczących komunikacji i późniejsze wykorzystanie przedmiotowych danych przez służby państwowe uciekające się do środków niejawnego nadzoru (zob. pkt 125 powyżej).

259. Trybunał odwołuje się do zasad określonych w pkt 248–251 powyżej, z których wynika, że prawo krajowe powinno, w ramach minimalnych gwarancji i w sposób odpowiedni dla danej formy nadzoru, określać zakres danego środka nadzoru i przewidywać odpowiednie procedury zatwierdzania lub przeglądu w celu utrzymania go w granicach tego, co jest konieczne do osiągnięcia jednego lub więcej uzasadnionych celów przewidzianych przez władze. W niniejszej sprawie Trybunał, mając na uwadze powagę przedmiotowej ingerencji w korzystanie przez skarżących z ich praw należących do sfery chronionej przez art. 8 Konwencji, jest zdania, że przedmiotowy środek powinien być otoczony podobnymi zabezpieczeniami. Uznaje, że brak w obowiązującym ustawodawstwie przepisów lub mechanizmów mogących dostosować do tego, co jest „niezbędne w społeczeństwie demokratycznym”, zakres ingerencji, na którą skarżą się skarżący, w korzystanie przez nich z praw chronionych na mocy art. 8 Konwencji, sprawia, że sporny system nadzoru jest niezgodny z tym postanowieniem Konwencji.

260. Trybunał zauważa, że przepisy zaskarżone przez skarżących wzbudziły zastrzeżenia zarówno Trybunału Konstytucyjnego, jak i Komisji Weneckiej co do ich zgodności z wymogami „jasności” i „przewidywalności” prawa. Odnosi się również do orzecznictwa TSUE przedstawionego w pkt 104–108 powyżej, z którego wynika, że TSUE uważa, iż system nakładający ogólne i nieodróżnicowane zatrzymywanie danych o ruchu i lokalizacji dotyczących łączności elektronicznej do celów zwalczania poważnej przestępczości nie spełnia wymogu proporcjonalności. Zauważa, że późniejsze orzecznictwo TSUE (pkt 111–112 powyżej) jasno wskazuje, że nawet w kontekście ochrony bezpieczeństwa narodowego, gdzie zatrzymywanie danych dotyczących komunikacji może, pod pewnymi warunkami, zostać nakazane jako środek ogólny i bezkrytyczny, stosowanie

przedmiotowego środka powinno być dozwolone jedynie przez okres, który jest czasowo ograniczony do tego, co jest ściśle konieczne i powinno podlegać niezależnemu nadzorowi.

261. W niniejszej sprawie jest jasne, zdaniem Trybunału, że zaskarżone przez skarżących przepisy nakładają obowiązek ogólnego i masowego zatrzymywania danych dotyczących telekomunikacji, łączności pocztowej i łączności cyfrowej wszystkich użytkowników usług łączności oraz że mają one wpływ na osoby, których dane są zatrzymywane, nawet jeśli nie znajdują się one, nawet pośrednio, w sytuacji mogącej stanowić podstawę wszczęcia postępowania karnego. Trybunał zauważa, że dane przechowywane w ten sposób przez okres dwunastu miesięcy są udostępniane właściwym służbom Policyjnym i wywiadowczym, które mogą uzyskać do nich dostęp i wykorzystywać je w dowolnym celu związanym z wykonywaniem ich ustawowych obowiązków.

262. W tym względzie Trybunał zauważa, że chociaż dostępowi przedmiotowych służb państwowych do danych udostępnionych im przez dostawców usług ICT towarzyszy szereg zabezpieczeń chroniących przed możliwymi nadużyciami, w tym mechanizm kontroli sądowej, zabezpieczenia te są niewystarczające, aby zaradzić wskazanym powyżej niedociągnięciom w systemie zatrzymywania danych dotyczących komunikacji, a zatem nie mogą doprowadzić do zgodności przedmiotowego systemu z wymogami art. 8 Konwencji. Trybunał odnosi się do cytowanego powyżej wyroku TSUE w sprawie *SpaceNet i Telekom Deutschland* (pkt 115 powyżej), w którym europejski sąd najwyższy orzekł, że zatrzymywanie danych o ruchu i danych o lokalizacji oraz dostęp do takich danych stanowią odrębne ingerencje w prawa podstawowe osób, których dane dotyczą, wymagające odrębnego uzasadnienia, oraz że w związku z tym przepisy krajowe zapewniające pełną zgodność z warunkami wynikającymi z orzecznictwa w sprawie dostępu do zatrzymanych danych nie mogą, ze względu na swój charakter, być w stanie ograniczyć ani nawet zaradzić poważnej ingerencji w prawa osób, których dane dotyczą, która wynikałaby z ogólnego zatrzymywania przedmiotowych danych.

263. W niniejszej sprawie Trybunał zauważa, że skarżący zarzucają również, że obowiązujące ustawodawstwo, w zakresie, w jakim przewiduje dostęp Policji i służb wywiadowczych do danych przechowywanych w sposób opisany powyżej, jest sprzeczne z art. 8 Konwencji. W tym względzie Trybunał zauważa, że w przypadku, gdy zatrzymanie danych dotyczących komunikacji nie spełnia wymogów „zgodności z prawem” lub zasady proporcjonalności, tak że jest sprzeczne z art. 8, dostęp do przedmiotowych danych, ich zatrzymanie i jakiegokolwiek przetwarzanie przez władze nie może, z tego samego powodu, być zgodne z art. 8. Trybunał odnosi się w tym względzie do wyroku TSUE w sprawie *Commissioner of An Garda Síochána e.a.* (pkt 114 powyżej), z którego wynika, że TSUE orzekł, iż zatrzymywanie danych o ruchu i lokalizacji dotyczących łączności elektronicznej nie może podlegać ogólnemu i bezkrytycznemu zatrzymywaniu w celu zwalczania poważnej przestępczości, a zatem dostęp do tych danych również nie może być uzasadniony tym samym celem. W niniejszej sprawie Trybunał nie widzi powodu, dla którego miałby odstąpić od wniosków TSUE w tej kwestii.

– Wnioski

264. Z powodów przedstawionych powyżej Trybunał uznaje, że przepisy

krajowe, zgodnie z którymi dostawcy usług ICT są zobowiązani do przechowywania danych dotyczących komunikacji w sposób ogólny i niezróżnicowany do celów ewentualnego dostępu przez właściwe organy krajowe, są niewystarczające, aby ograniczyć ingerencję w korzystanie przez skarżących z ich prawa do poszanowania życia prywatnego do tego, co jest „niezbędne w demokratycznym społeczeństwie”. W związku z tym stwierdza, że doszło do naruszenia art. 8 Konwencji również w odniesieniu do zatrzymywania danych dotyczących komunikacji w celu ewentualnego dostępu do nich przez właściwe organy krajowe.

iii. System niejawnego nadzoru na mocy ustawy o działaniach antyterrorystycznych

265. Trybunał zauważa, że polski ustawodawca przyjął ustawę o działaniach antyterrorystycznych w celu wzmocnienia krajowego systemu zwalczania terroryzmu i ochrony bezpieczeństwa narodowego. Uznaje on, że zgodnie z odpowiednimi przepisami przedmiotowej ustawy funkcjonariusze ABW są uprawnieni do prowadzenia niejawnego nadzoru cudzoziemców podejrzanych o działalność terrorystyczną. Zauważa również, że katalog środków nadzoru, które wspomniani funkcjonariusze mogą zastosować w tym celu, jest określony w art. 9 tej samej ustawy.

266. Trybunał przypomina, że stwierdził, iż demokratyczne społeczeństwa są dziś zagrożone terroryzmem, a zatem państwo musi być w stanie, w celu skutecznego zwalczania tych zagrożeń, potajemnie monitorować elementy wywrotowe działające na jego terytorium. W związku z tym przyjmuje, że istnienie przepisów prawnych przyznających uprawnienia do niejawnego nadzoru korespondencji, przesyłek pocztowych i telekomunikacji jest, w wyjątkowej sytuacji, konieczne w społeczeństwie demokratycznym w interesie bezpieczeństwa narodowego i/lub w celu zapobiegania zakłóceniom porządku lub przestępczości (*Klass i Inni*, cytowany powyżej, ust. 48).

267. Trybunał podkreśla jednak, że Umawiające się Państwa nie mają nieograniczonej swobody w poddawaniu osób podlegających ich jurysdykcji środkom niejawnego nadzoru. Zdając sobie sprawę z niebezpieczeństwa nieodłącznie związanego z takim prawem, podważania, a nawet niszczenia demokracji w imię jej obrony, potwierdza, że nie mogą podejmować żadnych środków, które uznają za stosowne w imię walki ze szpiegostwem i terroryzmem. W związku z tym, niezależnie od wybranego systemu nadzoru, Trybunał musi być przekonany, że istnieją odpowiednie i wystarczające zabezpieczenia przed nadużyciami (idem, ust. 50).

268. Przechodząc do faktów niniejszej sprawy, Trybunał zauważa, że zakres *ratione personae* ustawy o działaniach antyterrorystycznych, choć zasadniczo ograniczony do cudzoziemców, jest w praktyce szerszy, ponieważ pozwala funkcjonariuszom ABW na pośrednie monitorowanie komunikacji każdej osoby, która ma kontakt z osobami będącymi celem nadzoru, niezależnie od tego, czy sama została objęta nadzorem (*Ekimdzhiiev i inni*, cytowany powyżej, ust. 263).

269. Zauważa, że skarżący utrzymują, że sformułowanie kluczowych pojęć w przedmiotowej ustawie, od których zależy zdolność funkcjonariuszy ABW do prowadzenia tajnej nadzoru cudzoziemców, a mianowicie „działalność terrorystyczna”, „incydenty o charakterze terrorystycznym” i „osoby podejrzane o działalność terrorystyczną”, jest szerokie. W tym względzie Trybunał przypomina, że stwierdził już, w kontekście wspomnianej wyżej sprawy *Szabó i Vissy*, która jest podobna do niniejszej

sprawy i dotyczyła przepisów dotyczących operacji niejawnego nadzoru antyterrorystycznego, że potrzeba uniknięcia nadmiernej sztywności i nadążania za zmieniającymi się okolicznościami oznacza, że wiele przepisów jest nieuchronnie formułowanych w mniej lub bardziej niejasny sposób. Jest zatem przekonany, że nawet w dziedzinie niejawnego nadzoru, gdzie przewidywalność ma szczególne znaczenie, przedmiotowe koncepcje wydają się wystarczająco jasne, aby spełnić wymogi legalności. Zdaniem Trybunału wymóg, aby prawo było „przewidywalne”, nie idzie tak daleko, aby zobowiązywać państwa do przyjęcia przepisów prawnych szczegółowo wymieniających wszystkie sytuacje, które mogą prowadzić do podjęcia decyzji o rozpoczęciu operacji niejawnego nadzoru. Odniesienie do zagrożeń terrorystycznych lub akcji poszukiwawczych można zatem zasadniczo uznać za dające obywatelom wymagane wskazówki (*mutatis mutandis Szabó i Vissy*, cytowany powyżej, ust. 64).

270. Trybunał wskazuje jednak również, że w sprawach dotyczących praw podstawowych prawo byłoby sprzeczne z zasadą rządów prawa, jedną z podstawowych zasad społeczeństwa demokratycznego zapisanych w Konwencji, gdyby nie zawierało ograniczeń swobody decyzyjnej przyznanej władzy wykonawczej w sprawach bezpieczeństwa narodowego. W związku z tym ustawodawstwo musi określać zakres i sposób wykonywania takiego uprawnienia z wystarczającą jasnością – biorąc pod uwagę uzasadniony cel – aby zapewnić jednostce odpowiednią ochronę przed arbitralnością (*Roman Zakharov*, ust. 247 oraz *Szabó i Vissy*, ust. 65, oba cytowane powyżej).

271. Trybunał zauważa, że w odniesieniu do niejawnego nadzoru cudzoziemców, art. 9 ust. 1 ustawy o działaniach antyterrorystycznych ustanowił zasady legis specialis w stosunku do przepisów dotyczących tajnej nadzoru zawartych w ustawie o Policji oraz że zezwalał funkcjonariuszom ABW na prowadzenie tajnej nadzoru cudzoziemca przez trzy miesiące bez uprzedniego zezwolenia sądu. Trybunał zauważył ponadto, że z brzmienia przepisów omawianego artykułu wynika, że szef ABW podejmuje decyzję o wprowadzeniu środków nadzoru, a następnie przekazuje swoją uzasadnioną decyzję ministrowi właściwemu do spraw nadzoru nad służbami specjalnymi państwa oraz prokuratorowi generalnemu Prokuratury Krajowej, który może zakończyć stosowanie tych środków.

272. Trybunał orzeka, że „uprawnienia do niejawnego nadzoru obywateli (...) są tolerowane na mocy Konwencji tylko w takim zakresie, w jakim są ściśle niezbędne do ochrony instytucji demokratycznych” (*Klass i inni*, cyt. powyżej, ust. 42). W tym miejscu Trybunał pragnie podkreślić, że ze względu na szczególny charakter przedmiotowej ingerencji i potencjał zaawansowanych technologii nadzoru w zakresie naruszania prywatności obywateli, środek niejawnego nadzoru można uznać za zgodny z Konwencją tylko wtedy, gdy jest on absolutnie konieczny, w ogólnej perspektywie, w celu ochrony instytucji demokratycznych oraz, w szczególnej perspektywie, w celu uzyskania istotnych informacji w kontekście indywidualnej operacji. Zdaniem Trybunału każdy nadzór, który nie spełnia tych kryteriów, może stanowić nadużycie przez władze, które dysponują potężnymi technologiami (*Szabó i Vissy*, cyt. powyżej, ust. 71–73).

273. W niniejszej sprawie Trybunał zauważa, że stosowanie przez funkcjonariuszy ABW środków niejawnego nadzoru wobec cudzoziemców nie podlega, w początkowym trzymiesięcznym okresie, żadnemu zatwierdzeniu ani nadzorowi ze strony niezależnego od nich organu, który

byłby w stanie ograniczyć ich swobodę w odczytywaniu ogólnych formuł stosowanych przez ustawę o działaniach antyterrorystycznych i ustalić, czy w każdym przypadku istniały wystarczające podstawy do przechwytywania komunikacji danej osoby (zob. *mutatis mutandis*, *Roman Zakharov*, cytowany powyżej, ust. 249). Zdaniem Trybunału jest to jedyny sposób, aby zaspokoić potrzebę zapewnienia, że środki nadzwyczajne są stosowane oszczędnie i tylko w należycie uzasadnionych przypadkach (*idem*, cytowany powyżej, ust. 266).

274. Ponadto Trybunał stwierdza, po pierwsze, że funkcjonariusze ABW prowadzą tajną nadzór na podstawie decyzji szefa ABW, przed którym odpowiadają, a po drugie, że taka decyzja szefa ABW podlega nadzorowi prokuratora generalnego Prokuratury Krajowej i ministra właściwego do spraw służb specjalnych państwa. Wskazuje, że interwencja sędziego jest przewidziana tylko w przypadku późniejszego przedłużenia środków nadzoru po upływie początkowego trzymiesięcznego okresu. Zauważa zatem, że ani wprowadzenie niejawnego nadzoru, ani jego stosowanie w tym początkowym okresie nie podlega żadnej kontroli ze strony niezależnego organu zewnętrznego w stosunku do funkcjonariuszy ABW prowadzących przedmiotowy nadzór.

275. Trybunał wskazał już w przeszłości, że zatwierdzanie niejawnych środków nadzoru przez organ niesądowy może być zgodna z Konwencją, pod warunkiem, że dany organ jest wystarczająco niezależny od władzy wykonawczej. Przypomina również, że orzekł, iż w świetle współczesnych zagrożeń terrorystycznych mogą wystąpić sytuacje nadzwyczajne, w których obowiązkowe stosowanie zezwolenia sądowego jest niewykonalne i przyniosłoby efekt przeciwny do zamierzonego ze względu na brak konkretnej wiedzy lub po prostu oznaczałoby stratę cennego czasu (*Szabó i Vissy*, cyt. powyżej, ust. 80). Takie środki muszą jednak podlegać kontroli a posteriori, która jest zazwyczaj wymagana w przypadkach, gdy nadzór został wcześniej zatwierdzony przez organ pozasądowy (*idem*, ust. 81).

276. W niniejszej sprawie Trybunał uznaje, że zatwierdzenie niejawnych środków nadzoru przez szefa ABW, któremu podlegają wykonujący je funkcjonariusze, oraz późniejszy nadzór nad stosowaniem tych środków przez członka władzy wykonawczej o odpowiedzialności politycznej i członka prokuratury, którzy nie dawali odpowiednich gwarancji niezależności od władzy wykonawczej, nie zapewniają niezbędnych zabezpieczeń przed nadużyciami, tym bardziej, że osoby podlegające nadzorowi nigdy nie są o tym informowane i nie mają skutecznych środków kwestionowania legalności prowadzonej wobec nich nadzoru.

277. Trybunał zauważa również, że zgodnie z art. 9 ust. 8 ustawy o działaniach antyterrorystycznych prokurator generalny Prokuratury Krajowej ma prawo zarządzić zniszczenie nieistotnych materiałów. Jednakże, ponieważ obecny prokurator generalny Prokuratury Krajowej jest również ministrem sprawiedliwości, Trybunał uważa, że bezstronność i niezależność prokuratora generalnego Prokuratury Krajowej nie są wystarczająco zagwarantowane.

Wnioski

278. Z powodów przedstawionych powyżej Trybunał stwierdza, że przepisy dotyczące tajnej nadzoru zawarte w ustawie o działaniach antyterrorystycznych również nie spełniają wymogów art. 8 Konwencji.

279. Stwierdza zatem, że doszło do naruszenia tego postanowienia Konwencji.

III. ODNOŚNIE DO DOMNIEMANEGO NARUSZENIA ARTYKUŁU 13 KONWENCJI

280. Skarżący skarżą się na brak skutecznego środka odwoławczego, który umożliwiłby im wniesienie skargi na podstawie art. 8. Powołują się oni na art. 13 Konwencji, który brzmi następująco:

„Każdy, czyje prawa i wolności zawarte w niniejszej konwencji zostały naruszone, ma prawo do skutecznego środka odwoławczego do właściwego organu państwowego także wówczas, gdy naruszenia dokonały osoby wykonujące swoje funkcje urzędowe.”

281. W świetle wniosku, do którego Trybunał doszedł w odniesieniu do art. 8 Konwencji (zob. pkt 246, 264 i 278–279 powyżej), uważa on, że nie ma potrzeby oddzielnego badania skargi na podstawie art. 13, chociaż jest ona ściśle związana ze skargą na podstawie art. 8 i dlatego musi zostać uznana za dopuszczalną (zob. *Liberty i Inni*, cyt. powyżej, oraz *Roman Zakharov*, obydwie cyt. powyżej).

IV. ODNOŚNIE DO STOSOWANIA ARTYKUŁU 41 KONWENCJI

282. Zgodnie z artykułem 41 Konwencji:

„Jeśli Trybunał stwierdzi, że nastąpiło naruszenie Konwencji lub jej protokołów, oraz jeśli prawo wewnętrzne zainteresowanej Wysokiej Układającej się Strony pozwala tylko na częściowe usunięcie konsekwencji tego naruszenia, Trybunał orzeka, gdy zachodzi potrzeba, słuszne zadośćuczynienie pokrzywdzonej stronie.”

A. Odszkodowanie

283. Skarżący nie domagają się żadnego odszkodowania, uważając, że stwierdzenie naruszenia samo w sobie stanowiłoby wystarczającą rekompensatę. Rząd nie ma zastrzeżeń. Trybunał uważa zatem, że nie ma powodu, aby przyznać skarżącym jakąkolwiek kwotę za szkodę majątkową lub niemajątkową.

B. Opłaty i koszty

284. Skarżący Mikołaj Pietrzak wnosi o zwrot kosztów związanych z jego udziałem w rozprawie 26 września 2022 przed Trybunałem oraz udziałem skarżących Wojciecha Klickiego i Barbary Grabowskiej-Moroz, a także ich pełnomocnika, dzieląc je w następujący sposób: 2166,08 zł (459,97 euro) za zakwaterowanie w hotelu dla skarżących Mikołaja Pietrzaka, Wojciecha Klickiego i Barbary Grabowskiej-Moroz oraz ich pełnomocnika, a także 10 196,99 zł (2142,95 euro) za bilety lotnicze dla skarżących Mikołaja Pietrzaka i Wojciecha Klickiego oraz ich pełnomocnika. Skarżąca Barbara Grabowska-Moroz wnosi również o zwrot kwoty 1201,85 zł (252,58 euro) za bilet lotniczy. Wreszcie, skarżąca Dominika Bychawska-Siniarska domaga się

zwrotu kwoty 2479,73 zł (526,48 euro) z tytułu zakwaterowania w hotelu. Skarżący przedstawiają kopie odpowiednich faktur.

285. Rząd nie kwestionuje kwot dochodzonych przez skarżących, z wyjątkiem kwoty dochodzonej przez skarżącą Dominikę Bychawską-Siniarską. W tym względzie stwierdza, że z treści faktury hotelowej przedłożonej przez tę ostatnią jasno wynika, że przedmiotowe zakwaterowanie w hotelu było przeznaczone dla trzech osób. Jednakże na rozprawie przed Trybunałem stawiała się tylko skarżąca.

286. Zgodnie z orzecznictwem Trybunału skarżący może uzyskać zwrot poniesionych kosztów i wydatków tylko wtedy, gdy zostanie wykazane, że zostały one rzeczywiście poniesione, były konieczne i rozsądnej wysokości. W niniejszej sprawie, mając na uwadze przedłożone dokumenty i kryteria określone powyżej, Trybunał przyznaje skarżącym Mikołajowi Pietrzakowi, Barbarze Grabowskiej-Moroz i Dominice Bychawskiej-Siniarskiej następujące kwoty: 2602,92 euro, 252,58 euro i 300 euro tytułem kosztów i wydatków związanych z postępowaniem przed Trybunałem i oddała wniosek złożony w tym zakresie przez skarżącą Dominikę Bychawską-Siniarską.

NA TYCH PODSTAWACH SĄD JEDNOGŁOŚNIE,

1. *Postanawia* połączyć skargi;
2. *Uznaje* skargi za dopuszczalne;
3. *Stwierdza*, że doszło do naruszenia art. 8 Konwencji w odniesieniu do skargi dotyczącej systemu kontroli operacyjnej;
4. *Stwierdza*, że doszło do naruszenia art. 8 Konwencji w zakresie, w jakim skarga dotyczy zatrzymywania danych dotyczących komunikacji do celów ewentualnego dostępu do nich przez właściwe organy krajowe;
5. *Stwierdza*, że doszło do naruszenia art. 8 Konwencji w odniesieniu do skargi dotyczącej systemu niejawnego nadzoru na mocy ustawy o działaniach antyterrorystycznych;
6. *Stwierdza*, że nie ma potrzeby rozpatrywania skargi na podstawie art. 13 Konwencji;
7. *Stwierdza*
 - a) że pozwane Państwo zapłaci, w terminie trzech miesięcy od dnia, w którym orzeczenie stanie się prawomocne zgodnie z art. 44 ust. 2 Konwencji, następujące kwoty, które zostaną przeliczone na walutę pozwanego Państwa po kursie obowiązującym w dniu rozliczenia:
 - i. 2602, 92 euro na rzecz skarżącego Mikołaja Pietrzaka, powiększone o wszelkie kwoty, które mogą być należne od tego skarżącego tytułem podatku, tytułem kosztów i wydatków;
 - ii. 252,58 euro na rzecz skarżącej Barbary Grabowskiej-Moroz, powiększone o wszelkie kwoty, które mogą być należne od tej skarżącej tytułem podatku, tytułem kosztów i wydatków;
 - iii. 300 euro na rzecz skarżącej Dominiki Bychawskiej-Siniarskiej,

- powiększone o wszelkie kwoty, które mogą być należne od tej skarżącej tytułem podatku, tytułem kosztów i wydatków;
- b) że od upływu tego terminu do dnia zapłaty kwoty te będą oprocentowane według stopy procentowej równej stopie oprocentowania kredytów marginalnych Europejskiego Banku Centralnego obowiązującej w tym okresie, powiększonej o trzy punkty procentowe;

8. *Oddala* jednogłośnie pozostałą część roszczenia o słuszne zadośćuczynienie.

Sporządzono w języku francuskim, a następnie ogłoszono na posiedzeniu jawnym w Strasburgu, w Palais des droits de l’homme, 28 maja 2024.

Ilse Freiwirth

Marko Bošnjak

Sekretarz

Przewodniczący

ZAŁĄCZNIK NR 1

Lista skarżących:
Skarga nr 72038/17

Nr	Imię NAZWISKO	Rok urodzeni	Miejsce zamieszkania
1.	Mikołaj PIETRZAK	1973	Warszawa

Skarga nr 25237/18

N r	Imię NAZWISKO	Rok urodzeni	Miejsce zamieszkania
1.	Dominika BYCHAWSKA- SINIARSKA	1982	Warszawa
2.	Barbara GRABOWSKA- MOROZ	1986	Warszawa
3.	Wojciech KLIICKI	1987	Warszawa
4.	Katarzyna SZYMIELEWICZ	1981	Warszawa

ZAŁĄCZNIK NR 2

WŁAŚCIWE PRZEPISY PRAWA REGULUJĄCE DZIAŁALNOŚĆ SŁUŻB PAŃSTWOWYCH STOSUJĄCYCH NIEJAWNY NADZÓR⁴²

I. USTAWA O POLICJI Z 6 KWIETNIA 1990

Artykuł 19

„1. Przy wykonywaniu czynności operacyjno-rozpoznawczych,

podejmowanych przez Policję w celu zapobieżenia, wykrycia, ustalenia sprawców, a także uzyskania i utrwalenia dowodów, ściganych z oskarżenia publicznego,

umyślnych przestępstw:

1) przeciwko życiu, określonych w art. 148–150 Kodeksu karnego (zabójstwo, dzieciobójstwo, eutanazja);

2) określonych w art. 134 (napaść na Prezydenta Rzeczypospolitej), 135 ust. 1 (napaść na Prezydenta lub jego znieważenie), 136 ust. 1 (napaść na głowę obcego państwa lub jej znieważenie), 156 ust. 1 i 3 (ciężkie uszkodzenie ciała), (...) 163 ust. 1 i 3 (zagrożenie życia innych osób), 164 ust. 1 (bezpośrednie zagrożenie), 165 ust. 1 i 3 (inne zagrożenie), 166 (piractwo), 167 (stworzenie niebezpieczeństwa na pokładzie statku lub samolotu lub [posiadanie] substancji niebezpiecznych), 173 ust. 1 i 3 ([spowodowanie] katastrofy na lądzie, na wodzie lub dotyczącej ruchu lotniczego), 189 (bezprawne zatrzymanie), 189a (handel ludźmi), (...) 211a (nielegalna adopcja), 223 (napaść), (...) 228 ust. 1 i 3–5 (łapownictwo bierne), 229 ust. 1 i 3–5 (łapownictwo czynne), 230 ust. 1 (handel wpływami), 230a ust. 1 i 231 ust. 2 (handel wpływami – klauzula nietykalności), 232 (bezprawna przemoc i groźby wobec sądu lub trybunału międzynarodowego), 233 ust. 1, 1a, 4 i 6 (fałszywe zeznania), 234 (fałszywe oskarżenie), 235 (fałszowanie dowodów obciążających), 236 ust. 1 (fałszowanie dowodów niewinności), 238 (fałszywe oskarżenie o popełnienie przestępstwa), 239 ust. 1 (pomocnictwo w popełnieniu przestępstwa), 240 ust. 1 (niezawiadomienie o popełnieniu przestępstwa), 245 (zastraszanie świadków), 246 (bezprawne wymuszanie zeznań), 252 ust. 1–3 (branie zakładników), 258 (zmowa przestępcza), (...) 269 (sabotaż komputerowy), (...) 270a ust. 1 i 2 (fałszerstwo), 271a ust. 1 i 2 (fałszowanie faktur), 277a ust. 1 (fałszowanie faktur na kwotę przekraczającą 10 milionów złotych), (...) 280–282 (rozbój z bronią w rękę, rozbój kwalifikowany, wymuszenie

⁴² Niniejszy dokument zawiera odpowiednie przepisy ustawy o Policji i ustaw regulujących inne służby państwowe stosujące niejawną nadzór (o ile różnią się one od odpowiednich przepisów ustawy o Policji) w brzmieniu obowiązującym w danym czasie.

rozbójnicze), 285 ust. 1 (wyłudzenie podłączenia do linii telefonicznej [należącej] do innej osoby), 286 ust. 1 (oszustwo), (...) 296 ust. 1–3 (nadużycie zaufania), 296a ust. 1–2 i 4 (przekupstwo osób kierujących), 299 ust. 1–6 (pranie pieniędzy) i 310 ust. 1, 2 i 4 (fałszerstwo) Kodeksu karnego;

2a) określonych w art. 46 ust. 1–2 i 4 (przyjmowanie lub wręczanie korzyści majątkowych lub osobistych w związku z zawodami sportowymi), art. 47 (udział w zakładach wzajemnych na imprezy sportowe ze świadomością [istnienia] czynu zabronionego, o którym mowa w art. 46) i art. 48 ust. 1–2 (wynagrodzenie za ustalenie określonego wyniku lub wystawienie imprezy sportowej) ustawy z 25 czerwca 2010 o sporcie;

2b) określonych w art. 178–183 ustawy z 29 lipca 2005 o obrocie

instrumentami finansowymi (Dz. U. z 2023 poz. 646, 825, 1723 i 1941) oraz art. 99–100 ustawy z 29 lipca 2005 o ofercie publicznej i warunkach

wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych (...);

3) przeciwko obrotowi gospodarczemu, określonych w art. 296–306 Kodeksu

karnego, powodujących szkodę majątkową lub skierowanych przeciwko mieniu, jeżeli wysokość szkody lub wartość mienia przekracza pięćdziesięciokrotną wysokość najniższego wynagrodzenia (...) (przestępstwa nadużycia zaufania, przekupstwa członków zarządu, czynnej i biernej korupcji w sektorze prywatnym, oszustwa finansowego, kredytowego i dotacyjnego, oszustwa ubezpieczeniowego, prania brudnych pieniędzy, bezprawnego pozbawienia wierzyciela możliwości egzekucji z majątku dłużnika, pozornej upadłości, działania [popełnionego] na szkodę wierzyciela, [a mianowicie] niewykonania lub ograniczenia wykonania zobowiązań wobec wierzycieli przez utworzenie nowej jednostki organizacyjnej, przez umyślne doprowadzenie do upadłości, nierozważne doprowadzenie do upadłości, faworyzowanie wierzycieli lub korupcję gospodarczą wierzycieli, wyrządzenie szkody majątkowej osobie fizycznej, prawnej lub jednostce organizacyjnej nieposiadającej osobowości prawnej przez nieprowadzenie dokumentacji działalności gospodarczej lub prowadzenie jej w sposób nierzetelny lub wprowadzający w błąd, nadużycie lub utrudnianie postępowania o udzielenie zamówienia publicznego, fałszowanie oznakowania produktów);

3a) przeciwko wolności seksualnej i obyczajności, gdy pokrzywdzonym jest

małoletni albo gdy treści pornograficzne, o których mowa w art. 202 Kodeksu karnego, obejmują udział małoletniego,

3b) określonych w rozdziale 11 ustawy z 23 lipca 2003 o ochronie

zabytków

i opiece nad zabytkami, w rozdziale 5 ustawy z 14 lipca 1983 o narodowym zasobie archiwalnym i archiwach, w rozdziale 5a ustawy z 21 listopada 1996 o muzeach, w rozdziale 11a

ustawy z dnia 27 czerwca 1997 r. o bibliotekach oraz w rozdziale 6 ustawy z dnia 25 maja 2017 o restytucji narodowych dóbr kultury;

4) skarbowych, jeżeli wartość przedmiotu czynu lub uszczuplenie należności publicznoprawnej przekraczają pięćdziesięciokrotną wysokość najniższego wynagrodzenia za pracę określonego na podstawie odrębnych przepisów;

4a) skarbowych, o których mowa w art. 107 ust. 1 Kodeksu karnego skarbowego,

5) nielegalnego wytwarzania, posiadania lub obrotu bronią, amunicją, materiałami wybuchowymi, środkami odurzającymi, substancjami psychotropowymi, ich prekursorami lub nowymi substancjami psychoaktywnymi oraz materiałami jądrowymi i promieniotwórczymi,

6) określonych w art. 8 ustawy z 6 czerwca 1997 – Przepisy wprowadzające Kodeks karny;

7) określonych w art. 43–46 ustawy z 1 lipca 2005 o pobieraniu,

przechowywaniu i przeszczepianiu komórek, tkanek i narządów;

8) ściganych na mocy umów międzynarodowych ratyfikowanych za uprzednią zgodą wyrażoną w ustawie, określonych w polskiej ustawie karnej;

9) o których mowa w pkt 1–8 lub, o których mowa w art. 45 § 2 Kodeksu karnego albo art. 33 ust. 2 Kodeksu karnego skarbowego (...);

– gdy inne środki okazały się bezskuteczne albo będą nieprzydatne, sąd okręgowy może, w drodze postanowienia, zarządzić kontrolę operacyjną, na pisemny wniosek

Komendanta Głównego Policji, Komendanta CBŚP, złożony po uzyskaniu pisemnej zgody Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego.

1a. Wniosek, o którym mowa w ust. 1, przedstawia się wraz z materiałami

uzasadniającymi potrzebę zastosowania kontroli operacyjnej.

2. Postanowienie, o którym mowa w ust. 1, wydaje sąd okręgowy właściwy

miejscowo ze względu na siedzibę składającego wniosek organu Policji.

3. W przypadkach niecierpiących zwłoki, jeżeli mogłoby to spowodować utratę

informacji lub zatarcie albo zniszczenie dowodów przestępstwa, Komendant Główny Policji, Komendant CBŚP, albo komendant wojewódzki Policji może zarządzić, po uzyskaniu pisemnej zgody właściwego prokuratora, o którym mowa w ust. 1, kontrolę operacyjną, zwracając się jednocześnie

do właściwego miejscowo sądu okręgowego z wnioskiem o wydanie postanowienia w tej sprawie. W razie nieudzielenia przez sąd zgody w terminie 5 dni od dnia zarządzenia kontroli operacyjnej, organ zarządzający wstrzymuje kontrolę operacyjną

oraz dokonuje protokolarnego, komisyjnego zniszczenia materiałów zgromadzonych podczas jej stosowania.

(...)

5. W przypadku potrzeby zarządzenia kontroli operacyjnej wobec osoby

podejrzanej lub oskarżonego, we wniosku organu Policji, o którym mowa w ust. 1, o zarządzenie kontroli operacyjnej zamieszcza się informację o toczącym się wobec tej osoby postępowaniu.

6. Kontrola operacyjna prowadzona jest niejawnie i polega na:

1) uzyskiwaniu i utrwalaniu treści rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą sieci telekomunikacyjnych;

2) uzyskiwaniu i utrwalaniu obrazu lub dźwięku osób z pomieszczeń, środków

transportu lub miejsc innych niż miejsca publiczne;

3) uzyskiwaniu i utrwalaniu treści korespondencji, w tym korespondencji

prowadzonej za pomocą środków komunikacji elektronicznej;

4) uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach

danych, telekomunikacyjnych urządzeniach końcowych, systemach

informatycznych i teleinformatycznych;

5) uzyskiwaniu dostępu i kontroli zawartości przesyłek.

6a. Kontroli operacyjnej nie stanowią czynności, o których mowa w ust. 6 pkt 2, polegające na uzyskiwaniu i utrwalaniu obrazu w pomieszczeniach, o których mowa w art. 15 ust. 1 pkt 4a

6b. Realizacja czynności, o których mowa w ust. 6a, nie wymaga zgody sądu.

7. Wniosek organu Policji, o którym mowa w ust. 1, o zarządzenie przez sąd

okręgowy kontroli operacyjnej powinien zawierać w szczególności:

- 1) numer sprawy i jej kryptonim, jeżeli został jej nadany;
- 2) opis przestępstwa z podaniem, w miarę możliwości, jego kwalifikacji prawnej;
- 3) okoliczności uzasadniające potrzebę zastosowania kontroli operacyjnej, w tym stwierdzonej bezskuteczności lub nieprzydatności innych środków;
- 4) dane osoby lub inne dane, pozwalające na jednoznaczne określenie podmiotu lub przedmiotu, wobec którego stosowana będzie kontrola operacyjna, ze wskazaniem miejsca lub sposobu jej stosowania;
- 5) cel, czas i rodzaj prowadzonej kontroli operacyjnej, o której mowa.

8. Kontrolę operacyjną zarządza się na okres nie dłuższy niż 3 miesiące. Sąd okręgowy może, na pisemny wniosek właściwego komendanta Policji, złożony po uzyskaniu pisemnej zgody właściwego prokuratora, na okres nie dłuższy niż kolejne 3 miesiące, wydać postanowienie o jednorazowym przedłużeniu kontroli operacyjnej, jeżeli nie ustały przyczyny tej kontroli.

9. W uzasadnionych przypadkach, gdy podczas stosowania kontroli operacyjnej

pojawiają się nowe okoliczności istotne dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawców i uzyskania dowodów przestępstwa, sąd okręgowy, na pisemny wniosek Komendanta Głównego Policji, złożony po uzyskaniu pisemnej zgody Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego, może, również po upływie okresów, o których mowa w ust. 8, wydawać kolejne postanowienia o przedłużeniu kontroli operacyjnej na następujące po sobie okresy, których łączna długość nie może przekraczać 12 miesięcy.

9a. Komendant Główny Policji, Komendant CBŚP, albo komendant wojewódzki Policji może upoważnić swojego

zastępcę do składania wniosków, o których mowa w ust. 1, 3, 8 i 9, lub do zarządzania kontroli operacyjnej w trybie ust. 3

10. Do wniosków, o których mowa w ust. 3, 8 i 9, stosuje się odpowiednio ust.

1a i 7. Sąd przed wydaniem postanowienia, o którym mowa w ust. 1, 3, 8 i 9, zapoznaje się z materiałami uzasadniającymi wniosek, w szczególności zgromadzonymi podczas

stosowania kontroli operacyjnej zarządzanej w tej sprawie.

11. Wnioski, o których mowa w ust. 1, 3–5, 8 i 9, sąd okręgowy rozpoznaje

jednoosobowo, przy czym czynności sądu związane z rozpoznawaniem tych wniosków powinny być realizowane w warunkach przewidzianych dla przekazywania, przechowywania i udostępniania informacji niejawnych oraz z

odpowiednim zastosowaniem przepisów wydanych na podstawie art. 181 ust. 2 Kodeksu postępowania karnego. W posiedzeniu sądu może wziąć udział wyłącznie prokurator i przedstawiciel organu Policji wnioskującego o zarządzenie kontroli operacyjnej.

12. Przedsiębiorca telekomunikacyjny, operator pocztowy oraz usługodawca

świadczący usługi drogą elektroniczną są obowiązani do zapewnienia na własny koszt warunków technicznych i organizacyjnych umożliwiających prowadzenie przez Policję kontroli operacyjnej.

12a. Usługodawca świadczący usługi drogą elektroniczną będący mikroprzedsiębiorcą lub małym przedsiębiorcą w rozumieniu przepisów ustawy z 6 lipca 2004 o swobodzie działalności gospodarczej zapewnia warunki techniczne i organizacyjne umożliwiające prowadzenie

przez Policję kontroli operacyjnej stosownie do posiadanej infrastruktury.

13. Kontrola operacyjna powinna być zakończona niezwłocznie po ustaniu

przyczyn jej zarządzenia, najpóźniej jednak z upływem okresu, na który została wprowadzona.

14. Organ Policji, o którym mowa w ust. 1, informuje właściwego prokuratora o

wynikach kontroli operacyjnej po jej zakończeniu, a na jego żądanie również o przebiegu tej kontroli.

15. W przypadku uzyskania dowodów pozwalających na wszczęcie postępowania karnego lub mających znaczenie dla toczącego się

postępowania karnego Komendant Główny Policji, Komendant CBŚP, albo komendant wojewódzki Policji przekazuje prokuratorowi, o

którym mowa w ust. 1, wszystkie materiały zgromadzone podczas stosowania kontroli operacyjnej. W postępowaniu przed sądem, w odniesieniu do tych materiałów, stosuje

się odpowiednio art. 393 ust. 1 zdanie pierwsze Kodeksu postępowania karnego.

(...)

15f. W przypadku, gdy materiały, o których mowa w ust. 15:

1) zawierają informacje, o których mowa w art. 178 Kodeksu postępowania

karnego, Komendant Główny Policji, Komendant CBŚP, albo komendant wojewódzki Policji zarządza ich

niezwłoczne, komisyjne i protokolarne zniszczenie;

2) mogą zawierać informacje, o których mowa w art. 178a i art. 180 § 3 Kodeksu postępowania karnego, z wyłączeniem informacji o przestępstwach, o których

mowa w art. 240 ust 1 Kodeksu karnego, albo informacje stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 ust. 2 Kodeksu postępowania karnego, Komendant Główny Policji, Komendant CBŚP, albo komendant wojewódzki Policji przekazuje prokuratorowi te materiały.

15g. W przypadku, o którym mowa w ust. 15f pkt 2, prokurator niezwłocznie po

otrzymaniu materiałów kieruje je do sądu, który zarządził kontrolę operacyjną albo wyraził na nią zgodę w trybie określonym w ust. 3, wraz z wnioskiem o:

1) stwierdzenie, które z przekazanych materiałów zawierają informacje, o których mowa w ust. 15f pkt 2;

2) dopuszczenie do wykorzystania w postępowaniu karnym materiałów

zawierających informacje stanowiące tajemnice związane z wykonywaniem

zawodu lub funkcji, o których mowa w art. 180 ust. 2 Kodeksu postępowania

karnego, nieobjęte zakazami, określonymi w art. 178a i art. 180 ust. 3

Kodeksu postępowania karnego z wyłączeniem informacji o przestępstwach, o których

mowa w art. 240 ust. 1 Kodeksu karnego.

15h. Sąd, niezwłocznie po złożeniu wniosku przez prokuratora, wydaje postanowienie o dopuszczeniu do wykorzystania w postępowaniu karnym materiałów, o których mowa w ust. 15g pkt 2, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu,

a także zarządza niezwłoczne zniszczenie materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne.

15i. Na postanowienie sądu w przedmiocie dopuszczenia do wykorzystania w

postępowaniu karnym materiałów, o których mowa w ust. 15g pkt 2, prokuratorowi przysługuje zażalenie. Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.

15j. Organ Policji jest obowiązany do wykonania zarządzenia sądu o zniszczeniu materiałów, o którym mowa w ust. 15h, oraz niezwłocznego, komisijnego i protokolarnego zniszczenia materiałów, których wykorzystanie w postępowaniu

karnym jest niedopuszczalne. Niezwłocznie informuje również prokuratora, o którym mowa w ust. 15g, o zniszczeniu przedmiotowych przedmiotów.

16. Osobie, wobec której kontrola operacyjna była stosowana, nie udostępnia się materiałów zgromadzonych podczas trwania tej kontroli. Przepis nie narusza

uprawnień wynikających z art. 321 Kodeksu postępowania karnego.

16a. Sąd okręgowy, Pierwszy Zastępca Prokuratora Generalnego Prokurator

Krajowy, prokurator okręgowy i organ Policji prowadzą rejestry postanowień,

pisemnych zgód, wniosków i zarządzeń dotyczących kontroli operacyjnej.

16b. Komendant Główny Policji prowadzi rejestr centralny wniosków i

zarządzeń dotyczących kontroli operacyjnej prowadzonej przez organy Policji w zakresie przewidzianym dla prowadzonych przez nie rejestrów.

16c. W komórkach organizacyjnych Policji wykonujących zarządzenia w

sprawie kontroli operacyjnej można odrębnie rejestrować dane zawarte w

dokumentacji z kontroli operacyjnej (...)

16d. Rejestry, o których mowa w ust. 16a–16c, prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych.

(...)

17. Zgromadzone podczas stosowania kontroli operacyjnej materiały niezawierające dowodów pozwalających na wszczęcie postępowania karnego lub

dowodów mających znaczenie dla toczącego się postępowania karnego podlegają niezwłocznemu, protokolarnemu i komisyjnemu zniszczeniu. Zniszczenie materiałów zarządza organ Policji, który wnioskuje o zarządzenie kontroli operacyjnej.

17a. O wydaniu i wykonaniu zarządzenia dotyczącego zniszczenia materiałów,

o których mowa w ust. 17, organ Policji jest obowiązany do niezwłocznego

poinformowania prokuratora.

(...)”

Artykuł 20c

„1. W celu zapobiegania lub wykrywania przestępstw, przestępstw skarbowych albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych, Policja może uzyskiwać dane niestanowiące treści odpowiednio, przekazu telekomunikacyjnego, przesyłki pocztowej albo

przekazu w ramach usługi świadczonej drogą elektroniczną, określone w:

1) art. 180c i art. 180d ustawy z 16 lipca 2004 – Prawo telekomunikacyjne (...),

2) art. 82 ust. 1 pkt 1 ustawy z 23 listopada 2012 – Prawo pocztowe (...),

3) art. 18 ust. 1–5 ustawy z 18 lipca 2002 o świadczeniu usług drogą

elektroniczną (...)

– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.

2. Przedsiębiorca telekomunikacyjny, operator pocztowy lub usługodawca

świadczący usługi drogą elektroniczną udostępnia nieodpłatnie dane, o których mowa:

1) policjantowi wskazanemu w pisemnym wniosku Komendanta Głównego Policji, Komendanta CBŚP, komendanta wojewódzkiego Policji albo osoby przez nich upoważnionej;

2) na ustne żądanie policjanta posiadającego pisemne upoważnienie osób, o których mowa w pkt 1;

3) za pośrednictwem sieci telekomunikacyjnej policjantowi posiadającemu pisemne upoważnienie osób, o których mowa w pkt 1.

3. W przypadku, o którym mowa w ust. 2 pkt 3, udostępnianie danych, o których

mowa w ust. 1, odbywa się bez udziału pracowników przedsiębiorcy telekomunikacyjnego, operatora pocztowego lub usługodawcy świadczącego usługi drogą elektroniczną lub przy niezbędnym ich udziale, jeżeli możliwość taka jest

przewidziana w porozumieniu zawartym pomiędzy Komendantem Głównym Policji a tym podmiotem.

4. Udostępnienie Policji danych, o których mowa w ust. 1, może nastąpić za

pośrednictwem sieci telekomunikacyjnej, jeżeli:

1) wykorzystywane sieci telekomunikacyjne zapewniają:

a) możliwość ustalenia osoby uzyskującej dane, ich rodzaju oraz czasu, w którym zostały uzyskane,

b) zabezpieczenie techniczne i organizacyjne uniemożliwiające osobie nieuprawnionej dostęp do danych;

2) jest to uzasadnione specyfiką lub zakresem zadań wykonywanych przez

jednostki organizacyjne Policji albo prowadzonych przez nie czynności.

5. Komendant Główny Policji, Komendant CBŚP, i komendant

wojewódzki Policji prowadzą rejestry wystąpień o

uzyskanie danych telekomunikacyjnych, pocztowych i internetowych zawierające

informacje identyfikujące jednostkę organizacyjną Policji i funkcjonariusza Policji uzyskującego te dane, ich rodzaj, cel uzyskania oraz czas, w którym zostały uzyskane. Rejestry prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie

informacji niejawnych.

6. Dane, o których mowa w ust. 1, które mają znaczenie dla postępowania

karnego, Komendant Główny Policji, Komendant CBŚP, albo komendant wojewódzki Policji przekazują prokuratorowi właściwemu miejscowo lub rzeczowo. Prokurator podejmuje decyzję o zakresie i sposobie wykorzystania przekazanych danych.

6a. Komendant Główny Policji, Komendant CBŚP, albo komendant wojewódzki (Stołeczny) Policji może upoważnić

swojego zastępcę do realizacji czynności, o których mowa w ust. 6.

7. Dane, o których mowa w ust. 1, które nie mają znaczenia dla postępowania

karnego, podlegają niezwłocznemu, komisijnemu i protokolarnemu zniszczeniu.

8. Dane, o których mowa w ust. 1, pobiera się i udostępnia się także organom

ścigania państw członkowskich Unii Europejskiej i innych państw, agencjom Unii Europejskiej zajmującym się zapobieganiem i zwalczaniem przestępczości oraz Międzynarodowej Organizacji Policji Kryminalnej – Interpol na ich wniosek, jeżeli

następuje to w celu wykrywania przestępstw oraz ścigania ich sprawców, ratowania życia lub zdrowia ludzkiego albo poszukiwania osób zaginionych.”

Artykuł 20cb

„1. W celu zapobiegania lub wykrywania przestępstw, przestępstw skarbowych albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań

poszukiwawczych lub ratowniczych, Policja może uzyskiwać dane:

1,2), które zostały wskazane w art. 161 i 179 al. ust. 9 ustawy z 16

lipca 2004 – Prawo telekomunikacyjne,

3) w przypadku użytkownika, który nie jest osobą fizyczną numer zakończenia sieci oraz siedzibę lub miejsce wykonywania działalności gospodarczej, firmę lub nazwę i formę organizacyjną tego użytkownika,

4) w przypadku stacjonarnej publicznej sieci telekomunikacyjnej – także nazwę

miejsowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi

– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.

2. Do udostępniania i przetwarzania danych, o których mowa w ust. 1, przepisy art. 20c ust. 2–8 stosuje się.”

Artykuł 20da

„1. W celu poszukiwania osób zaginionych Policja może uzyskiwać dane telekomunikacyjne, pocztowe i internetowe oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą; przepisy art. 20c ust. 2–8 stosuje się.

2. Materiały uzyskane w wyniku czynności określonych w ust. 1, które nie

zawierają informacji mających znaczenie dla poszukiwania osób zaginionych, podlegają niezwłocznemu komisijnemu i protokolarnemu zniszczeniu.”

Artykuł 20ca

„1. Kontrolę nad uzyskiwaniem przez Policję danych telekomunikacyjnych, pocztowych lub internetowych sprawuje sąd okręgowy właściwy dla siedziby organu Policji, któremu udostępniono te dane.

2. . Organ Policji, o którym mowa w ust. 1, przekazuje, z zachowaniem przepisów o ochronie informacji niejawnych, sądowi okręgowemu, o którym mowa w ust. 1, 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.

3. W ramach kontroli, o której mowa w ust. 1, sąd okręgowy może zapoznać się

z materiałami uzasadniającymi udostępnienie Policji danych telekomunikacyjnych, pocztowych lub internetowych.

4. Sąd okręgowy informuje organ Policji o wyniku kontroli w terminie 30 dni od

jej zakończenia.

5. Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 20cb ust. 1.”

II. USTAWA Z 24 MAJA 2002 O AGENCJI BEZPIECZEŃSTWA NARODOWEGO ORAZ AGENCJI WYWIADU

Artykuł 27

„1. Przy wykonywaniu czynności operacyjno-rozpoznawczych,

podejmowanych przez ABW, gdy inne środki okazały się bezskuteczne albo zachodzi wysokie prawdopodobieństwo, że będą nieskuteczne lub nieprzydatne,

sąd, na pisemny wniosek Szefa ABW, złożony po uzyskaniu pisemnej

zgody Prokuratora Generalnego, może, w drodze postanowienia, zarządzić

kontrolę operacyjną w celu przeciwdziałania przestępstwom określonym w:

1) w art. 5 ust. 1 pkt 2 litery a), c), d) i e),

2) rozdziałach XXXV-XXXVII Kodeksu karnego (przestępstwa przeciwko mieniu, przeciwko obrotowi gospodarczemu, przeciwko obrotowi pieniędzmi i papierami wartościowymi) oraz rozdziałów 6–7 Kodeksu karnego skarbowego – jeżeli godzą w podstawy ekonomiczne państwa,

3) art. 232, 233 ust. 1, 1a, 4 i 6, 234, 235, 236 ust. 1 i 239 ust. 1 KK, (...);

– wykrycie sprawców tych przestępstw, poszukiwanie dowodów ich popełnienia oraz wykrycie mienia podlegającego konfiskacie w wyniku popełnienia tych przestępstw.

(...)

15. W przypadku uzyskania dowodów pozwalających na wszczęcie

postępowania karnego lub mających znaczenie dla toczącego się

postępowania karnego Szef ABW przekazuje Prokuratorowi Generalnemu

materiały zgromadzone podczas stosowania kontroli operacyjnej, w razie potrzeby z wnioskiem o wszczęcie postępowania karnego. W postępowaniu przed sądem, w odniesieniu do tych materiałów, stosuje się odpowiednio przepis art. 393 § 1 zdanie pierwsze Kodeksu postępowania karnego.

(...)

15f. Sąd Okręgowy w Warszawie, działając na pisemny wniosek Szefa ABW i za pisemnym upoważnieniem prokuratora generalnego Prokuratury Krajowej, orzeka o zatrzymaniu dowodów zgromadzonych w wyniku kontroli operacyjnej, jeżeli dowody te mają znaczenie dla bezpieczeństwa państwa (...)

16. Zgromadzone podczas stosowania kontroli operacyjnej materiały, które nie są istotne dla bezpieczeństwa państwa lub nie stanowią informacji potwierdzających zaistnienie przestępstwa, podlegają niezwłocznemu, protokolarnemu, komisyjnemu zniszczeniu. Zniszczenie materiałów zarządza Szef ABW.

16a. Szef ABW niezwłocznie informuje Prokuratora Generalnego o zniszczeniu przedmiotów, o których mowa w ust. 16.

(...)”

Artykuł 28

„1. Funkcjonariusze ABW mogą zatrzymywać dane [dotyczące komunikacji] (...) w celu realizacji zadań powierzonych im na podstawie art. 5 [ustawy o ABW] oraz przetwarzać te dane bez wiedzy i zgody osoby, której dotyczą.

(...)

6. Szef ABW przekazuje dane, o których mowa w ust. 1, mające znaczenie dla postępowania karnego, prokuratorowi nadziedzemu prokuratury krajowej. Prokurator, o którym mowa, decyduje [w jakim zakresie] dane te powinny zostać wykorzystane.

7. Dane, które nie są istotne dla postępowania karnego lub bezpieczeństwa państwa, są natychmiast niszczone przez komisję protokolarną.”

Artykuł 28b

„1. Sąd Okręgowy w Warszawie jest odpowiedzialny za nadzorowanie stosowania środka zatrzymywania danych [dotyczących komunikacji].

(...)”

III. USTAWA Z 9 CZERWCA 2006 O CENTRALNYM BIURZE ANTYKORUPCYJNYM

Artykuł 17

„1. Przy wykonywaniu czynności operacyjno-rozpoznawczych,

podejmowanych przez CBA w celu rozpoznawania, zapobiegania i wykrywania przestępstw, uzyskania i utrwalenia dowodów przestępstw, a także ujawnienia mienia

zagrożonego przepadkiem w związku z przestępstwami:

1) określonymi w art. 228–231, art. 250a, art. 258, art. 270a § 1 i 2, art. 271a § 1 i 2, art. 277a § 1, art. 286, art. 296–297, art. 299, art. 305, art. 310 § 1, 2 i 4 ustawy z 6 czerwca 1997 – Kodeks karny,

2) skarbowymi, o których mowa w art. 2 ust. 1 pkt 1 lit. d, jeżeli wartość przedmiotu czynu lub uszczuplenie należności publicznoprawnej przekraczają pięćdziesięciokrotną wysokość minimalnego wynagrodzenia za pracę;

3) określonymi w art. 232, art. 233 § 1, 1a, 4 i 6, art. 234, art. 235, art. 236 § 1

i art. 239 § 1 ustawy z dnia 6 1997 – Kodeks karny, jeżeli dotyczą

przestępstw, o których mowa w pkt 1 i 2

– – gdy inne środki okazały się bezskuteczne albo będą nieprzydatne, sąd, na pisemny wniosek Szefa CBA, złożony po uzyskaniu pisemnej zgody Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego, może, w drodze postanowienia,

zarządzić kontrolę operacyjną.

(...)

16. Zgromadzone podczas stosowania kontroli operacyjnej materiały, które nie

stanowią informacji potwierdzających zaistnienie przestępstwa, podlegają

niezwłocznemu, protokolarnemu, komisijnemu zniszczeniu.
Zniszczenie materiałów zarządza Szef CBA.

(...)”

Artykuł 18

„1. Funkcjonariusze CBA mogą przechowywać dane [dotyczące komunikacji] (...) i mogą je przetwarzać bez wiedzy lub zgody osoby, której te dane dotyczą do celów wykonywania swoich obowiązków na podstawie art. 2 [tej ustawy].”

IV. USTAWA Z 9 CZERWCA 2006

O SŁUŻBIE KONTRWYWIADU WOJSKOWEGO ORAZ SŁUŻBIE WYWIADU WOJSKOWEGO

Artykuł 31

„1. W przypadku, gdy funkcjonariusze SKW stosują czynności operacyjno-rozpoznawcze w celu wykonania obowiązków wynikających z art. 5 ust. 1 pkt 1, 5, 7, 8 i 2, a inne środki okazują się bezskuteczne lub zbędne, sąd, działając na pisemny wniosek Szefa SKW zatwierdzony uprzednio przez Prokuratora Generalnego Prokuratury Krajowej, może zarządzić kontrolę operacyjną.

(...)

2. Postanowienie, o którym mowa w ust. 1, wydaje Wojskowy Sąd Okręgowy w Warszawie.”

Artykuł 32

„1. SKW może przechowywać dane [dotyczące komunikacji] do celów wykonywania swoich zadań na mocy art. 5 (...) i może je przetwarzać bez wiedzy lub zgody osoby, której dane dotyczą.

(...)

9. Dane, o których mowa w ust. 1, które nie mają znaczenia dla postępowania

karnego albo nie są istotne dla obronności Państwa, podlegają niezwłocznemu, komisijnemu i protokolarnemu zniszczeniu.”

Artykuł 32a

„1. Kontrolę nad uzyskiwaniem przez SKW danych telekomunikacyjnych, pocztowych lub internetowych sprawuje Wojskowy Sąd Okręgowy w Warszawie.

(...)”

V. USTAWA Z 16 LISTOPADA 2016 O KRAJOWEJ ADMINISTRACJI
SKARBOWEJ

Artykuł 115

„1. Funkcjonariusze KAS realizujący środki kontroli operacyjnej mogą przechowywać dane [dotyczące komunikacji] w celu ujawnienia naruszeń przepisów prawa podatkowego określonych w art. 2 ust. 1 pkt 14-16 oraz wykonywania obowiązków wynikających z art. 2 ust. 1 pkt 16a w zw. z art. 5 (...), a także przetwarzać te dane bez wiedzy lub zgody osoby, której one dotyczą.

(...)”

Artykuł 116

„1. Kontrolę nad uzyskiwaniem danych telekomunikacyjnych, danych pocztowych lub danych internetowych sprawuje sąd okręgowy właściwy dla siedziby organu KAS, któremu udostępniono te dane.

(...)”

Artykuł 118

„1. W ramach czynności operacyjno-rozpoznawczych, podejmowanych przez funkcjonariuszy wykonujących czynności operacyjno-rozpoznawcze, jeżeli inne środki okazały się bezskuteczne albo będą nieprzydatne, Sąd Okręgowy

w Warszawie, na pisemny wniosek Szefa Krajowej Administracji Skarbowej, złożony po uzyskaniu pisemnej zgody Pierwszego Zastępcy

Prokuratora Generalnego Prokuratora Krajowego, może, w drodze postanowienia, zarządzić kontrolę operacyjną w celu wykrycia, ustalenia sprawców oraz uzyskania i utrwalenia dowodów przestępstw:

1) skarbowych, jeżeli wartość przedmiotu czynu lub uszczuplenie należności publicznoprawnej przekracza w dniu popełnienia czynu zabronionego pięćdziesięciokrotną wysokość minimalnego wynagrodzenia za pracę;

2) skarbowych, o których mowa w art. 107 ust. 1 Kodeksu karnego skarbowego,

3) przeciwko obrotowi gospodarczemu, powodujących szkodę majątkową, jeżeli

wysokość szkody przekracza w dniu popełnienia czynu zabronionego

pięćdziesięciokrotną wysokość minimalnego wynagrodzenia za pracę,

3a), określonych w art. 270a § 1 i 2, art. 271a § 1 i 2 oraz art. 277a § 1 Kodeksu

karnego,

4) przeciwko mieniu, jeżeli wartość mienia przekracza w dacie popełnienia czynu zabronionego pięćdziesięciokrotną wysokość minimalnego wynagrodzenia za pracę,

5) określonych w przepisach art. 258, art. 270, art. 271 lub art. 273 Kodeksu

karnego, w związku z którymi nastąpiło uszczuplenie lub narażenie na

uszcuplenie należności publicznoprawnej przekraczające pięćdziesięciokrotną wysokość minimalnego wynagrodzenia za pracę,

6) określonych w art. 228–231 Kodeksu karnego, popełnionych przez osoby

zatrudnione w jednostkach organizacyjnych KAS albo funkcjonariuszy, w związku z wykonywaniem czynności służbowych;

7) określonych w art. 229 Kodeksu karnego, popełnionych przez osoby niezatrudnione w jednostkach organizacyjnych KAS (...);

8) ściganych na mocy umów międzynarodowych ratyfikowanych za uprzednią zgodą wyrażoną w ustawie, określonych w polskiej ustawie karnej;

9) określonych w pkt 1–8 lub art. 33 § 2 Kodeksu karnego skarbowego (...);
(...)”

Artykuł 122

„1. Dane, o których mowa w art. 114 ust. 1 i art. 115 ust. 1, oraz materiały uzyskane w trybie art. 113 ust. 1, art. 117 ust. 1, art. 118 ust. 1 i 3, art.

119 ust. 1 i 2, art. 120 ust. 1 oraz art. 127a ust. 1 i 2, które:

1) zawierają informacje mające znaczenie dla kontroli celno-skarbowej, postępowania podatkowego, postępowania w sprawach celnych lub

postępowania w sprawach o przestępstwa skarbowe oraz przestępstwa, o których mowa w art. 2 ust. 1 pkt 14–16, a także dla ujawniania i odzyskiwania mienia zagrożonego przypadkiem w związku z przestępstwami, o których mowa w art.

2 ust. 1 pkt 13–16 albo art. 33 § 2 Kodeksu karnego skarbowego, są
przekazywane właściwemu miejscowo organowi KAS;

2) zawierają dowody pozwalające na wszczęcie postępowania albo
mające

znaczenie dla postępowania w sprawie o przestępstwo inne niż określone

w pkt 1, odpowiednio Szef Krajowej Administracji Skarbowej albo
naczelnik

urzędu celno-skarbowego przekazuje Pierwszemu Zastępcy Prokuratora

Generalnego Prokuratorowi Krajowemu albo prokuratorowi
okręgowemu

właściwemu miejscowo (...)

(...)”

Artykuł 123

„1. Dane, o których mowa (...) niezawierające dowodów pozwalających
na wszczęcie postępowania w sprawie o przestępstwo lub przestępstwo
skarbowe albo

niemające znaczenia dla kontroli celno-skarbowej (...) lub dla ujawniania
i odzyskiwania mienia zagrożonego przypadkiem w związku z
przestępstwami, o których mowa w art. 2 ust. 1 pkt 13–16 albo art. 33 §
2 Kodeksu karnego skarbowego, a także materiały uzyskane w wyniku
kontroli operacyjnej, o których mowa w art. 122 ust. 4, których
zniszczenie zarządził

Sąd, podlegają niezwłocznemu, komisijnemu i protokolarnemu
zniszczeniu.

2. Zniszczenie, o którym mowa w ust. 1, z wyjątkiem materiałów,
których

zniszczenie zarządza Sąd, zarządza:

1) Szef Krajowej Administracji Skarbowej albo naczelnik

urzędu celno-skarbowego (...),

2) Szef Krajowej Administracji Skarbowej (...)

3. O wydaniu i wykonaniu zarządzenia dotyczącego zniszczenia
wspomnianych materiałów (...) odpowiednio Szef

Krajowej Administracji Skarbowej albo naczelnik urzędu celno-skarbowego

niezwłocznie informuje Pierwszego Zastępcę Prokuratora Generalnego Prokuratora Krajowego albo właściwego prokuratora okręgowego.”

VI. USTAWA Z 12 PAŹDZIERNIKA 1990 O STRAŻY GRANICZNEJ

Artykuł 9e

„1. Przy wykonywaniu czynności operacyjno-rozpoznawczych,

podejmowanych przez Straż Graniczną w celu zapobieżenia, wykrycia, ustalenia

sprawców oraz uzyskania i utrwalenia dowodów, ściganych z oskarżenia publicznego, umyślnych przestępstw:

1) określonych w art. 163 § 1, art. 164 § 1, art. 165 § 1, art. 166 § 1 i 2, art. 167, art. 168, art. 171, art. 172, art. 173 § 1, art. 258, art. 264 § 2–4, art. 270a § 1 i 2, art. 271a § 1 i 2, art. 277a § 1 i art. 299 § 1 Kodeksu karnego,

2) określonych w art. 270–276 Kodeksu karnego w zakresie wiarygodności

dokumentów uprawniających do przekraczania granicy państwowej,

dokumentów uprawniających do pobytu na terytorium Rzeczypospolitej Polskiej

lub dokumentów wymaganych do ich wydania;

3) skarbowych, o których mowa w art. 134 § 1 pkt 1 Kodeksu karnego skarbowego, jeżeli wartość przedmiotu czynu lub uszczuplenie należności publicznej przekraczają pięćdziesięciokrotną wysokość najniższego wynagrodzenia za

pracę (...),

4) określonych w art. 183 § 2, 4 i 5, art. 184 § 1 i 2, art. 263 § 1 i 2, art. 278 § 1, art. 291 § 1 i art. 306 Kodeksu karnego, art. 55 i art. 56 ustawy z 29 lipca 2005 o przeciwdziałaniu narkomanii, a także art. 44 i

art. 46a ustawy z 1 lipca 2005 o pobieraniu, przechowywaniu

i przeszczepianiu komórek, tkanek i narządów, art. 109 ust. 1 ustawy z 23 lipca 2003 o ochronie zabytków i opiece nad zabytkami, art. 11–13 ustawy z 13 kwietnia 2016 o bezpieczeństwie obrotu prekursorami materiałów wybuchowych, art. 53 ust.

1 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach, art. 34a ust. 1 ustawy z 21 listopada 1996 o muzeach oraz art. 29a ust. 1 ustawy z 27 czerwca 1997 o bibliotekach, jeżeli przestępstwa te pozostają w związku z przemieszczaniem przedmiotów

przestępstwa przez granicę państwową;

5) określonego w art. 464 ustawy z 12 grudnia 2013 o cudzoziemcach,

6) określonych w art. 228, art. 229 i art. 231 Kodeksu karnego, popełnionych przez funkcjonariuszy lub pracowników Straży Granicznej w związku

z wykonywaniem obowiązków służbowych, a także funkcjonariuszy

i pracowników Policji i Służby Ochrony Państwa lub strażaków Państwowej

Straży Pożarnej w przypadku, o którym mowa w art. 1 ust. 2 pkt 4a,

6a) określonych w art. 229 Kodeksu karnego, popełnionych przez osoby niebędące funkcjonariuszami lub pracownikami Straży Granicznej w związku z wykonywaniem czynności służbowych przez funkcjonariuszy lub

pracowników Straży Granicznej,

6b) określonych w art. 264a Kodeksu karnego oraz art. 10 ustawy z dnia 15 czerwca 2012 o skutkach powierzania wykonywania pracy cudzoziemcom

przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej,

6c) określonych w art. 189a i art. 191b Kodeksu karnego i w art. 8 ustawy z 6 czerwca 1997 – Przepisy wprowadzające Kodeks karny,

7) ściganych na mocy umów międzynarodowych ratyfikowanych za uprzednią zgodą wyrażoną w ustawie, określonych w polskiej ustawie karnej;

8) określonych w art. 232, art. 233 § 1, 1a, 4 i 6, art. 234, art. 235, art. 236 § 1 i art. 239 § 1 Kodeksu karnego, jeżeli dotyczą przestępstw, o których mowa w pkt 1–7,

9) o których mowa w pkt 1–8 lub, o których mowa w art. 45 § 2 Kodeksu karnego albo art. 33 § 2 Kodeksu karnego skarbowego – w celu ujawnienia mienia zagrożonego przypadkiem w związku z tymi przestępstwami

– gdy inne środki okazały się bezskuteczne albo będą nieprzydatne, sąd, na pisemny wniosek Komendanta Głównego Straży Granicznej lub

Komendanta BSWSG, po

uzyskaniu pisemnej zgody Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego, albo na pisemny wniosek komendanta oddziału Straży Granicznej, po uzyskaniu pisemnej zgody właściwego prokuratora okręgowego, może, w drodze

postanowienia, zarządzić kontrolę operacyjną.

(...)”

Artykuł 10b

„1. Funkcjonariusze Straży Granicznej mogą zatrzymywać dane [dotyczące komunikacyjne] do celów zapobiegania przestępstwom lub naruszeniom prawa podatkowego lub ich wykrywania (...) i mogą je przetwarzać bez wiedzy lub zgody osoby zainteresowanej.

(...)”

Artykuł 10ba

„1. Kontrolę nad uzyskiwaniem przez Straż Graniczną danych telekomunikacyjnych, pocztowych lub internetowych sprawuje sąd okręgowy właściwy dla siedziby składającego wniosek organu Straży Granicznej.

(...)”

Artykuły 10bb (gromadzenie danych uzupełniających)

„1. W celu zapobiegania lub wykrywania przestępstw oraz przestępstw skarbowych Straż Graniczna może uzyskiwać dane:

1) z wykazu, o którym mowa w art. 179 ust. 9 ustawy z 16 lipca 2004

–

Prawo telekomunikacyjne,

2) o których mowa w art. 161 ustawy z 16 lipca 2004 – Prawo

telekomunikacyjne,

3) w przypadku użytkownika, który nie jest osobą fizyczną numer zakończenia sieci oraz siedzibę lub miejsce wykonywania działalności gospodarczej, firmę lub nazwę i formę organizacyjną tego użytkownika,

4) w przypadku stacjonarnej publicznej sieci telekomunikacyjnej – także nazwę

miejscowości oraz ulicy, przy której znajduje się zakończenie sieci,

udostępnione użytkownikowi

– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.

2. Do udostępniania i przetwarzania danych, o których mowa w ust. 1, przepisy art. 10b ust. 2–8 stosuje się.”

VII. USTAWA Z 24 SIERPNIA 2001 O ŻANDARMERII WOJSKOWEJ I WOJSKOWYCH ORGANACH PORZĄDKOWYCH

Artykuł 30

„1. 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, albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych, Żandarmeria Wojskowa może uzyskiwać dane niestanowiące treści odpowiednio, przekazu telekomunikacyjnego, przesyłki pocztowej albo przekazu w ramach usługi świadczonej drogą

elektroniczną (...) oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.

(...)”

Artykuł 30b

„1. Kontrolę nad uzyskiwaniem przez Żandarmerię Wojskową danych telekomunikacyjnych, pocztowych lub internetowych sprawuje wojskowy

sąd okręgowy właściwy dla siedziby organu Żandarmerii Wojskowej, któremu udostępniono te dane.

(...)”

Artykuł 31

„1. Przy wykonywaniu czynności operacyjno-rozpoznawczych

podejmowanych przez Żandarmerię Wojskową w granicach zadań określonych w art. 4 ust. 1 oraz w stosunku do osób wskazanych w art. 3 ust. 2 pkt 1, 3, 5 i 6, w celu zapobieżenia, wykrycia, ustalenia sprawców oraz uzyskania i utrwalenia

dowodów, umyślnych przestępstw ściganych z oskarżenia publicznego:

1) przeciwko pokojowi i ludzkości,

2) przeciwko Rzeczypospolitej Polskiej, z wyjątkiem przestępstw określonych

w art. 127–132 Kodeksu karnego,

3) przeciwko życiu, określonych w art. 148–150 Kodeksu karnego,

4) określonych w art. 140, art. 156 § 1 i 3, art. 163 § 1 i 3, art. 164 § 1, art. 165

§ 1 i 3, art. 166, art. 167, art. 171 § 1, art. 173 § 1 i 3, art. 189, art. 189a, art. 200, art. 200a, art. 202 § 3 i 4, art. 211a, art. 223, art. 228 § 1 i 3–6,

art. 229 § 1 i 3–5, art. 230 § 1, art. 230a § 1, art. 231 § 1 i 2, art. 232, art. 233 § 1, 1a, 4 i 6, art. 234, art. 235, art. 236 § 1, art. 238, art. 239 § 1, art. 240 § 1, art. 245, art. 246, art. 252 § 1–3, art. 258, art. 263 § 1 i 2, art. 265, art. 269, art. 270a § 1 i 2, art. 271a § 1 i 2, art. 277a § 1, art. 280–282, art. 285 § 1,

art. 286 § 1 i 2, art. 299 § 1–6, art. 305, art. 310 § 1, 2 i 4, art. 339 § 2, art. 345

§ 2 i 3 oraz art. 358 § 2 Kodeksu karnego,

5) skarbowych, jeżeli wartość przedmiotu czynu lub uszczuplenie należności publicznoprawnej przekraczają pięćdziesięciokrotną wysokość najniższego wynagrodzenia za pracę (...);

6) określonych w art. 8 ustawy z 6 czerwca 1997 – Przepisy

wprowadzające Kodeks karny

6a) określonych w rozdziale 11 ustawy z 23 lipca 2003 o ochronie

zabytków i opiece nad zabytkami, w rozdziale 5 ustawy z 14 lipca 1983 o narodowym zasobie archiwalnym i archiwach, w rozdziale 6 ustawy z 25 maja 2017 o restytucji narodowych dóbr kultury, w rozdziale 5a ustawy z 21 listopada 1996 o muzeach oraz w rozdziale 11a ustawy z 27 czerwca 1997 o bibliotekach;

7) określonych w art. 43 i art. 44 ustawy z 1 lipca 2005 o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów,

8) określonych w art. 53 ust. 1, art. 55 ust. 1, art. 56 ust. 1, art. 58 ust. 1,

art. 59 ust. 1, art. 62 ust. 1 oraz art. 62b ust. 1 i 2 ustawy z 29 lipca

2005 o przeciwdziałaniu narkomanii,

9) ściganych na mocy umów międzynarodowych ratyfikowanych za

uprzednią zgodą wyrażoną w ustawie, określonych w polskiej ustawie karnej,

– gdy inne środki okazały się bezskuteczne albo będą nieprzydatne, wojskowy sąd okręgowy, na pisemny wniosek Komendanta Głównego Żandarmerii Wojskowej, złożony po uzyskaniu pisemnej zgody Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego, lub na pisemny wniosek komendanta

oddziału Żandarmerii Wojskowej, złożony po uzyskaniu zgody Komendanta Głównego Żandarmerii Wojskowej i pisemnej zgody właściwego zastępcy prokuratora okręgowego do spraw wojskowych, może, w drodze postanowienia,

zarządzić kontrolę operacyjną.

(...)

21. Kontrola operacyjna, na którą Żandarmeria Wojskowa uzyskała zgodę,

w trybie określonym w niniejszej ustawie, jest realizowana (...) przez Służbę Kontrwywiadu Wojskowego.

(...)”