© Prokurator Generalny – Minister Sprawiedliwości

© Copyright for the Polish translation by Prokurator Generalny – Minister Sprawiedliwości

Warszawa 2016

WIELKA IZBA

**SPRAWA ROMAN ZAKHAROV przeciwko ROSJI**

*(Skarga nr 47143/06)*

WYROK

STRASBOURG

4 grudnia 2015

*Ten wyrok jest prawomocny, ale może podlegać korekcie wydawniczej.*

W sprawie Roman Zakharov przeciwko Rosji,

Europejski Trybunał Praw Człowieka, zasiadający jako Wielka Izba w składzie:

 Dean Spielmann, *Przewodniczący,* Josep Casadevall, Guido Raimondi, Ineta Ziemele,

 Mark Villiger,  Luis López Guerra, Khanlar Hajiyev, Angelika Nußberger, Julia Laffranque, Linos-Alexandre Sicilianos, Erik Møse, André Potocki, Paul Lemmens, Helena Jäderblom, Faris Vehabović, Ksenija Turković, Dmitry Dedov, *sędziowie,*
oraz Lawrence Early, *Radca Prawny,*

Obradując na posiedzeniu niejawnym w dniu 24 września 2014 i 15 października 2015,

Wydał następujący wyrok, który został przyjęty w wyżej wspomnianym terminie:

PROCEDURA

1. Sprawa została wszczęta skargą (nr 47143/06) złożoną przeciwko Federacji Rosyjskiej do Trybunału na mocy Artykułu 34 Konwencji o ochronie praw człowieka i podstawowych wolności (“Konwencja”) przez obywatela Rosji, Pana Romana Zakharov (“skarżący”), dnia 20 października 2006.

2.  Skarżący był reprezentowany przez Pana B. Gruzd, adwokata mającego praktykę w St. Petersburgu. Następnie był reprezentowany przez adwokatów z NGO EHRAC/ Centrum Praw Człowieka „Memoriał”, znajdującego się w Moskwie. Rząd Rosyjski (“Rząd”) był reprezentowany przez Pana G. Matyushkin, Przedstawiciela Federacji Rosyjskiej przy Europejskim Centrum Praw Człowieka.

3. Skarżący stwierdził, że system tajnego przechwytywania rozmów telefonicznych w Rosji, naruszył jego prawo do poszanowania życia prywatnego i korespondencji oraz że nie przysługiwały mu żadne efektywne środki odwoławcze w tym zakresie.

4.  Dnia 19 października skarga została zakomunikowana Rządowi.

5.  Dnia 11 marca 2014 Izba Sekcji Pierwszej, do której trafiła sprawa (Reguła 52 § Regulaminu Trybunału), w składzie której zasiadali Przewodnicząca Isabelle Berro-Lefèvre oraz: Khanlar Hajiyev, Julia Laffranque, Linos‑Alexandre Sicilianos, Erik Møse, Ksenija Turković, Dmitry Dedov, sędziowie, a także Søren Nielsen, Kanclerz Sekcji, przekazali jurysdykcję Wielkiej Izbie, czemu żadna ze stron się nie sprzeciwiła (Artykuł 30 Konwencji i Reguła 72).

6.  Rozprawa otwarta dla publiczności miała miejsce w Budynku Praw Człowieka w Strasbourgu, dnia 24 września 2014 (Reguła 59 § 3).

Przed Trybunałem stawili się:

(a)  *w imieniu Rządu*
Pan G. Matyushkin, *Przedstawiciel Federacji Rosyjskiej przy Europejskim Trybunale Praw Człowieka*, *Pełnomocnik*,

 Pani O. Sirotkina,

 Pani I. Korieva,

 Pani O. Iurchenko,

 Pan O. Afanasev,

 Pan A. Lakov, *Konsultanci;*

(b)  *w imieniu skarżącego*
Pan P. Leach,

 Pani K. Levine,

 Pan K. Koroteev,

 Pani A. Razhikova, *Obrońca,*

 Pani E. Levchishina, *Konsultant.*

Trybunał wysłuchał zarzutów Pana Matyushkin, Pana Leach, Pani Levine, Pani Razhikova and Pana Koroteev, oraz odpowiedzi Pana Matyushkin i Pana Leach na pytania zadawane przez sędziów.

FAKTY

I.  OKOLICZNOŚCI SPRAWY

7.  Skarżący urodził się w roku 1977 i mieszka w St. Petersburgu.

8.  Skarżący jest redaktorem naczelnym wydawnictwa oraz magazynu o tematyce lotniczej. Jest również przewodniczącym oddziału Fundacji Obrony Glasnost, organizacji pozarządowej monitującej stan wolności mediów w różnych regionach Rosji, promującej niezależność regionalnych środków masowego przekazu, wolność słowa i poszanowanie dla praw dziennikarzy, a także zapewnia pomoc prawną dla dziennikarzy, także w dotyczących ich postępowaniach sądowych.

9.  Skarżący korzystał z usług kilku sieci operatorów komórkowych.

10.  Dnia 23 grudnia 2003 wniósł sprawę przeciwko trzem operatorom sieci, twierdząc, że dopuścili się ingerencji w jego prawo do prywatności komunikacji telefonicznej. Twierdził, że zgodnie z Rozporządzeniem nr 70 (zob. par. 115 i 122 poniżej) poprzednika Ministerstwa Komunikacji, (Państwowego Komitetu do spraw Komunikacji i Technologii Komunikacyjnych) operatorzy sieci telefonicznych zainstalowali urządzenie, które umożliwiło Federalnej Służbie Bezpieczeństwa (“FSB”) przechwycenie rozmów telefonicznych bez uprzedniego zezwolenia sądowego. Skarżący twierdził również, że Rozporządzenie nr 70, które nigdy nie zostało opublikowane, nadmiernie ograniczało jego prawo do prywatności. Zwrócił się do sądu o wydanie nakazu usunięcia urządzenia zainstalowanego na mocy Rozporządzenia nr 70, oraz by udostępniać komunikację telefoniczną tylko osobom upoważnionym. Minister Komunikacji i Technologii Informacyjnych (dalej zwany jako “Minister Komunikacji”) oraz Departament Regionalny St. Petersburga i Leningradu FSB dołączyli do sprawy na prawach strony trzeciej.

11.  Dnia 5 grudnia 2005, Sąd Rejonowy w Vasileostrovskiy oddalił skargę skarżącego. Stwierdził, że skarżący nie udowodnił, że operatorzy sieci komórkowych transmitowali jakieś informacje chronione osobom nieupoważnionym lub zezwalali na nieograniczone lub bezprawne przechwytywanie transmisji komunikacyjnej. Urządzenie, o którym mowa, zostało zainstalowane, by umożliwić organom odpowiedzialnym za egzekwowanie prawa, prowadzenie czynności operacyjnych zgodnie z procedurą przewidzianą przez prawo. Instalacja takiego urządzenia sama w sobie nie naruszała prywatności komunikacji skarżącego. Skarżący nie przedstawił żadnych faktów, które potwierdzałyby naruszenie jego prawa do prywatności komunikacji telefonicznej.

12.  Skarżący złożył apelację. Twierdził, w szczególności, że Sąd Rejonowy odmówił przyjęcia kilku dokumentów jako dowodów w sprawie. Dokumenty te stanowiły dwa orzeczenia sądowe zezwalające na ingerencję w komunikację telefoniczną w sposób wsteczny oraz aneks do standardowej umowy dostawcy usług telefonicznych, zawartej przez jednego z operatorów sieci komórkowych. Jedno z tych orzeczeń sądowych, wydanych w dniu 8 grudnia 2002, umożliwiło ingerencję w komunikację telefoniczną kilku osób, w okresie od 1 do 5 kwietnia, od 19 do 23 czerwca, od 30 czerwca do 4 lipca oraz od 16 do 20 października 2001. Drugie orzeczenie sądowe, wydane 18 lipca 2003, zezwoliło na ingerencję w komunikację telefoniczną Pana E. w okresie od 11 kwietnia do 11 października 2003. Aneks zawierał informację dla usługobiorcy, że jeżeli jego numer był wykorzystywany do gróźb terrorystycznych, operator sieci komórkowej może zawiesić świadczenie usług telefonicznych i przekazać zebrane dane do organów ścigania. W opinii skarżącego, orzeczenia sądowe oraz aneks udowadniał, że operatorzy sieci komórkowych i organy ścigania były technicznie w stanie zakłócać wszystkie komunikacje telefoniczne, zanim uzyskały zezwolenie sądowe, oraz regularnie dopuszczali się bezprawnych ingerencji.

13.  W dniu 26 kwietnia 2006 Sąd Miejski w St. Petersburgu utrzymał zaskarżone orzeczenie w mocy. Potwierdził stanowisko Sądu Rejonowego, że skarżący nie udowodnił, że jego rozmowy telefoniczne były przechwytywane, a także nie udowodnił, że istniało bezprawne naruszenie prywatności jego komunikacji telefonicznych. By ustalić istnienie takiego zagrożenia, skarżący musiałby udowodnić, że pozwani działali bezprawnie. Jednakże, prawo wymagało od operatorów sieci komórkowej instalowania urządzeń umożliwiających organom śledczym prowadzenie czynności operacyjno-rozpoznawczych, a samo istnienie tych urządzeń nie ingerowało w prywatność komunikacji skarżącego. Odmowa przyznania mocy dowodowej orzeczeniom sądowym z 8 października 2002 i 18 lipca 2003 była legalna, ponieważ orzeczenia te były wydane w stosunku osób trzecich i nie znajdowały zastosowania w sprawie skarżącego. Sąd Miejski dalej przyznał moc dowodową aneksowi do umowy z dostawcą usług oraz zadecydował się go zbadać, ale uznał, że nie zawiera żadnych informacji uzasadniających podważenie wyroku Sądu Rejonowego.

14. Można zauważyć w dokumencie złożonym przez skarżącego, że w styczniu 2007, NGO “Kontrola Cywilna” zwróciła się do biura Prokuratora Generalnego o zbadanie Rozporządzeń Ministra Komunikacji w zakresie ich zgodności z prawem federalnym. W lutym 2007, urzędnik z biura Prokuratora Generalnego zatelefonował do “Kontroli Cywilnej” i poprosił o kopie nieupublicznionych załączników do Rozporządzenia nr 70 twierdząc, że biuro prokuratora nie było w stanie uzyskać ich od Ministra Komunikacji. W kwietniu 2007 biuro Prokuratora Generalnego odmówiło dokonania wnioskowanego badania.

II.  WŁAŚCIWE PRAWO KRAJOWE

A.  Prawo do poszanowania życia prywatnego i korespondencji

15.  Konstytucja gwarantuje każdemu prawo do poszanowania jego życia prywatnego, osobistych i rodzinnych tajemnic, a także prawa do ochrony honoru i reputacji (Artykuł 23 § 1). Dalej gwarantuje prawo do poszanowania korespondencji, a także komunikacji telefonicznych, pocztowych, telegraficznych i innych. Mogą zostać one ograniczone jedynie na mocy orzeczenia sądowego (Artykuł 23 § 2).

16.  Konstytucja także stanowi, że niedozwolone jest zbieranie, przechowywanie, korzystanie lub rozpowszechnianie informacji o życiu prywatnym osoby bez jej zgody. Państwowe i rządowe władze muszą zapewnić każdej osobie dostęp do dokumentów i materiałów dotyczących jej praw, wolności, za wyjątkiem sytuacji, w których ustawa stawowi inaczej (Artykuł 24).

17.  Ustawa o Komunikacji z 7 lipca 2003 (nr 126‑FZ) gwarantuje prywatność pocztowych, telegraficznych oraz innych form komunikacji przekazywanych za pomocą sieci telekomunikacyjnych lub mailowych. Ograniczenia w prywatności komunikacji dozwolone są wyłącznie w przypadkach określonych przez ustawy (sekcja (63)). Przechwytywanie transmisji komunikacyjnej jest przedmiotem uprzedniego upoważnienia sądowego, za wyjątkiem sytuacji wskazanych w ustawach (sekcja 63(3)).

18.  Dnia 2 października 2003 w swojej decyzji nr 345-O Trybunał Konstytucyjny uznał, że prawo do prywatności komunikacji telefonicznej obejmuje wszystkie transmitowane dane, przechowywane lub odkryte przez urządzenia telefoniczne, włączając także nieoparte na treści dane, takie jak przychodzące i wychodzące połączenia z poszczególnym odbiorcą. Monitorowanie takich danych było również przedmiotem uprzedniego upoważnienia sądowego.

B.  Odpowiedzialność za naruszenie prywatności

19.  Bezprawne zbieranie lub rozpowszechnianie informacji o życiu prywatnym lub rodzinnym danej osoby, bez jej zgody, które jest popełnione bez jakiegokolwiek osobistego interesu i jest szkodliwe dla praw obywateli oraz ich interesów prawnych, karane jest grzywną, karą pracy poprawczej lub karą pozbawienia wolności do czterech miesięcy. Te same działania, popełnione przez urzędników wykraczające ponad ich kompetencje, karane są grzywną, zakazem zajmowania określonego stanowiska lub karą więzienia do sześciu miesięcy (Artykuł 137 Kodeksu Karnego).

20.  Każde naruszenie prawa obywatela do prywatności jego komunikacji pocztowej, telegraficznej, telefonicznej lub innej formy komunikacji, karane jest grzywną lub karą pracy poprawczej. Te same działania popełnione przez urzędników wykraczające ponad ich kompetencje, karane są grzywną, zakazem zajmowania określonego stanowiska lub karą pozbawienia wolności do czterech miesięcy (Artykuł 138 Kodeksu Karnego).

21.  Nadużycie władzy przez urzędnika, którego nie popełniono dla osiągnięcia korzyści majątkowych lub osobistych, a które stanowi istotne naruszenie praw i interesów prawnych osoby fizycznej lub prawnej, karane jest grzywną, zakazem zajmowania określonego stanowiska lub obowiązkiem podjęcia pewnych działań na okres do pięciu lat, karą pracy poprawczej do lat czterech lub karą pozbawienia wolności na okres od czterech miesięcy do czterech lat (Artykuł 285 § 1 Kodeksu Karnego).

22.  Działania podejmowane przez urzędników, które wyraźnie przekraczają zakres ich uprawnień i powodują istotne naruszenie praw i interesów prawnych osoby fizycznej lub prawnej, karane są grzywną, zakazem zajmowania określonego stanowiska lub obowiązkiem podjęcia pewnych działań na okres do pięciu lat, karą pracy poprawczej do lat czterech lub karą pozbawienia wolności na okres od czterech miesięcy do czterech lat (Artykuł 286 § 1 Kodeksu Karnego).

 23. Uchwała nr 19 z dnia 16 października 2009 przyjęta przez Zgromadzenie Ogólne Sądu Najwyższego stanowi, że dla celów Artykułów 285 i 286 Kodeksu Karnego “istotne naruszenie praw i interesów prawnych osoby fizycznej lub prawnej” oznacza naruszenie praw i wolności gwarantowanych przez ogólnie przyjęte zasady, przepisy prawa międzynarodowego oraz Konstytucji Federacji Rosyjskiej – takich jak: prawo do poszanowania honoru i godności osoby, życia prywatnego i rodzinnego, korespondencji telefonicznej, pocztowej, telegraficznej, telefonicznej i innych form komunikacji, nienaruszalność mieszkania, itp. Do oceny, czy naruszenie było “istotne” w odniesieniu do osoby prawnej, konieczne jest wzięcie pod uwagę rozmiaru szkód wywołanych bezprawnym działaniem, naturą i liczbą szkód majątkowych, a także liczby osób, które doznały szkód psychicznych, majątkowych i niemajątkowych (par. 18(2)).

24.  Postępowania karne zostają wszczęte, jeżeli dostarczone fakty są wystarczające do wykazania, że popełniono przestępstwo (Artykuł 140 § 2 Kodeksu Postępowania Karnego).

C.  Ogólne przepisy dotyczące przejmowania komunikacji

25.  Przejmowanie komunikacji jest regulowane przez Ustawę o czynnościach operacyjno – rozpoznawczych z 12 sierpnia 1995 (nr 144‑FZ, zwaną dalej “OSAA”), stosowaną w przypadku przejmowania komunikacji, zarówno w ramach postępowania karnego jak i w sytuacji, gdy nie toczy się tego rodzaju postępowanie. Kodeks Postępowania Karnego z 18 grudnia 2001 (nr 174-FZ, w mocy od 1 lipca 2002, zwany dalej “KPK”), stosowany jest wyłącznie w przypadku przechwytywania komunikacji w ramach postępowania karnego.

26.  Celami działań operacyjno – rozpoznawczych są: (1) wykrycie, prewencja, tłumienie i rozpoznanie przestępstw, a także identyfikacja osób konspirujących w celu popełniania przestępstw, popełniających przestępstwa oraz tych, którzy już dopuścili się przestępstw; (2) namierzanie osób uchylających się od odpowiedzialności karnej oraz osób zaginionych (3) uzyskiwanie informacji o zdarzeniach lub działaniach zagrażających krajowemu, wojskowemu, gospodarczemu lub ekologicznemu bezpieczeństwu Federacji Rosyjskiej (sekcja 2 OSAA). Dnia 25 grudnia 2008 sekcja ta została zmieniona poprzez dodanie kolejnego celu, jakim jest uzyskiwanie informacji o mieniu, będącym przedmiotem konfiskaty.

27.  Urzędnicy państwowi oraz służby wykonujące czynności operacyjno-rozpoznawcze w swoich działaniach muszą wykazywać się poszanowaniem dla życia prywatnego i rodzinnego, domu i korespondencji obywateli. Zakazane jest wykonywanie działań operacyjno-rozpoznawczych służących osiągnięciu innych celów niż te wymienione w Ustawie (sekcja 5(1) i (2) OSAA).

28.  Urzędnicy państwowi i służby nie mogą (1) prowadzić działań operacyjno-rozpoznawczych w interesie partii politycznych, organizacji non-profit lub religijnych (2) prowadzić tajnych działań operacyjno-rozpoznawczych dla władz federalnych, regionalnych lub miejskich, partii politycznych, organizacji non-profit lub religijnych w celu wywarcia wpływu na ich działania lub decyzje; (3) udostępniać komukolwiek dane zebrane w toku działań operacyjno-rozpoznawczych, jeżeli dane te dotyczą życia prywatnego lub rodzinnego lub mogłyby zniszczyć czyjąś reputację lub dobre imię, z wyłączeniem sytuacji wyszczególnionych w ustawach; (4) podżegać skłaniać lub wciągać innych do popełniania przestępstwa; (5) fałszować wyniki działań operacyjno-rozpoznawczych (sekcja 5(8) OSAA).

29. Czynności operacyjno-rozpoznawcze obejmują, *inter alia*, przechwytywanie pocztowych, telegraficznych, telefonicznych i innych form komunikacji, a także zbieranie danych z kanałów technicznych komunikacji. Ustawa stanowi, że nagrywanie audio i video, fotografowanie, filmowanie i inne środki techniczne mogą był używane podczas działań operacyjno-rozpoznawczych, pod warunkiem, że nie są szkodliwe dla życia lub zdrowia osób, których dotyczą lub dla środowiska. Czynności operacyjno-rozpoznawcze uwzględniające przechwytywanie pocztowych, telegraficznych, telefonicznych i innych form komunikacji i zbierania danych z kanałów technicznych komunikacji, przy wykorzystaniu urządzenia zainstalowanego przez dostawców usług komunikacyjnych są podejmowane przez środki techniczne przez FSB i organy Ministerstwa Spraw Wewnętrznych, zgodnie z decyzjami i umowami zawartymi pomiędzy organizacjami w to zaangażowanymi (sekcja 6 OSAA).
30. Dekret Prezydenta nr 891 z dnia 1 września 1995 stanowi, że przechwytywanie pocztowych, telegraficznych i innych transmisji komunikacyjnych jest podejmowane przez FSB w interesie i w imieniu organów śledczych (par.1). W sytuacjach, w których FSB nie posiada potrzebnych urządzeń technicznych, przechwytywanie może być dokonywane przez organy Ministerstwa Spraw Wewnętrznych w imieniu organów śledczych (par.2). Podobne przepisy są zawarte w par. 2 i 3 Rozporządzenia nr 538 wydanego przez Rząd w dniu 27 sierpnia 2005.

D.  Sytuacje, które wzbudzały podejrzenia co do przechwytywania komunikacji

31.  Czynności operacyjno-rozpoznawcze obejmujące ingerencję w konstytucyjne prawo do prywatności komunikacji pocztowej, telegraficznej i innej środkami sieci telekomunikacyjnej lub poprzez usługi mailowe, a także w prywatność mieszkania, mogą być prowadzone w celu uzyskania następujących informacji: (1) że przestępstwo zostało popełnione lub jest popełniane, a także gdy jest planowane (2) o osobach konspirujących w celu popełnienia, popełniających oraz takich, które już popełniły przestępstwa (3) o zdarzeniach lub działaniach zagrażających bezpieczeństwu narodowemu, militarnemu, gospodarczemu lub ekologicznemu Federacji Rosyjskiej (sekcja 8(2) OSAA).

32.  OSAA stanowi, że ingerencja w telefoniczną i inną komunikację może być zgodna z prawem tylko w sytuacjach, gdy osoba jest podejrzana lub oskarżona o przestępstwo średniej wagi, poważne przestępstwo lub szczególnie poważne przestępstwo (sekcja 8(4) OSAA). KPK stanowi również, że przechwytywanie telefonicznej lub innej korespondencji osoby podejrzanej, oskarżonej i innej, może być zgodne z prawem, jeżeli zaistniały powody, aby twierdzić, że mogą zawierać informacje istotne dla sprawy karnej w związku z przestępstwem średniej wagi, poważnym przestępstwem lub szczególnie poważnym przestępstwa (art. 186 § 1 KPK).

33.  Art. 15 KK stanowi, że „przestępstwa średniej wagi” są przestępstwami umyślnymi, za które KK przewiduje maksymalny wymiar kary w wysokości od trzech do pięciu lat pobawienia wolności lub przestępstwami nieumyślnymi, za które KK przewiduje karę powyżej trzech lat pozbawienia wolności. „Poważne przestępstwa” to przestępstwa popełnione umyślnie, za które KK przewiduje maksymalną karę od pięciu do dziesięciu lat pozbawienia wolności. “Szczególnie poważne przestępstwa” to przestępstwa popełnione umyślnie, za które KK przewiduje maksymalną karę powyżej dziesięciu lat pozbawienia wolności lub karę surowszą.

E.  Procedura upoważnienia i limity czasowe

1.  Ustawa o Działaniach Operacyjno-Rozpoznawczych

34.  Środki operacyjno-rozpoznawcze ingerujące w konstytucyjne prawo do prywatności komunikacji pocztowej, telegraficznej lub innej, transmitowanej środkami sieci telekomunikacyjnej lub usługami mailowymi lub w prywatność mieszkania – takie jak inspekcja pomieszczeń lub budynków, przechwytywanie transmisji komunikacji pocztowej, telegraficznej, telefonicznej i innej lub zbieranie danych z kanałów technicznej komunikacji – mogą być podejmowane wyłącznie po uzyskaniu uprzedniego upoważnienia sądowego (sekcja 8(2) OSAA).

35.  W pilnych sprawach, gdzie występuje bezpośrednie niebezpieczeństwo poważnego lub szczególnie poważnego popełnienia przestępstwa lub kiedy pojawiła się informacja o zdarzeniach lub działaniach zagrażających bezpieczeństwu narodowemu, wojskowemu, gospodarczemu lub ekologicznemu, środki operacyjno-rozpoznawcze określone w sekcji 8(2), mogą zostać użyte dopiero po uzyskaniu uprzedniego sądowego upoważnienia. W takich przypadkach sędzia musi zostać poinformowany w ciągu dwudziestu czterech godzin od rozpoczęcia działań operacyjno-rozpoznawczych. Jeżeli upoważnienie sądowe nie zostanie uzyskane w ciągu dwudziestu czterech godzin od rozpoczęcia działań operacyjno-rozpoznawczych, działania te muszą zostać natychmiast wstrzymane (sekcja ustęp 8(3) Ustawy).

36.  Zbadanie wniosku o powzięcie środków ingerujących w konstytucyjne prawo do prywatności korespondencji oraz telefonicznej, pocztowej, telegraficznej lub innej komunikacji transmitowanej przez środki sieci telekomunikacyjnych lub usług mailowych lub w prawo mieszkania, podlega kompetencjom sądu właściwego miejscowo dla miejsca podjęcia danych środków lub siedziby organu właściwego do ich podjęcia. Wniosek musi zostać zbadany niezwłocznie przez sąd w składzie jednego sędziego (ustęp 9(1) Ustawy).

37.  Sędzia wydaje postanowienie na podstawach uzasadnionego wniosku złożonego przez szefa danego organu, właściwego do podjęcia działań operacyjno-rozpoznawczych. Odpowiednie materiały popierające wniosek, z wyłączeniem materiałów zawierających informację o agentach działających pod przykryciem lub informatorach policyjnych, a także o organizacji i taktyce środków operacyjno-rozpoznawczych, powinny zostać dostarczone, gdy sędzia ich zażąda ( ustęp 9(2) i (3) Ustawy).

38.  Sędzia badający wniosek powinien wydać postanowienie o dopuszczalności podjęcia środków ingerujących w wyżej wymienione prawa konstytucyjne lub odmowie ich podjęcia, przedstawiając powody wydania odpowiedniego rozstrzygnięcia. Sędzia musi określić czas, na jaki wydawane jest upoważnienie, który z reguły nie powinien przekraczać sześciu miesięcy. Jeżeli jest to konieczne, sędzia może przedłużyć upoważnienie po ponownym zbadaniu wszystkich istotnych materiałów (ustęp 9(4) i (4) Ustawy).

39.  Postanowienie upoważniające do czynności operacyjno-rozpoznawczych oraz materiały, które posłużyły jako podstawa do wydania takiego rozstrzygnięcia, muszą być w wyłącznym posiadaniu organu rządowego podejmującego czynności operacyjno-śledcze (ust. 12(3) Ustawy).

40.  Dnia 14 lipca 1998 Trybunał Konstytucyjny w swojej decyzji nr 86-O, oddalił jako niedopuszczalny wniosek o zbadanie konstytucyjności niektórych przepisów OSAA. Uznał, w szczególności, że sędzia jest uprawniony do wydania rozstrzygnięcia w przedmiocie dopuszczalności środków śledczych ingerujących w prawa konstytucyjne, jeżeli zostanie wykazane, że środki te są zgodne z prawem, konieczne i usprawiedliwione oraz że są zgodne ze wszystkimi wymogami OSAA. Ciężar dowodu leży po stronie wnioskującego organu rządowego, który musi udowodnić konieczność podjęcia środków. Materiały dostarczone w celu poparcia wniosku powinny zostać zaprezentowane sędziemu na jego żądanie. Mając na uwadze, że niektóre z tych materiałów mogą zawierać tajemnicę państwową, wyłącznie sędziowie posiadający wymagany stopień poświadczenia bezpieczeństwa mogą zbadać wniosek [w przedmiocie upoważnienia do podjęcia czynności operacyjno-rozpoznawczych] Co więcej, mając na uwadze tajemnicę środków nadzoru, Trybunał Konstytucyjny podniósł, że zasady rozprawy publicznej, a także postępowania dowodowego nie są stosowane w przypadku tych postępowań. Fakt, że osoba, której postępowanie dotyczy nie jest uprawniona do brania udziału w tych postępowaniach, ani do uzyskania informacji o podjętych decyzjach, a także do ich zaskarżenia do sądu wyższej instancji, nie narusza praw konstytucyjnych tej osoby.

41.  Dnia 2 października 2003 Trybunał Konstytucyjny uznał w swojej decyzji nr 345-O, że sędzia ma obowiązek uważnego i dokładnego zbadania przedstawionych mu materiałów na poparcie wniosku o przechwytywanie komunikacji. Jeżeli wniosek nie został wystarczająco udowodniony, sędzia może zażądać dodatkowych informacji.

42.  Następnie, 8 lutego 2007 Trybunał Konstytucyjny w swojej decyzji nr 1-O oddalił jako niedopuszczalny wniosek o sprawdzenie konstytucyjności ustępu 9 OSAA. Trybunał uznał, że przed przyznaniem upoważnienia do podjęcia czynności operacyjno-rozpoznawczych, sędzia ma obowiązek zweryfikowania podstaw do podjęcia tego środka. Rozstrzygnięcie sądowe upoważniające do podjęcia środków operacyjno-rozpoznawczych powinno zawierać powody, a także odwoływać się do konkretnych przyczyn uzasadniających podejrzenie o popełnieniu przestępstwa, jego popełnianiu lub jego planowanym popełnieniu, a także o zaistnieniu działań zagrażających bezpieczeństwu narodowemu, wojskowemu, gospodarczemu lub ekologicznemu, a także o tym, że osoba, w stosunku do której środki operacyjno-rozpoznawcze miałyby zostać podjęte, jest zaangażowana w te przestępstwa lub w inne stanowiące zagrożenie działania.

43.  Dnia 15 lipca 2008 Trybunał Konstytucyjny w swojej decyzji nr 460-O, oddalił jako niedopuszczalny wniosek o zbadanie konstytucyjności ustępów 5, 11 i 12 OSAA. Trybunał Konstytucyjny uznał, że osoba, której komunikacja została przechwycona, jest upoważniona do złożenia zażalenia na postanowienie sądowe upoważaniające do przechwytywania komunikacji. Fakt, że [dana osoba] nie posiada odpisu tego postanowienia nie odbiera jej prawa do złożenia zażalenia, ponieważ właściwy sąd może zażądać tego odpisu od odpowiednich władz.

2.  Kodeks Postępowania Karnego

44.  Działania dochodzeniowe obejmujące przeszukanie mieszkania lub przechwytywanie czyichś połączeń telefonicznych i innej komunikacji są przedmiotem uprzedniego upoważnienia sądowego. Wniosek o przeszukanie mieszkania lub przechwycenie komunikacji danej osoby musi być złożony przez oficera śledczego za zgodą prokuratora i musi zostać rozpoznany przez sędziego w ciągu dwudziestu czterech godzin. Prokurator i oficer śledczy są upoważnieni do wzięcia udziału w postępowaniu. Sędzia rozpoznający wniosek powinien zadecydować, czy przyznać upoważnienie do podjęcia odpowiednich działań, czy odmówić [wydania upoważnienia] podając [przy tym] powody [odmowy] (Art. 165 KPK).

45.  Sąd przyznaje upoważnienie do przechwytywania transmisji komunikacyjnej podejrzanego, oskarżonego lub innej osoby, jeżeli zaistniały przesłanki do stwierdzenia, iż w jej ramach mogą być przekazywane informacje istotne dla danej sprawy karnej (art. 186 § 1 KPK).

46.  Wniosek o upoważnienie do przechwytywania komunikacji musi wskazywać: (1) sprawę karną, której dotyczy; (2) podstawy dla powzięcia odpowiednich czynności; (3)nazwisko, imię i nazwisko rodowe osoby, której komunikacja miałaby być przechwytywana; (4) czas trwania czynności; (5) organ rządowy, który podejmie się przechwytywania (art. 186 § 3 KPK).

47.  Postanowienie sądowe upoważniające do przechwytywania transmisji komunikacyjnej musi być przekazane przez oficera śledczego do organu śledczego zobowiązanego do jego implementacji. Przechwytywanie transmisji komunikacyjnej może być dozwolone przez okres nieprzekraczający sześciu miesięcy i jest przerywane przez oficera śledczego, kiedy ustanie taka konieczność. Musi zostać przerwane w każdej sytuacji, jeżeli dochodzenie dobiegło końca (art. 186 § 4 i 5 KPK).

48.  Sąd może również zezwolić na monitorowanie danych komunikacji związanych z telefonem osoby lub jej połączeń bezprzewodowych, jeżeli zaistnieje podejrzenie, że dane te mogą być istotne w sprawie karnej. Wniosek o upoważnienie musi zawierać te same elementy, o których mowa w par. 46 powyżej. Kopia postanowienia sądowego upoważniającego do nadzorowania komunikacji danej osoby przekazywana jest przez oficera śledczego do odpowiedniego dostawcy usług komunikacyjnych, który zostaje zobowiązany do przekazywania danych do oficera śledczego co najmniej raz w tygodniu. Nadzorowanie komunikacji może być dozwolone przez okres nieprzekraczający sześciu miesięcy i jest przerywane przez oficera śledczego, kiedy taka konieczność dobiegnie końca. Musi zostać przerwane każdej sytuacji, jeżeli dochodzenie dobiegło końca (art. 186.1 KPK dodany 1 lipca 2010).

F.  Przechowywanie, wykorzystanie i zniszczenie zebranych danych

1.  Przechowywanie zebranych danych

49. Ustęp 10 OSAA stanowi, że organy ścigania wykonujące czynności operacyjno-rozpoznawcze mogą tworzyć i wykorzystywać bazy danych lub jawne akta osobowe. Akta osobowe muszą być zamknięte, jeżeli cel określony w ust. 2 OSAA został osiągnięty lub ustalono, że jest niemożliwy do osiągnięcia.

50.  W swojej decyzji z 14 lipca 1998 (cyt. par. 40 powyżej) Trybunał Konstytucyjny w odniesieniu do przewidzianego w ust. 10 uprawnienia organów śledczych prowadzących czynności operacyjno-rozpoznawcze do tworzenia baz danych lub jawnych akt osobowych zauważył, że tylko w przypadkach dotyczących prewencji lub śledztwa, dane te mogą zostać umieszczone w bazach danych lub aktach osobowych. Mając na uwadze fakt, że działania przestępcze nie wchodzą w sferę życia prywatnego, zbieranie informacji o takich działaniach nie ingeruje w prawo do poszanowania życia prywatnego. Jeżeli informacje o działaniach przestępczych zostaną umieszczone w aktach, a nie będą one następnie udowodnione, akta osobowe muszą zostać zamknięte.

51.  Nagrania przechwyconych komunikacji telefonicznych i innych muszą być opieczętowane i przechowywane w warunkach wyłączających niebezpieczeństwo ich wysłuchania lub skopiowania przez nieuprawnioną osobę (ust. 8(4) OSAA).

52.  Informacje o urządzeniach wykorzystanych przy czynnościach operacyjno-rozpoznawczych, użytych metodach, urzędnikach zaangażowanych w zbieranie danych stanowią tajemnicę państwową, Informacje te mogą zostać wyłączane z tajemnicy państwowej tylko na mocy decyzji szefa organu rządowego wykonującego czynności operacyjno-rozpoznawcze (ust. 12(1) OSAA i ust. 5(4) Ustawy o Tajemnicy Państwowej, Ustawa nr 5485-I z dnia 21 lipca 1993).

53.  Materiały zawierające tajemnicę państwową powinny zawierać oznaczenia wskazujące następujące informacje: stopień tajemnicy, organ rządowy podejmujący decyzję o ich klasyfikacji, numer rejestracyjny, data i warunki zmiany ich klasyfikacji (ust. 12 Ustawy i Tajemnicy Państwowej).

2.  Wykorzystanie zebranych danych i warunki ich ujawnienia

54.  Informacje zawierające tajemnicę państwową mogą być ujawnione innemu organowi władzy państwowej, organizacji lub osobie fizycznej tylko po wydaniu uprawnienia przez władze państwowe, które podjęły decyzje o odpowiednim zakwalifikowaniu danych informacji. Można ujawnić te informacje wyłącznie władzom państwowym posiadającym specjalne uprawnienie lub osobom fizycznym z wymaganym poświadczeniem bezpieczeństwa. Władze państwowe lub organizacje, którym zaklasyfikowane informacje są ujawnione, muszą zapewnić, że informacje są adekwatnie chronione. Osoba kierująca organem władzy państwowej lub organizacji jest osobiście odpowiedzialna za ochronę zaklasyfikowanych informacji przed nieuprawnionym dostępem lub ujawnieniem (ust. 16 i 17 Ustawy o Tajemnicy Państwowej).

55.  Uprawnienie do dostępu do tajemnicy państwowej może być wydane organizacji lub firmie tylko po potwierdzeniu, że posiada ona specjalne wewnętrzne sekcje, odpowiedzialne za ochronę danych, to znaczy wykwalifikowanych pracowników do pracy z zakwalifikowanymi informacjami i wykorzystuje potwierdzone systemy ochrony danych (ust. 27 Ustawy o Tajemnicy Państwowej).

56.  Poświadczenie bezpieczeństwa jest przyznawane wyłącznie tym organom krajowym, które rzeczywiście potrzebują go do wykonywania swoich obowiązków. Jest również przyznawane sędziom na okres ich pracy, a także obrońcom biorącym udział w sprawie karnej, jeżeli akta sprawy zawierają materiały z tajemnicą państwową. Każdy, komu przyznano poświadczenie bezpieczeństwa musi przedstawić pisemne zobowiązanie o nieudostępnianiu powierzonych mu zakwalifikowanych informacji (par. 7, 11, 21 Regulacji nr 63 z dnia 6 lutego 2010 Rządu Federacji Rosyjskiej).

57.  Osoba kierująca organem władz państwowych lub organizacji będących w posiadaniu informacji zawierających tajemnicę państwową jest odpowiedzialna za udostępnianie tych informacji organom krajowym i innym osobom uprawnionym. Musi ona zapewnić, że udostępnione zostaną tylko te informacje, których odbiorca potrzebuje do wykonywania swoich obowiązków (ust. 25 Ustawy o Tajemnicy Państwowej).

58.  Jeżeli dane zebrane w toku czynności operacyjno-rozpoznawczych zawierają informacje o popełnieniu przestępstwa, informacje te, łącznie ze wszystkimi materiałami potwierdzającymi, takimi jak fotografie, nagraniami audio lub video, muszą zostać wysłane do właściwego organu śledczego lub do sądu. Jeżeli informacje zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych (w tym poprzez ingerencję w prawo do prywatności komunikacji pocztowej, telegraficznej i innej, transmitowanej środkami sieci telekomunikacyjnej lub usługami mailowymi lub prawo do mieszkania), muszą one zostać wysłane do organu śledczego lub prokuratorskiego łącznie z postanowieniem sądowym upoważniającym do podjęcia tych czynności. Informacje muszą zostać transmitowane zgodnie ze specjalną procedurą dotyczącą posługiwania się zakwalifikowanymi informacjami, chyba że organy rządowe podejmujące czynności operacyjno-rozpoznawcze zdecydowały o ich zdeklasyfikowaniu (par. 1, 12, 14 i 16 Rozporządzenia nr 776/703/509/507/1820/42/535/398/68 z dnia 27 września 2013 Ministra Spraw Wewnętrznych).

59.  Jeżeli osoba, której komunikacja telefoniczna lub inna była przechwytywana została oskarżona, nagrania powinny zostać przekazane oficerowi śledczemu oraz załączone do akt sprawy. Ich dalsze wykorzystanie i przechowywanie jest regulowane przepisami z zakresu postępowania karnego (ust. 8(5) OSAA).

60.  Dane zebrane w wyniku czynności operacyjno-rozpoznawczych mogę być wykorzystane do przygotowania i prowadzenia dochodzenia i postępowania sądowego, a także wykorzystane jako dowód w postępowaniu karnym, zgodnie z przepisami prawa regulującymi zbieranie i ocenę dowodów. Decyzję o przekazaniu zebranych danych do organów śledczych lub do sądów podejmuje przewodniczący organu rządowego podejmującego czynności operacyjno-rozpoznawcze (ust. 11 OSAA).

61. Jeżeli przechwytywanie danych było dozwolone w ramach postępowań karnych, oficer śledczy może w czasie obowiązywania upoważnienia uzyskać nagrania od organu wykonującego odpowiednie czynności. Nagrania muszą być opieczętowane oraz opatrzone listem wskazującym datę i czas rozpoczęcia oraz zakończenia nagrywanych komunikacji oraz środków technicznych wykorzystywanych do ich przechwytywania. Nagrania muszą być wysłuchane przez oficera śledczego w obecności świadków, w razie konieczności eksperta oraz osób, których komunikacje były przechwytywane. Oficer śledczy musi sporządzić oficjalny raport zawierający dosłowną transkrypcję tych części, które są istotne dla sprawy (art. 186 § 6 i 7 KPK). Dnia 4 marca 2013 art. 186 § 7 został zmieniony i wymaganie dotyczące obecności świadków zostało usunięte.

62.  Nagrania i dane uzyskane z komunikacji są dołączane do akt sprawy. Muszą zostać opieczętowane i przechowywane w warunkach wyłączających jakiekolwiek ryzyko ich odsłuchania lub skopiowania przez nieupoważnione osoby (art. 186 § 8 KPK i art. 186.1 dodany 1 lipca 2010).

63.  Wyniki czynności operacyjno-rozpoznawczych zawierających ograniczenie prawa do poszanowania korespondencji, komunikacji telefonicznej, pocztowej, telegraficznej i innej mogą być wykorzystane jako dowód w postępowaniu karnym tylko wtedy, jeżeli zostały uzyskane zgodnie z nakazem sądowym, a także jeżeli czynności operacyjno-rozpoznawcze zostały dokonane zgodnie z regulacjami z zakresu postępowania karnego (par. 14 Orzeczenia nr 8 z dnia 31 października 1995 przez Plenarny Sąd Najwyższy Federacji Rosyjskiej).

64.  Zabronione jest wykorzystanie jako dowód danych uzyskanych w wyniku czynności operacyjno-rozpoznawczych, które nie spełniają wymogów dopuszczalności dowodów KPK (art. 89 KPK). Dowody uzyskane z naruszeniem KPK są niedopuszczalne. Niedopuszczalny dowód nie posiada mocy prawnej i nie może być wykorzystany do sformułowania zarzutów karnych lub do udowodnienia okoliczności, do których dowód jest wymagany w postępowaniu karnym. Jeżeli sąd postanowi o wyłączeniu dowodu, dowód ten nie ma mocy prawnej i nie można na jego podstawie wydać orzeczenia ani żadnej innej decyzji, nie można go badać ani wykorzystywać w trakcie procesu (art. 75 i art. 235 KPK).

3.  Zniszczenie zebranych danych

65.  Dane zebrane w trakcie czynności operacyjno-rozpoznawczych w stosunku do osoby, której wina nie została udowodniona w związku z procedurą przewidzianą przez prawo, muszą być przechowywane przez jeden rok, a następnie zniszczone, chyba że informacje są potrzebne dla wymiaru sprawiedliwości. Nagrania audio i inne materiały zebrane w wyniku przechwytywania komunikacji telefonicznej lub innych, muszą być przechowywane przez sześć miesięcy, a następnie zniszczone, jeżeli osoba nie została do tej pory oskarżona. Sędzia, który zezwolił na przechwytywanie komunikacji musi zostać poinformowany o wyznaczonym terminie zniszczenia trzy miesiące przed jego wykonaniem (ust. 5(7) OSAA).

66. Jeżeli osoba została oskarżona, w ostatniej fazie postępowania karnego sąd wydaje postanowienie o dalszym przechowywaniu danych wykorzystanych jako dowód lub ich zniszczeniu. Zniszczenie musi zostać odnotowane w raporcie, który musi zostać podpisany przez przewodniczącego organu śledczego oraz włączony do akt sprawy (art.81 § 3 KPK i par. 49 Rozporządzenia nr 142 z dnia 30 września 2011 Komitetu Śledczego).

G.  Nadzór nad przechwytywaniem transmisji komunikacyjnej

67.  Szefowie organów prowadzących czynności operacyjno-rozpoznawcze ponoszą osobistą odpowiedzialność za zgodność z prawem wszystkich czynności operacyjno-rozpoznawczych (ust. 22 OSAA).

68.  Całościowy nadzór nad czynnościami operacyjno-rozpoznawczymi jest wykonywany przez Prezydenta, Parlament i Rząd Federacji Rosyjskiej w zakresie ich kompetencji (ust. 20 OSAA).

69.  Prokurator Generalny i właściwi prokuratorzy mogą również wykonywać nadzór nad czynnościami operacyjno-rozpoznawczymi. W wyniku wniosku kompetentnego prokuratora, szef organu rządowego podejmującego czynności operacyjno-rozpoznawcze, musi dostarczyć materiały operacyjno-rozpoznawcze, w tym także: akta personalne, informacje o wykorzystaniu sprzętu technicznego, logi rejestracyjne i instrukcje wewnętrzne. Materiały zawierające informacje o agentach działających pod przykryciem lub policyjnych informatorach mogą zostać ujawnione prokuratorowi wyłącznie za zgodą agenta lub informatora, wyłączając przypadki postępowań karnych przeciwko nim. Szef agencji rządowej może zostać pociągnięty do odpowiedzialności zgodnie z prawem za niewykonanie żądania prokuratora. Prokurator musi zapewnić ochronę danych zawartych w dostarczonych materiałach (ust. 21 OSAA).

70.  Ustawa o Prokuraturze (Ustawa federalna nr 2202-I z dnia 17 stycznia 1992) stanowi, że Prokurator generalny jest mianowany lub odwoływany przez Radę Federacyjną (wyższa izba parlamentu) po uprzedniej propozycji kandydatury przez Prezydenta (ust.12). Pozostali prokuratorzy mianowani są przez Prokuratora Generalnego po konsultacji z władzami lokalnymi (ust. 13). By zostać mianowanym na stanowisko prokuratora, należy posiadać obywatelstwo rosyjskie oraz tytuł prawny zdobyty w Rosji (ust.40.1).

71.  Dodatkowo oprócz funkcji prokuratorskich, prokuratorzy są odpowiedzialni za nadzór nad zgodnością z Konstytucją i prawem rosyjskim administracji zakładów karnych, działalności komorników, czynności operacyjno-rozpoznawczych i śledztw (ust. 1). Prokuratorzy również koordynują działania wszystkich organów rządowych w zwalczaniu przestępczości (ust. 8).

72.  Co się tyczy nadzoru czynności operacyjno-rozpoznawczych, prokuratorzy mogą sprawdzać, czy środki podjęte w toku czynności operacyjno-rozpoznawczych są zgodne z prawem i z zasadą poszanowania praw człowieka (ust. 29). Polecenia prokuratorów wydawane w kontekście takiego nadzoru muszą być zgodne z wyznaczonym limitem czasowym. Niespełnienie tego wymogu może skutkować odpowiedzialnością prawną (ust.6).

73.  Prokuratorzy mogą również rozpoznawać skargi o naruszenie prawa i wydawać uzasadnione decyzje w przedmiocie tych skarg. Decyzja taka nie uniemożliwia wniesienia tej samej skargi do sądu. Jeżeli prokurator stwierdzi naruszenie prawa, musi podjąć środki, aby dana osoba poniosła odpowiedzialność prawną (ust. 10).

74.  Ustawa o Federalnych Służbach Bezpieczeństwa z dnia 3 kwietnia 1995 (nr 40-FZ, zwana dalej “Ustawa FSB”) stanowi, że informacja o agentach służby bezpieczeństwa działających pod przykryciem, jak i o taktyce, metodach i środkach przez nich używanych znajduje się poza zakresem prokuratorskiego nadzoru (ust. 24).

75.  Procedury nadzoru prokuratorskiego nad czynnościami operacyjno-rozpoznawczymi, zostały określone w Rozporządzeniu nr 33 wydanym przez Biuro Prokuratora Generalnego w dniu 15 lutego 2011.

76.  Rozporządzenie nr 33 stanowi, że prokuratorzy mogą wykonywać rutynowe inspekcje organów wykonujących czynności operacyjno-rozpoznawcze oraz inspekcje *ad hoc* w przypadku otrzymania poszczególnej skargi lub informacji o potencjalnych naruszeniach. Czynności operacyjno-rozpoznawcze wykonywane przez FSB w zakresie kontrwywiadu mogą zostać skontrolowane tylko w przypadku otrzymania skargi indywidualnej (par. 5 Rozporządzenia nr 33).

77.  Podczas inspekcji prokurator musi zweryfikować, czy spełnione zostały następujące wymagania:

-  przestrzeganie praw konstytucyjnych obywateli, takich jak prawo do prywatności i życia rodzinnego, mieszkania, korespondencji, komunikacji telefonicznej, pocztowej, telegraficznej i innej;

-  legalność i zasadność środków podjętych w ramach czynności operacyjno-rozpoznawczych, w tym także środki, na których zastosowanie sąd wydał zgodę (par. 4 i 6 Rozporządzenia nr 33).

78.  Podczas inspekcji prokurator musi zbadać oryginały materiałów operacyjno-rozpoznawczych, w tym także akta personalne, informacje o wykorzystaniu urządzeń technicznych, logów rejestracyjnych i instrukcji wewnętrznych oraz może zażądać wyjaśnień od właściwych władz. Prokuratorzy muszą chronić powierzone im dane wrażliwe przed nieupoważnionym dostępem lub ujawnieniem (par. 9 i 12 Rozporządzenia nr 33).

79.  Jeżeli prokurator stwierdzi naruszenie prawa, musi zażądać od odpowiednich władz usunięcia tego naruszenia. Musi również powziąć środki, aby zaprzestać tego naruszenia praw obywateli oraz zadośćuczynić, a także pociągnąć właściwe osoby do odpowiedzialności (par. 9 i 10 Rozporządzenia nr 33). Organ rządowy, który odmawia zastosowania się do poleceń prokuratora, może zostać pociągnięty do odpowiedzialności prawnej (par. 11).

80.  Prokuratorzy odpowiedzialni za nadzór nad czynnościami operacyjno-rozpoznawczymi muszą składać raporty sześciomiesięczne, wyszczególniające wyniki inspekcji do Biura Prokuratora Generalnego (par. 15 Rozporządzenia nr 33). Formularz raportu do uzupełnienia przez prokuratora jest załączony do Rozporządzenia nr 33 i jest on poufny. Zawiera dwie sekcje, obie w formie tabeli. Pierwsza sekcja dotyczy inspekcji powziętej w tym czasie i zawiera informacje o ilości inspekcji, ilości zbadanych akt oraz ilości wykrytych naruszeń. Druga sekcja dotyczy skarg obywateli i zawiera informacje o ilości skarg zbadanych i uznanych za zasadne.

H.  Dostęp osób fizycznych do danych o nich zebranych w toku przechwytywania komunikacji

81.  Prawo rosyjskie nie zapewnia, że osoba, której komunikacje są przechwytywane, musi być w którymś momencie o tym poinformowana. Jednakże, osoba która jest w posiadaniu faktów o środkach operacyjno-rozpoznawczych, którym została poddana i czyjej wina nie została udowodniona zgodnie z procedurą przewidzianą przez prawo (tzn. nie została oskarżona lub zarzuty wobec niej zostały oddalone na tej podstawie, że rzekome przestępstwo nie zostało popełnione lub, że nie ziściły się znamiona określonego przestępstwa), jest upoważniona do otrzymania informacji o danych zebranych w toku czynności operacyjno-rozpoznawczych w zakresie zgodnym z wymaganiami poufności operacyjnej (“*конспирации*”) (wyłączając dane, które mogłyby doprowadzić do ujawnienia tajemnic państwowych) (ust. 5(4-6) OSAA).

82.  W swojej decyzji z dnia 14 lipca 1998 (cyt. par. 40 powyżej) Trybunał Konstytucyjny zauważył, że każda osoba będąca w posiadaniu wiedzy o czynnościach operacyjno-rozpoznawczych, którym została poddana jest uprawniona to otrzymania informacji o danych zebranych w toku tych czynności, chyba że dane te zawierały tajemnice państwowe. Na mocy ustępu 12 OSAA, dane zebrane w toku czynności operacyjno-rozpoznawczych – takie jak informacje o przestępstwach i osobach zaangażowanych w ich popełnienie – są objęte tajemnicą państwową. Jednakże, informacje o naruszeniu praw obywateli lub bezprawnych działaniach po stronie władz nie mogły być zaklasyfikowane jako tajemnica państwowa i powinny zostać ujawnione. Ustęp 12 nie może zatem służyć za podstawę odmowy dostępu do informacji dotyczących praw osoby, jeśli informacja taka nie zawierała celu lub podstaw czynności operacyjno-rozpoznawczych. W związku z powyższym, zgodnie z zakwestionowaną Ustawą, jeżeli dana osoba nie była uprawniona do dostępu do całości zgromadzonych informacji, to nie stanowi to naruszenia praw konstytucyjnych tej osoby.

I.  Pogląd judykatury

1.  Ogólne zasady kontroli sądowej przechwytywania komunikacji według OSAA

83.  Osoba twierdząca, że jej prawa są lub zostały naruszone przez władze państwowe wykonujące czynności operacyjno-rozpoznawcze, może złożyć skargę do przełożonego danego urzędnika, prokuratora lub sądu. Jeżeli prawa obywatela zostały pogwałcone w toku czynności operacyjno-rozpoznawczych przez władze państwowe, przełożony danego urzędnika, prokurator lub sąd muszą podjąć środki, aby zaprzestać naruszeniu oraz zrekompensować krzywdę (sekcja 5(3) i (9) OSAA).

84.  Jeżeli danej osobie odmówiono dostępu do informacji o danych o niej zebranych w toku czynności operacyjno-rozpoznawczych, to jest ona uprawniona do poznania powodów odmowy oraz może odwoływać się od tej decyzji do sądu. Ciężar dowodu spoczywa na organach ścigania, które muszą udowodnić, że odmowa dostępu jest usprawiedliwiona. Aby zagwarantować pewne i dokładne badanie sądowe, organy ścigania są odpowiedzialne za dostarczenie, na żądanie sędziego, materiałów pochodzących z czynności operacyjno-rozpoznawczych, zawierających informacje o danych, do których odmówiono dostępu, za wyjątkiem materiałów zawierających informacje o agentach działających pod przykryciem lub informatorach policyjnych, Jeżeli sąd uzna, że odmowa przyznania dostępu była nieusprawiedliwiona, może zmusić organy ścigania do ujawnienia materiałów osobie zainteresowanej (sekcja 5(4 do 6) OSAA).

85. W swojej decyzji z dnia 14 lipca 1998 (cyt. w par. 40 powyżej), Trybunał Konstytucyjny zauważył, że osoba, która dowiedziała się o tym, że została poddana czynnościom operacyjno-rozpoznawczym i uważała, że czynności władz państwowych naruszyły jej prawa, jest uprawniona, na mocy sekcji 5 OSAA, do zakwestionowania przed sądem  podstawy prowadzenia takich czynności, jak i szczegółowych działań powziętych przez właściwe władze w toku takich czynności, włączając w to sprawy, w których istniało upoważnienie sądowe.

86.  Co do kwestii proceduralnych, Trybunał Konstytucyjny utrzymał, że w postępowaniach, w których podstawy do powzięcia czynności operacyjno-rozpoznawczych lub działań właściwych władz były zakwestionowane (podobnie jak w postępowaniach dotyczących odmowy przydzielenia dostępu do zebranych danych), organy ścigania mają przedłożyć sędziemu, na jego żądanie, wszystkie właściwe materiały operacyjno-rozpoznawcze, za wyjątkiem materiałów zawierających informacje o agentach działających pod przykryciem lub informatorach policyjnych.

87.  Osoba chcąca złożyć skargę na przechwytywanie jej transmisji komunikacyjnej, może złożyć wniosek o dokonanie kontroli sądowej na podstawie Artykułu 125 KPK; wniosek o dokonanie kontroli sądowej na podstawie Rozdziału 25 Kodeksu Postępowania Cywilnego oraz Ustawy o Rewizji Sądowej zastąpionej od 15 września 2015 r. przez Kodeks Postępowania Administracyjnego, lub skargę na podstawie Artykułu 1069 Kodeksu Cywilnego.

2.  Wniosek o rewizję sądową na mocy Artykułu 125 KPK

88.  Zgromadzenie Ogólne Sądu Najwyższego w swojej uchwale nr 1 z dnia 10 stycznia 2009 r. uznało, że działania urzędników lub władz państwowych prowadzących czynności operacyjno-rozpoznawcze na żądanie śledczego, mogą być zakwestionowane zgodnie z procedurą przewidzianą przez Artykuł 125 KPK (par. 4). Skargi złożone na mocy tego Artykułu mogą być zbadane tylko podczas trwania śledztwa. Jeżeli sprawa została już przekazana do sądu, sędzia uznaje skargę za niedopuszczalną i wyjaśnia skarżącemu, że może złożyć skargę przed właściwym sądem (par. 9).

89.  Artykuł 125 KPK przewiduje rewizję sądową decyzji i działań lub zaniechania działania przez śledczego lub prokuratora, którzy są w stanie negatywnie wpływać na prawa i wolności konstytucyjne uczestników postępowania karnego. Złożenie skargi nie zawiesza stosowania zakwestionowanej decyzji lub działania, chyba że śledczy, prokurator lub sąd uzna przeciwnie. Sąd musi zbadać skargę w ciągu pięciu dni. Skarżący, jego adwokat, śledczy i prokurator są upoważnieni do udziału w rozprawie. Skarżący musi uzasadnić swoją skargę (Artykuł 125 § § 1-5 KPK).

90.  Uczestnicy rozprawy są upoważnieni do zbadania wszystkich materiałów właściwych dla skargi. Ujawnienie materiałów sprawy karnej jest możliwe tylko, jeżeli nie stoi to w sprzeczności z interesem śledztwa i nie narusza praw uczestników postępowania karnego. Sędzia może zażądać od stron przedstawienia materiałów, które stanowiły podstawę dla wydania zakwestionowanej decyzji lub inne właściwe materiały (par. 12 uchwały nr 1 z dnia 10 lutego 2009 Zgromadzenia Ogólnego Sądu Najwyższego Federacji Rosyjskiej).

91.  Podczas badania skargi skarżącego, sąd albo uznaje zakwestionowaną decyzję, działanie lub zaniechanie działania za bezprawne lub nieusprawiedliwione i poucza odpowiedzialnych za to urzędników o konieczności skorygowania wskazanych braków albo oddala skargę (Artykuł 125 § 5 KPK). Podczas pouczania urzędników o skorygowaniu wskazanych braków, sąd może nie wskazywać żadnych szczególnych środków, które urzędnicy powinni powziąć lub uchylić lub nakazać unieważnienie decyzji uznanej za bezprawną bądź nieuzasadnioną (par. 21 Orzeczenia nr 1 z dnia 10 lutego 2009 Plenarnego Sądu Najwyższego Federacji Rosyjskiej).

3.  Wniosek o rewizję sądową zgodnie z Rozdziałem 25 Kodeksu postępowania Cywilnego, Ustawą o Rewizji Sądowej oraz Kodeksem Postępowania Administracyjnego

92.  Uchwała nr 2 z dnia 10 lutego 2009 Zgromadzenia Ogólnego Sądu Najwyższego Federacji Rosyjskiej stanowi, że skargi na decyzje i działania urzędników i organów wykonujących czynności operacyjno-rozpoznawcze, które nie mogą być zakwestionowane w postępowaniu karnym, tak jak skargi na odmowę dostępu do informacji o danych zebranych w toku czynności operacyjno-rozpoznawczych, mogą być zbadane zgodnie z procedurą ustanowioną w Rozdziale 25 Kodeksu Postępowania Cywilnego (par.7).

93.  Rozdział 25 Kodeksu Postępowania Cywilnego (KPC), obowiązującego przed 15 września 2015 r. ustanowił procedurę badania skarg na decyzje i działania urzędników naruszających prawa i wolności obywateli, która następnie została dokładniej opisana w Ustawie o Rewizji Sądowej (Ustawa nr 4866-1 z dnia 27 kwietnia 1993 o Sądowej rewizji decyzji i czynności naruszających prawa i wolności obywateli). Dnia 15 września 2015 r. Rozdział 25 KPC i Ustawa o Rewizji Sądowej zostały uchylone i zastąpione Kodeksem Postępowania Administracyjnego (Ustawa nr 21-FZ z dnia 8 marca 2015, dalej zwana “KPA”), który wszedł w życie tego dnia. KPA potwierdził istotę wcześniejszego rozwiązania oraz doprecyzował przepisy Rozdziału 25 KPK oraz Ustawy o Rewizji Sądowej.

94. Zarówno KPC, Ustawa o Rewizji Sądowej i KPA stanowią, że obywatel może złożyć skargę przed sądem na decyzję lub działanie Państwa lub władzy krajowej albo urzędników, jeżeli uzna, że naruszyły one jego prawa i wolności (Artykuł 254 KPC i sekcja 1 Ustawy o Rewizji Sądowej). Skarga może dotyczyć każdej decyzji, działania lub zaniechania, które naruszyło prawa lub wolności obywatela, utrudniło korzystanie z praw i wolności lub nałożyło na niego obowiązek lub uczyniło go odpowiedzialnym (Artykuł 255 KPC, sekcja 2 Ustawy o Rewizji Sądowej i Artykuł 218 § 1 KPA).

95.  Skarga musi być złożona do sądu powszechnego w ciągu trzech miesięcy od dnia, w którym skarżący dowiedział się o naruszenia jego praw. Limit czasowy może zostać wydłużony ze słusznych powodów (Artykuł 254 KPC, sekcje 4 i 5 Ustawy o rewizji Sądowej oraz Artykuły 2018 § 5 i 219 §§ i 7 KPA). Skarżący musi wskazać numer identyfikacyjny oraz datę zakwestionowanego działania (Artykuł 220 § 2(3) KPA). Skarżący musi złożyć dokumenty potwierdzające lub wyjaśnić, dlaczego nie może ich złożyć (Artykuł 220 §§ 2 (8) i 3 KPA). Jeżeli skarżący nie spełni powyższych wymagań, sędzia uznaje skargę za niedopuszczalną(Artykuł 222 § 3 KPA).

96.  Ciężar dowodu co do legalności zakwestionowanej decyzji, działania lub zaniechania spoczywa na władzach lub urzędnikach, których dotyczy. Skarżący musi jednak udowodnić, że jego prawa i wolności zostały naruszone przez zakwestionowane decyzje, działania lub zaniechania (sekcja 6 Ustawy o Rewizji Sądowej i Artykuł 226 § 11 KPA).

97.  Zgodnie z przepisami KPC skarga musi zostać rozpoznana w ciągu dziesięciu dni (Artykuł 257 KPC), podczas gdy na mocy KPA musi być rozpoznana w ciągu dwóch miesięcy (Artykuł 226 § 1 KPA). Jeżeli sąd uzna skargę za uzasadnioną, wydaje decyzję unieważniająca zakwestionowaną decyzję lub działania i wymaga od władz lub urzędników zadośćuczynienia naruszeniu praw człowieka w całości (Artykuł 258 § 1 KPC, sekcja 7 Ustawy o Rewizji Sądowej oraz Artykuł 227 §§ 2 i 3 KPA). Sąd może określić limit czasowy spełnienia zadośćuczynienia naruszeniu i/lub szczególne kroki, jakie należy podjąć, aby zadośćuczynić naruszeniu w całości (par. 28 Uchwały nr 2 z dnia 10 lutego 2009 Zgromadzenia Ogólnego Sądu Najwyższego Federacji Rosyjskiej oraz Artykuł 227 § 3 KPA). Skarżący może wówczas żądać kompensaty za majątkowe i niemajątkowe szkody w oddzielnym postępowaniu cywilnym (sekcja 7 Ustawy o Rewizji Sądowej).

98.  Sąd może oddalić skargę, jeżeli uzna, że zakwestionowane działanie lub decyzja została podjęta przez kompetentną władzę lub urzędnika, jest legalne i nie narusza praw obywatela (Artykuł 258 § 4 KPC i Artykuły 226 § 9 i 227 § 2 KPA).

99.  Strona postępowania może wnieść odwołanie do sądu wyższej instancji (Artykuł 336 KPC obowiązujący przed 1 stycznia 2012, Artykuł 320 KPC obowiązujący od 1 stycznia 2012 i Artykuł 228 KPA). Decyzja wydana w postępowaniu odwoławczym wchodzi w życie z dniem wydania (Artykuł 367 KPC w mocy do 1 stycznia 2012, Artykuł 329 § 5 w mocy po 1 stycznia 2012 i Artykuły 186 i 227 § 5 KPA).

100.  KPC stanowi, że orzeczenie sądowe na korzyść skarżącego oraz zobowiązujące władze lub urzędników do zadośćuczynienia naruszeniu praw obywatela, ma być doręczone do osoby stojącej na czele władzy lub urzędu, do osoby, której dotyczy lub do jej przełożonych w ciągu trzech dni od jego wydania (Artykuł 258 § 2 KPC). Ustawa o Rewizji Sądowej wymaga, aby orzeczenie sądowe było doręczone w dniu wejścia w życie (Artykuł 227 § 7). Sąd i skarżący muszą zostać powiadomieni o wejściu w życie orzeczenia nie później niż w ciągu jednego miesiąca po jego otrzymaniu (Artykuł 258 § 3 KPC, sekcja 8 Ustawy o Rewizji Sądowej i Artykuł 227 § 9 KPA).

4.  Skarga cywilna na mocy Artykułu 1069 Kodeksu Cywilnego

101.  Wyrządzone szkody majątkowe i niemajątkowe powinny zostać zrekompensowane w całości przez osobę, która popełniła czyn zabroniony. Osoba, która popełniła czyn zabroniony nie jest odpowiedzialna za szkodę, jeżeli udowodniła, że szkoda nie została spowodowana jej winą (Artykuł 1064 §§ 1 i 2 Kodeksu Cywilnego).

102.  Organy państwowe i urzędnicy ponoszą odpowiedzialność za szkody doznane przez obywatela w wyniku ich bezprawnego działania lub zaniechania (Artykuł 1069 Kodeksu Cywilnego). Niezależnie od winy urzędników państwowych, Skarb Państwa lub regionu jest odpowiedzialny w przypadku szkód doznanych przez obywateli ze względu na (i) bezprawne skazanie lub oskarżenie; (ii) bezprawne stosowanie środków zapobiegawczych (iii) bezprawnie nałożoną karę administracyjną (Artykuł 1070 Kodeksu Cywilnego).

103.  Sąd może nałożyć na osobę, która popełniła czyn zabroniony zobowiązanie do rekompensaty za szkody niemajątkowe (fizyczne lub psychiczne cierpienie). Kompensata za szkody niemajątkowe nie jest związana z żadną kompensatą przyznaną za szkody majątkowe (Artykuły 151 § 1 i 1099 Kodeksu Cywilnego). Wysokość kompensaty jest określana poprzez odniesienie się do ciężaru winy osoby, popełniającej czyn zabroniony oraz do innych znaczących okoliczności. Sąd bierze również pod uwagę rozmiar fizycznego lub psychicznego cierpienia w stosunku do indywidualnego charakteru danej osoby (Artykuł 151 § 2 i Artykuł 1101 Kodeksu Cywilnego).

104.  Niezależnie od winy osoby popełniającej czyn zabroniony, szkoda niematerialna będzie zrekompensowana, jeżeli została spowodowana (i) uszkodzonym urządzeniem; (ii) w sytuacji bezprawnego skazania lub oskarżenia lub bezprawnego zastosowania środków zapobiegawczych lub kary administracyjnej, oraz (iii) ze względu na rozpowszechnianie informacji, które były krzywdzące dla honoru, godności lub reputacji (Artykuł 1100 Kodeksu Cywilnego).

105.  W postępowaniach cywilnych strona, która podnosi określone twierdzenie, musi udowodnić to twierdzenie, chyba, że ustawa stanowi inaczej (Artykuł 56 § 1 KPK).

5. Skarga do Trybunału Konstytucyjnego

106. Ustawa o Trybunale Konstytucyjnym (Ustawa nr 1-FKZ z dnia 21 lipca 1994) stanowi, że wyrażona w formie wyroku opinia Trybunału Konstytucyjnego co do tego, czy interpretacja przepisów ustawowych przyjętych przez praktykę prawną lub organy ścigania jest zgodna z Konstytucją musi być przestrzegana przez sądy i organy ścigania od dnia wydania tego wyroku (ust. 79(5)).

J.  Obowiązki dostawców usług komunikacyjnych

1.  Obowiązek ochrony danych osobistych i prywatności komunikacji

107.  Ustawa o komunikacji stanowi, że dostawcy usług komunikacyjnych muszą zapewnić prywatność komunikacji. Informacje o komunikacji transmitowanej środkami sieci telekomunikacyjnych lub usług mailowych oraz o treści tej komunikacji mogą zostać ujawnione tylko nadawcy i odbiorcy lub upoważnionym przez nich pełnomocnikom, z wyłączeniem sytuacji określonych w ustawie (ust. 63(2) i (4) Ustawy o Komunikacji).

108. Informacje o użytkownikach oraz usługach im dostarczanych są poufne. Informacje o użytkownikach zawierają ich nazwisko, imię, nazwisko rodowe i pseudonimy dla osób fizycznych; nazwę firmy i nazwisko, imię i nazwisko rodowe właścicieli firmy oraz osób zatrudnionych w przypadku osób prawnych; adresy zamieszkania użytkowników, numery i inne informacje umożliwiające identyfikację użytkownika i jego terminal; dane z płatniczych baz danych, włączając informacje o komunikacji użytkownika i przepływie płatności. Informacje o użytkownikach nie mogą być ujawniane osobom trzecim bez zgody użytkownika, wyłączając przypadki określone w ustawie (ust. 53 Ustawy o Komunikacji).

2.  Obowiązek współpracy z organami ścigania

109.  Ustawa o Komunikacji nakłada na dostawców usług komunikacyjnych obowiązek dostarczania organom ścigania informacji o użytkownikach i usługach, z których korzystają, w sprawach określonych w prawie federalnym, a także informacji, których wymagają, aby osiągnąć swoje cele (ust. 64(1) Ustawy o Komunikacji).

110. Dnia 31 marca 2008 Rada Miasta Moskwy dyskutowała nad zmianami zaproponowanymi do ust. 64(1) Ustawy o Komunikacji, polegającymi na konieczności przedstawienia sądowego upoważnienia przez organy śledcze dostawcom usług komunikacyjnych, gdy żądają udostępnienia informacji o użytkownikach. Przedstawiciele FSB i Ministerstwa Spraw Wewnętrznych poinformowali, że postanowienia sądowe upoważniające do przechwytywania komunikacji stanowiły dokumenty zaklasyfikowane i z tego powodu nie mogły być przedstawione dostawcom usług komunikacyjnych. Propozycja wprowadzenia zmian została później odrzucona.

111.  Dostawcy usług komunikacyjnych muszą zapewnić, że ich sieci i urządzenia spełniają wymagania techniczne wprowadzone przez Ministra Komunikacji we współpracy z organami ścigania. Dostawcy usług komunikacyjnych muszą również zapewnić, że sposób postępowania stosowany przez organy ścigania pozostanie poufny (ust. 64(2) Ustawy o Komunikacji).

112.  W sytuacjach określonych w ustawie, dostawcy usług komunikacyjnych muszą zawiesić świadczenie usług użytkownikom po otrzymaniu uzasadnionego pisemnego polecenia szefa organu ścigania prowadzącego czynności operacyjno-rozpoznawcze lub chroniącego bezpieczeństwo narodowe (ust. 64(3) Ustawy o Komunikacji).

113.  Ustawa o FSB wymaga od dostawców usług komunikacyjnych zainstalowania urządzenia pozwalającego FSB na prowadzenie czynności operacyjno-rozpoznawczych (ust.15).

3.  Wymagania techniczne dla urządzeń instalowanych przez dostawców usług

114.  Główne cechy systemu urządzeń technicznych umożliwiającego podjęcie czynności operacyjno-rozpoznawczych (“*Система технических средств для обеспечения функций оперативно-разыскных мероприятий” (*‘*СОРМ’)*, w dalszej części zwany jako “SORM”) są wymienione w kilku rozporządzeniach i regulacjach wydanych przez Ministra Komunikacji.

(a)  Rozporządzenie nr 70

115. Rozporządzenie nr 70 w sprawie wymagań technicznych systemu urządzeń technicznych umożliwiającego podjęcie czynności operacyjno-rozpoznawczych przy wykorzystaniu sieci telekomunikacyjnych, wydane przez Ministra Komunikacji w dniu 20 kwietnia 1999 stanowi, że urządzenie zainstalowane przez dostawców usług komunikacyjnych musi spełnić pewne określone wymagania, które są określone w załączniku do Rozporządzenia. Rozporządzenie wraz z załącznikami zostało opublikowane przez Ministerstwo Komunikacji w oficjalnym biuletynie *SvyazInform*,rozpowszechnianym w ramach subskrypcji. Dostępne jest również w prywatnej internetowej bazie aktów prawnych, która odtwarza go z publikacji z *SvyazInform*.

116.  Załączniki nr 1 i 3 opisują techniczne wymagania SOrM dla sieci telefonii komórkowej. Określają, że przechwytywanie komunikacji dokonywane jest przez organy śledcze z terminala zdalnego sterowania połączonego z urządzeniami przechwytywania zainstalowanymi przez operatora sieci komórkowej. Urządzenie musi być w stanie, *inter alia*, (a) tworzyć bazy danych przechwyconych podmiotów, które mogą być zdalnie zarządzane; (b) przechwytywać komunikacje i transmitować dane w ten sposób uzyskane do terminalu zdalnego sterowania; (c) chronić dane przed nieupoważnionym dostępem, także osób zatrudnionych przez operatora sieci komórkowej; (d) udostępniać adres baz danych użytkownikowi (par. 1.1 i 1.6 załącznika nr 1).

117.  W szczególności urządzenia muszą zapewniać: (a) przechwytywanie wszystkich przychodzących i wychodzących połączeń podmiotów przechwytywania; (b) dostęp do informacji o miejscu pobytu osoby, której komunikacja jest przechwytywana; (c) utrzymywanie zdolności przechwytywania komunikacji, gdy połączenia wychodzące są transferowane pomiędzy sieciami innych operatorów sieci komórkowych; (d) utrzymywanie zdolności przechwytywania w sytuacjach obejmujących usługi dodatkowe, takie jak przekazywanie połączeń, transferowanie połączeń lub połączenia konferencyjne, z możliwością rejestrowania numeru lub numerów, do których połączenie jest przekierowywane; (e) zbieranie danych komunikacyjnych dotyczących wszystkich rodzajów połączeń, włączając fax, krótkie wiadomości (SMS) lub inne; (f) dostęp do informacji o usługach dostarczanych osobie, której komunikacja jest przechwytywana (par. 2.1.2 Załącznika nr 1).

118.  Występują dwa rodzaje przechwytywania: “przechwytywanie całkowite” oraz “monitorowanie statystyczne”. Przechwytywanie całkowite odbywa się w czasie realnym, jest to przechwytywanie danych komunikacji, zawartości komunikacji przychodzącej do podmiotu lub przez niego wykonywanej. Monitorowanie statystyczne odbywa się w czasie realnym, jest to jedynie monitorowanie danych komunikacji, bez przechwytywania ich zawartości. Dane komunikacji zawierają numery telefonów, z którymi odbywało się połączenie, początek i zakończenie połączenia, użycie dodatkowych usług, lokalizacji podmiotu podlegającego przechwytywaniu oraz status danego połączenia (par. 2.2 i 2.4 Aneksu nr 1).

119.  Zainstalowane urządzenie musi uruchamiać przechwytywanie transmisji komunikacyjnej w ciągu trzydziestu sekund od przyjęcia polecenia od terminala zdalnego sterowania (par. 2.5 Aneks nr 1).

120. Informacje o przechwytywanych tematach lub transmisji danych do terminala zdalnego sterowania nie mogą być zapisywane lub nagrywane (par. 5.4 Aneksu nr 1).

121.   Terminal zdalnego sterowania dostaje hasło od operatora sieci komórkowej z pełnym dostępem do SORM. Terminal wówczas zmienia hasło, aby chronić dostęp do SORM przed nieuprawnionymi osobami. Z terminala zdalnego sterowania SORM może dostawać polecenia, miedzy innymi, aby rozpocząć przechwytywanie komunikacji użytkownika, przerywać lub zakłócać przechwytywanie, zakłócać komunikację wychodzącą użytkownika oraz przekazywać określone informacje o użytkowniku (par. 3.1.2 Aneksu nr 3).

122.  Centrum kontroli otrzymuje następnie automatyczne powiadomienia o przechwytywanych tematach: krótkich wiadomościach (SMS), wysłanych lub otrzymanych przed podmiot podlegający przechwytywaniu, włączając ich zawartość; wybrane numery; połączenia; połączenia zakłócone; korzystanie z usług dodatkowych; zmiany w statusie połączenia podmiotu lub jego lokalizacji (par. 3.1.4 Aneksu nr 4).

(b) Rozporządzenie nr 130

123.  Rozporządzenie nr 130 o procedurach instalacji dla urządzeń technicznych umożliwiających prowadzenie czynności operacyjno-rozpoznawczych, wydane przez Ministra Komunikacji w dniu 25 lipca 2000, stanowi, że dostawcy usług komunikacyjnych mają zainstalować urządzenie, które spełnia wymagania techniczne wymienione w Rozporządzeniu nr 70. Procedura instalacyjna i terminarz ma być zatwierdzony przez FSB (par. 1.4).

124.  Dostawcy usług komunikacyjnych mają podejmować środki w celu ochrony informacji o metodach stosowanych podczas czynności operacyjno-rozpoznawczych (par. 2.4).

125.  Dostawcy usług komunikacyjnych mają zapewnić, że każde przechwytywanie transmisji komunikacyjnej lub dostęp do danych komunikacji jest zapewniony tylko na podstawie nakazu sądowego w zgodzie z procedurą ustanowioną przez OSAA (par. 2.5).

126.  Dostawcy usług komunikacyjnych nie muszą zostać poinformowani o przechwytywaniu dotyczącym ich użytkowników. Nie ma również konieczności prezentowania im orzeczeń sądowych legalizujących przechwytywanie (par. 2.6).

127.  Przechwytywania podejmowane są przez pracowników FSB i przy wykorzystaniu ich urządzeń technicznych oraz przez agencje Ministra Spraw Wewnętrznych (par. 2.7).

128.  Paragrafy 1.4 i 2.6 Rozporządzenia nr 130 zostały zakwestionowane przez Pana N. przed Sądem Najwyższym. Pan N. podnosił, że odniesienia do Rozporządzenia nr 70 zawarte w par. 1.4 były bezprawne, ponieważ Rozporządzenie nr 70 nie było opublikowane i pozostawało nieważne. Co do par. 2.6, był on niezgodny z Ustawą o Komunikacji, która stanowiła, że dostawcy usług komunikacyjnych byli zobowiązani do zapewnienia prywatności komunikacji. Dnia 25 września 2000 Sąd Najwyższy uznał, że odesłanie do rozporządzenia nr 70 w par. 1.4 było zgodne z prawem, ponieważ Rozporządzenie nr 70 miało charakter techniczny i w związku z tym nie podlegało publikacji w ogólnodostępnym oficjalnym biuletynie. Co do par. 2.6, Sąd Najwyższy uznał, że jego treść mogłaby zostać zinterpretowana jako wymaganie wobec dostawców usług komunikacyjnych do zapewnienia organom śledczym dostępu do informacji o użytkownikach bez upoważnienia sądowego. Takie wymaganie byłoby, jednakże, niezgodne z Ustawą o Komunikacji. Sąd Najwyższy w związku z tym uznał, że par. 2.6 jest niezgodny z prawem i nie powinien znajdować zastosowania.

129.  Dnia 25 października 2000 Minister Komunikacji zmienił Rozporządzenie nr 130 poprzez uchylenie par. 2.6.

130.  W odpowiedzi na zapytanie o informacje, wniesione przez organizację pozarządową “Kontrola Cywilna”, Minister Komunikacji oznajmił w liście z dnia 20 sierpnia 2006, że uchylenie par. 2.6 Rozporządzenia 130 nie oznaczało, że dostawcy usług komunikacyjnych musieli zostać poinformowani o środkach operacyjno-rozpoznawczych w związku z użytkownikami ani [również nie oznaczało tego, iż] kopia odpowiedniego postanowienia sądowego upoważniającego do odpowiednich działań musiała zostać im dostarczona.

131.  Rozporządzenie nr 130 zostało uchylone dnia 16 stycznia 2008 (zob. par. 134 poniżej).

(c)  Rozporządzenie nr 538

132.  Rozporządzenie nr 538 o współpracy pomiędzy dostawcami usług komunikacyjnych a organami ścigania, wydane przez Rząd w dniu 27 sierpnia 2005 r. stanowi, że dostawcy usług komunikacyjnych muszą w sposób staranny aktualizować bazy danych zawierające informacje o użytkownikach i usługach, z których korzystają. Ta informacja musi być przechowywana przez 3 lata. Organy ścigania muszą mieć zdalny dostęp w każdym momencie do baz danych (par. 12).

133.  Bazy danych muszą zawierać następujące informacje o użytkownikach: (a) imię, nazwisko rodowe, nazwisko, adres zamieszkania i numer dostępu dla osób fizycznych; (b) nazwę firmy, adres i liczbę osób mających dostęp do zdalnych urządzeń, ich imiona, nazwiska rodowe i nazwiska, adres zamieszkania, numer dostępu dla osób prawnych; (c) informacje o ich kontaktach i płatnościach (par. 14).

(d)  Rozporządzenie nr 6

134.  Część I Rozporządzenia nr 6 o wymaganiach dla sieci telekomunikacyjnych dotyczących prowadzenia czynności operacyjno-rozpoznawczych, wydana przez Ministra Komunikacji w dniu 16 stycznia 2008 zastąpiła Rozporządzenie nr 130.

135. Zachowano wymaganie, że dostawcy usług komunikacyjnych muszą zapewnić  przekazanie do zdalnego terminala danego organu ścigania informacji o (a) numerach i kodach identyfikacyjnych użytkownika; oraz (b) treści ich komunikacji. Informacja ma zostać transmitowana w chwili wydania polecenia z terminala zdalnego sterowania. Dostawcy usług komunikacyjnych muszą również zapewnić identyfikację lokalizacji użytkownika (par. 2,3 oraz 5).

136.  Terminal zdalnego sterowania musi mieć dostęp do baz danych zawierających informacje o użytkownikach, włącznie z ich numerami i kodami identyfikacyjnymi (par. 7 i 8).

137.  Dostawcy usług komunikacyjnych muszą zapewnić, że osoba, której komunikacja jest przechwytywana nie jest świadoma przechwytywania jej komunikacji. Informacja o trwających lub przeszłych przechwytywaniach musi być chroniona przed nieupoważnionym dostępem ze strony pracowników dostawców usług komunikacyjnych (par. 9).

(e)  Rozporządzenie nr 73

138.  Część II Rozporządzenia nr 73 o wymaganiach dla sieci telekomunikacyjnych dotyczących prowadzenia czynności operacyjno-rozpoznawczych, wydanego przez Ministra Komunikacji w dniu 27 maja 2010, szczegółowo omawia wymagania zawarte w Rozporządzeniu nr 6. W szczególności stanowi, że urządzenie zainstalowane przez dostawców usług komunikacyjnych musi zapewnić dostęp organom ścigania wykonującym czynności operacyjno-rozpoznawcze do wszystkich danych transmitowanych przez sieci telekomunikacyjne oraz musi być w stanie segregować dane i transmitować posegregowane dane do ich terminala kontroli (par. 2).

III.  ODPOWIEDNIE INSTRUMENTY MIĘDZYNARODOWE I EUROPEJSKIE

A.  Organizacja Narodów Zjednoczonych

139.  Rezolucja nr 68/167 o Prawie do Prywatności w Erze Cyfrowej, przyjęta przez Zgromadzenie Ogólne w dniu 18 grudnia 2013, brzmi następująco:

“Zgromadzenie Ogólne,

...

4. *Wzywa* wszystkie Państwa:

...

(*c*) Do zbadania swoich procedur, praktyk i legislacji dotyczących nadzoru komunikacji, jej przechwytywania i zbierania danych prywatnych, włączając nadzór masowy, przechwytywanie i zbieranie, mając na uwadze poszanowanie prawa do prywatności poprzez pełną i efektywną implementację wszystkich obowiązków wynikających z międzynarodowego prawa w zakresie praw człowieka;

(*d*) Do ustanowienia lub utrzymania niezależnego, efektywnego krajowego mechanizmu nadzoru zapewniającego transparentność, oraz odpowiedzialność nadzoru państwowego nad komunikacjami, ich przechwytywaniem i zbieraniem prywatnych danych …”

B.  Rada Europy

140.  Konwencja o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych z dnia 28 stycznia 1981 (CETS nr 108, dalej zwana “Konwencja nr 108”) wyznacza standardy dla ochrony danych w sferze automatycznego przetwarzania danych osobowych w sektorze publicznym i prywatnym. Brzmi:

**“Artykuł 8 – Gwarancje dodatkowe dla podmiotu danych**

Każda osoba jest upoważniona do:

1. ustalenia informacji o istnieniu zautomatyzowanego zbioru danych osobowych, o jego zasadniczych celach, oraz o tożsamości i miejscu zamieszkania lub siedzibie kontrolera zbioru;
2. 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;
3. 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;
4. 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:
	1. ochrony Państwa, bezpieczeństwa publicznego, interesów wa1utowych państwa lub zwalczania przestępczości;
	2. ochrony podmiotu danych oraz praw i wolności innych osób....

**Artykuł 10 – Sankcje 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.”

141.  Konwencja nr 108 została ratyfikowana przez Federację Rosyjską w dniu 15 maja 2013 i weszła w życie w stosunku do Rosji w dniu 1 września 2013. Instrument ratyfikacji złożony przez Federację Rosyjską w dniu 15 maja 2013 zawiera następującą deklarację:

“Federacja Rosyjska deklaruje, że zgodnie z podpunktem “a” paragrafu 2 Artykułu 3 Konwencji, nie będzie stosować Konwencji do danych osobistych:

...

(b) stanowiących tajemnicę państwową, zgodnie z ustawodawstwem Federacji Rosyjskiej o tajemnicy państwowej.

Federacja Rosyjska deklaruje, że zgodnie z podpunktem “c” paragrafu 2 Artykułu 3 Konwencji, będzie ona stosowana w odniesieniu do danych osobowych, które nie są przetwarzane automatycznie, jeżeli stosowanie Konwencji będzie odpowiadać naturze czynności podejmowanych w stosunku do danych osobowych, bez korzystania ze środków zautomatyzowanych.

Federacja Rosyjska deklaruje, że zgodnie z podpunktem “a” paragrafu 2 Artykułu 9 Konwencji, zachowuje prawo do ograniczania prawa podmiotu danych do dostępu do jego danych osobowych w celu ochrony bezpieczeństwa Państwa i porządku publicznego.”

142.  Protokół dodatkowy do Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych dotyczący organów nadzoru i transgranicznych przepływów danych z dnia 8 listopada 2001 (CETS No. 181), podpisany lecz nieratyfikowany przez Rosję, stanowi, co następuje:

**“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 postępowanie prawne lub informowania właściwych organów sądowych o naruszeniach przepisów prawa krajowego, realizując zasady określone w artykule l ustęp l 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 swoich kompetencji.

3.  Organy nadzoru wykonują swe funkcje korzystając z całkowitej niezależności.

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

143.  Rekomendacja Komitetu Ministrów Rady Europy o ochronie danych osobowych wykorzystywanych w sektorze Policji, przyjęta dnia 17 września 1987 (Nr R (87) 15), stanowi, co następuje:

“1.1.  Każde Państwo Członkowskie powinno dysponować niezależnym i zewnętrznym w stosunku do Policji organem nadzorczym, upoważnionym do czuwania nad przestrzeganiem Zasad zawartych w niniejszej Rekomendacji...

2.1.  Gromadzenie danych osobowych dla potrzeb Policji winno ograniczać się do tych danych, które są konieczne dla zapobieżenia realnemu niebezpieczeństwu, bądź zwalczeniu określonego przestępstwa. Wszelkie wyjątki od powyższego postanowienia winny być przedmiotem szczególnego ustawodawstwa krajowego.

2.2.  Tam, gdzie dane dotyczące osoby były gromadzone i przechowywane bez jej wiedzy, powinna ona - jeśli dane takie nie zostały usunięte - zostać poinformowana w miarę możliwości o tym, iż informacje o niej są przetwarzane w zbiorze. Należy tego dokonać, gdy tylko przestanie istnieć ryzyko, iż przedmiot działań Policji poniesie jakąkolwiek szkodę wynikającą z ujawnienia osobie, której dane dotyczą faktu istnienia tych informacji...

3.1.  Na ile to tylko możliwe, rejestrowanie danych osobowych dla potrzeb Policji powinno dotyczyć jedynie konkretnych danych, niezbędnych do wypełniania zgodnych z prawem zadań realizowanych przez organy policyjne, w granicach przewidzianych przez prawo krajowe oraz postanowienia wynikające z prawa międzynarodowego...

5.2.i.  Przekazywanie danych organom publicznym winno być dozwolone jedynie w przypadku, gdy:

a.  istnieje wyraźny obowiązek prawny bądź zezwolenie organu nadzorczego; lub

b.  dane takie są odbiorcy niezbędne dla wypełnienia jego własnego zgodnego z prawem zadania oraz pod warunkiem, że cel gromadzenia lub przetwarzania dokonywanego przez takiego odbiorcę nie jest niezgodny z celem pierwotnie przewidzianym, oraz że nie stoi on w sprzeczności z prawnymi obowiązkami organu przekazującego.

5.2.ii.  Ponadto, przekazywanie danych innym organom publicznym jest w wyjątkowych sytuacjach dozwolone, jeśli w konkretnym przypadku:

a.  nie ma wątpliwości, iż przekazywanie danych leży w interesie osoby, której dane dotyczą lub jeśli ona sama wyrazi na to zgodę, bądź też okoliczności pozwalają na jednoznaczne domniemanie takiej zgody; lub jeśli

b.  takie przekazywanie danych jest konieczne dla uniknięcia poważnego i bezpośredniego niebezpieczeństwa.

5.3.i.  Przekazywanie danych osobom prywatnym winno być dozwolone jedynie w przypadku, gdy w grę wchodzi wyraźne zobowiązanie prawne lub upoważnienie, bądź też upoważnienie organu nadzorczego ...

6.4.  Korzystanie z prawa dostępu, sprostowania lub usunięcia może podlegać ograniczeniom tylko w takim stopniu, w jakim tego rodzaju ograniczenie jest konieczne dla wypełnienia zgodnego z prawem zadania Policji, bądź też konieczne jest dla ochrony osoby, której dane dotyczą, albo dla ochrony praw i wolności innych osób...

6.5.  Odmowa bądź ograniczenie korzystania z powyższych praw powinny być uzasadnione na piśmie. Nie można odmówić osobie, której dane dotyczą wydania uzasadnienia, chyba, że jest to niezbędne dla wypełnienia zgodnego z prawem zadania Policji, bądź konieczne dla ochrony praw i wolności innych osób.

6.6.  W przypadkach, w których osobie, której dane dotyczą odmówiono dostępu do dotyczących jej danych osobowych, osoba ta winna dysponować możliwością odwołania się do organu nadzorczego lub do innego niezależnego organu, który stwierdzi, czy odmowa była odpowiednio uzasadniona.

7.1.  Należy przedsięwziąć środki, by dane osobowe przechowywane dla potrzeb Policji, podlegały usunięciu, jeśli nie są już konieczne do celów, dla których zostały zarejestrowane.

W tym celu należy brać zwłaszcza pod uwagę następujące kryteria: konieczność zachowania danych w świetle wniosków wynikających z postępowania śledczego; ostateczne postanowienie sądu, a zwłaszcza uniewinnienie; rehabilitację; przedawnienie; amnestię; wiek osoby, której dane dotyczą; szczególne kategorie danych.

7.2.  Należy ustanowić - w porozumieniu z organem nadzorczym, bądź zgodnie z prawem krajowym - reguły służące określaniu czasu i okresu przetwarzania różnych kategorii danych osobowych, jak również regularne kontrole ich jakości.

8.  Organ odpowiedzialny winien podejmować wszelkie środki konieczne do zagwarantowania danym odpowiedniego bezpieczeństwa fizycznego i logicznego, jak również do uniemożliwienia dostępu do tych danych i ich przekazywania osobom nieupoważnionym oraz dokonywania w nich zmian. W tym celu, należy brać pod uwagę charakter zbiorów i ich różną zawartość.”

144.  Rekomendacja Komitetu Ministrów dotycząca ochrony danych osobowych w telekomunikacji, ze szczególnym uwzględnieniem usług telefonicznych przyjęta dnia 7 lutego 1995 (Nr R (95) 4), w odpowiednim zakresie brzmi następująco:

“2.4.  Ingerencja władz publicznych w zawartość komunikacji, włączając wykorzystanie podsłuchu urządzeń lub innych środków nadzoru lub przechwytywania komunikacji, może zostać powzięta wyłącznie, gdy prawo tak stanowi i konstytuuje konieczny środek w społeczeństwie demokratycznym, w interesie:

a.  ochrony bezpieczeństwa państwowego, publicznego, państwowych interesów finansowych lub zapobiegania przestępstwom;

b.  ochrony podmiotu danych lub praw i wolności innych osób;

2.5. W sytuacji ingerencji wykonywanej przez władze publiczne w treść komunikacji, prawo krajowe powinno regulować:

a.  korzystanie z prawa dostępu i korygowania przez podmiot danych;

b. okoliczności, w których odpowiedzialne władze są uprawnione do odmowy dostarczenia informacji osobie zainteresowanej lub opóźnienie ich dostarczenia;

c.  przechowywanie i niszczenie takich danych.

Jeżeli operator sieci lub dostawca usług jest pouczony przez władze państwowe o ingerencji, zebrane dane powinny być przekazywane wyłącznie do organu wyznaczonego w upoważnieniu do ingerencji...”

C.  Unia Europejska

145.  Rezolucja Rady z dnia 17 stycznia 1995 o przechwytywaniu telekomunikacji (96/C 329/01) stanowi, co następuje:

“Ta sekcja stanowi o wymogach wobec organów ścigania dotyczących przechwytywania telekomunikacji. Te wymogi podlegają prawu krajowemu i powinny być interpretowane zgodnie z obowiązującą polityką krajową...

1.3. Telekomunikacja przychodząca i wychodząca od obserwowanego podmiotu, która nie podlega zakresowi upoważnienia przechwytywania, powinna zostać wyłączona z telekomunikacji przekazywanej organom ścigania...

2.  Przechwytywanie telekomunikacji powinno odbywać się w czasie rzeczywistym, i być monitorowane całodobowo. Dane z połączenia również powinny być przekazywane w czasie rzeczywistym. Jeżeli dane z połączenia nie mogą być przekazywane w czasie rzeczywistym, powinny być udostępnione organom ścigania tak szybko, jak to możliwe po zakończeniu połączenia.

3.  Operatorzy sieci/dostawcy usług powinni dostarczać jeden interfejs lub więcej, z których przechwycone połączenia mogą być transmitowane do urządzeń monitorujących organów ścigania. Interfejsy te muszą podlegać powszechnej zgodzie pomiędzy władzami wykonującymi przechwytywanie i operatorami sieci/dostawcami usług. Pozostałe kwestie związane z interfejsami będą rozwiązywane zgodnie z przyjętymi praktykami w poszczególnych krajach...

5.  Przechwytywanie powinno być tak skonstruowane i implementowane, aby wykluczyć nieuprawnione lub niewłaściwe wykorzystanie a także by zapewnić ochronę informacji związanych z przechwytywaniem...

5.2 Operatorzy sieci/dostawcy usług powinni zapewnić, że przechwytywana komunikacja i transmitowana wyłącznie do organów monitorujących określonych w upoważnieniu przechwytywania...”

146.  Powyższe wymogi zostały potwierdzone i objaśnione w Rezolucji Rady nr 9194/01 z dnia 20 czerwca 2001 o potrzebach operacyjnych organów ścigania w związku z sieciami i usługami telekomunikacji publicznej.

147.  Wyrok wydany przez Trybunał Sprawiedliwości Unii Europejskiej (TSUE) w dniu 8 kwietnia 2014 w sprawach *Digital Rights Ireland* oraz *Seitinger i Inni,* rozpatrywanych łącznie, uznał za nieważną Dyrektywę o Przechowywaniu danych2006/24/EC ustanawiającą obowiązek dostawców publicznie dostępnych elektronicznych usług komunikacyjnych lub sieci publicznej komunikacji do przechowywania danych dotyczących ruchu i lokalizacji przez okres sześciu miesięcy do dwóch lat, w celu zapewnienia dostępności danych dla celów śledztwa, aresztowania i skazania za poważną zbrodnię, jak określona została w prawie krajowym każdego Państwa-Strony. TSUE podniósł, że pomimo zakazu wyrażonego w dyrektywie dotyczącego przechowywania treści komunikacji, dane dotyczące ruchu i lokalizacji w nim zawarte, zezwalają na wyciągnięcie precyzyjnych wniosków dotyczących życia prywatnego osób, których dane są przechowywane. W związku z tym, obowiązek przechowywania tych danych ustanowił ingerencję w prawo do poszanowania życia prywatnego i komunikacji zagwarantowane przez Artykuł 7 Karty Praw Podstawowych Unii Europejskiej i prawo do ochrony danych osobowych zagwarantowanych przez Artykuł 8 Karty. Co więcej, dostęp kompetentnego organu krajowego do danych, ustanowił dalszą ingerencję w te fundamentalne prawa. TSUE dalej utrzymał, że ingerencja była szczególnie poważna. Fakt, że dane były przechowywane, a następnie wykorzystywane bez informowania użytkownika, może wykreować w świadomości osoby, której dane dotyczą, uczucie, że jej życie prywatne podlega ciągłemu nadzorowi. Ingerencja spełniła cel interesu ogółu, mianowicie wkład w walkę przeciwko poważnym zbrodniom i terroryzmowi a poprzez to w szczególności spełniła cel bezpieczeństwa publicznego. Jednakże, nie spełniła wymogu proporcjonalności. Po pierwsze, dyrektywa objęła, w sensie ogólnym, wszystkie osoby i wszystkie rodzaje komunikacji oraz dane bez ich rozróżnienia, ograniczenia lub wyjątków poczynionych ze względu na realizację celu w postaci walki przeciwko poważnym zbrodniom. Poprzez to zezwala na ingerencję w fundamentalne prawa praktycznie całej europejskiej populacji. Dotyczyła również osób, wobec których nie było dowodów sugerujących, że prowadzą lub mają związek, pośredni lub odległy, z poważnym przestępstwem. Po drugie, dyrektywa nie formułuje materialnego lub proceduralnego warunku dotyczącego dostępu kompetentnych władz krajowych do danych i ich wykorzystania. Poprzez proste odniesienie, w sposób ogólny, do poważnego przestępstwa, jak zdefiniowano je w prawie krajowym Państwa-Strony, dyrektywa nie zawierała żadnego kryterium merytorycznego, które określałoby, które przestępstwa mogą być uznane za wystarczająco poważne do usprawiedliwienia tak szerokiej ingerencji w prawa fundamentalne, określone w Artykułach 7 i 8 Karty. Poza tym, dostęp kompetentnych władz krajowych do przechowywanych danych nie zależy od uprzedniej kontroli podjętej przez sąd lub niezależny organ administracyjny, których decyzje powinny ograniczać dostęp do danych i ich wykorzystania, co jest niezbędne do zrealizowania ww. celu. Po trzecie, dyrektywa wymagała przechowywania wszystkich danych na okres co najmniej sześciu miesięcy, bez rozróżnienia na kategorie danych na podstawie ich możliwej użyteczności dla powziętych celów dotyczących danych osób. TSUE podniósł, że dyrektywa upoważniała do szerokiej i szczególnie poważnej ingerencji w prawa fundamentalne, określone w Artykułach 7 i 8 Karty, bez precyzyjnego ograniczenia tej ingerencji przez przepisy, tak by zapewnić jej stosowanie w razie wyraźnej konieczności. TSUE również stwierdził, że dyrektywa nie zawierała żadnych wyraźnych gwarancji, poprzez wskazanie środków technicznych i organizacyjnych, które zapewniłyby efektywną ochronę przechowywanych danych przed ryzykiem ich nadużycia i przeciwko bezprawnemu dostępowi i wykorzystaniu tych danych.

PRAWO

I.  RZEKOME NARUSZENIE ARTYKUŁU 8 KONWENCJI

148.  Skarżący zaskarżył system niejawnego przechwytywania komunikacji komórkowej w Rosji, która nie spełniała wymogów Artykułu 8 Konwencji, który brzmi następująco:

“1.  Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji.

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.  Dopuszczalność

149.  Rząd podniósł, że skarżący nie mógł stwierdzić, że padł ofiarą rzekomego naruszenia jego prawa do poszanowania życia prywatnego lub korespondencji (zob. par. 152 i 157 poniżej). Co więcej, skarżący nie wyczerpał krajowych środków odwoławczych (zob. par. 219 i 226 poniżej).

150.  Trybunał stwierdza, że uwagi Rządu są blisko powiązane z treścią skargi skarżącego i muszą być włączone do meritum.

151.  Trybunał stwierdza również, że skarga nie jest oczywiście bezzasadna w znaczeniu Artykułu 35 § 3 lit. a Konwencji. Nie jest bezzasadna na żadnym innym gruncie. Z tego powodu uznana jest za dopuszczalną.

B.  Meritum

1.  Status ofiary skarżącego i istnienie “ingerencji”

(a)  Wnioski stron

(i)  Rząd

152.  Rząd stwierdził, ze skarżący nie mógł uznać się za ofiarę rzekomego naruszenia Artykułu 8 Konwencji oraz, że ingerencja w jego prawa nie miała miejsca. Skarżący nie zarzucił, że jego komunikacja była przechwytywana. Istota jego sprawy przed sądami krajowymi oraz Trybunałem dotyczyła faktu, że dostawcy usług komunikacyjnych zainstalowali specjalne urządzenie umożliwiające władzom podejmowanie czynności operacyjno-rozpoznawczych. W opinii Rządu, sprawa *Orange Slovensko, A. S. przeciwko Słowacji* ((dec.), nr 43983/02, 24 października 2006) potwierdziła, że instalowanie urządzeń przechwytywania lub nawet ich finansowanie przez prywatne firmy samo w sobie nie stoi w sprzeczności z Konwencją.

153. Rząd dalej wniósł, że Artykuł 34 nie mógł zostać wykorzystany do złożenia skargi w naturze *actio popularis*; ani dawał podstaw do sformułowania skargi *in abstracto,* że prawo stoi w sprzeczności z Konwencją (odniesiono się do *Aalmoes i 112 Innych przeciwko Holandii* (dec.), nr 16269/02, 25 listopada 2004). Podniesiono, że podejście do statusu ofiary przyjęte w sprawach *Klass i Inni przeciwko Niemcom* (6 września 1978, § 34, Serie A nr 28) i *Malone przeciwko Zjednoczonemu Królestwu* (2 sierpnia 1984, § 64, Serie A nr 82)– zgodnie z którym jednostka może, pod pewnymi warunkami, uznać się za ofiarę przy samym wystąpieniu tajnych środków lub ustawodawstwa, które zezwala na wykorzystanie tajnych środków, bez stwierdzania, że środki te były w rzeczywistości wobec niego lub niej zastosowane – nie może być interpretowane tak szeroko, by obejmowało każdą osobę w odpowiednim Państwie, która obawiała się, że służby bezpieczeństwa mogą zbierać o niej informacje. Skarżący musiał wykazać, że wystąpiło “uzasadnione prawdopodobieństwo”, że służby bezpieczeństwa zbierały i przechowywały informacje dotyczącego jego prywatnego życia (odniesiono się do *Esbester przeciwko Zjednoczonemu Królestwu*, nr 18601/91, decyzja Komisji z dnia 2 kwietnia 1993; *Redgrave przeciwko Zjednoczonemu Królestwu*, nr 20271/92, decyzja Komisji z dnia 1 września 1993; *Matthews przeciwko Zjednoczonemu Królestwu*, nr 28576/95, decyzja Komisji z dnia 16 października 1996; *Halford przeciwko Zjednoczonemu Królestwu*, 25 czerwca 1997, § 17, Raporty Wyroków i Decyzji 1997‑III; *Weber i Saravia przeciwko Niemcom* (dec.), nr 54934/00, §§ 4-6 i 78, ETPCZ 2006-XI; oraz *Kennedy przeciwko Zjednoczonemu Królestwu*, nr 26839/05, §§ 122 i 123, 18 maja 2010).

154.  Rząd utrzymał, że wyjątki od zasady “uzasadnionego prawdopodobieństwa’’ były dopuszczalne jedynie w wyjątkowych okolicznościach. Jednostka mogła stwierdzić ingerencję w rezultacie samego istnienia legislacji zezwalającej na środki tajnego nadzoru jedynie w wyjątkowych okolicznościach, mając na uwadze możliwość wniesienia środków odwoławczych na poziomie krajowym i ryzyko zastosowania wobec niej środków tajnego nadzoru (zacytowano *Kennedy*, cyt. pow. § 124). Jak stwierdził Rząd, owe specjalne powody nie mogą zostać ustalone w niniejszej sprawie.

155.  Po pierwsze, nie wystąpiło “uzasadnione prawdopodobieństwo” lub w rzeczy samej jakiekolwiek ryzyko, że skarżący został poddany środkom nadzoru, ponieważ nie był podejrzewany o popełnienie jakiegokolwiek przestępstwa. Fakt, że był redaktorem naczelnym wydawnictwa nie stanowił powodu do przechwytywania komunikacji, na podstawie prawa rosyjskiego. Rząd zapewnił, że rozmowy telefoniczne skarżącego nigdy nie były przechwytywane. Skarżący nie przedstawił żadnego dowodu świadczącego przeciwnie. Dokumenty przez niego złożone w postępowaniach krajowych dotyczyły osób trzecich i nie zawierały żadnego dowodu, że jego telefon był na podsłuchu.

156.  Po drugie, środki odwoławcze, dzięki którym mógł zaskarżyć zarówno rzekome niewystarczające gwarancje dotyczące nadużyć w prawie rosyjskim oraz szczególne środki nadzoru stosowane wobec jednostek, były dostępne na poziomie krajowym. Istniała możliwość wniesienia zapytania do Trybunału Konstytucyjnego o konstytucyjność OSAA. Można było również złożyć skargę do Sądu Najwyższego, co skutecznie zrobił Pan N., dzięki czemu uznano bezprawność przepisów Rozporządzenia nr 130 Ministra Komunikacji (zob. par. 128 pow.). Co się tyczy Rozporządzenia nr 70, przeciwnie do zarzutów skarżącego, zostało ono należycie opublikowane (zob. par. 181 poniżej) i związku z tym, nie mogło zostać zmienione przed sądami. Osoba, której komunikacje były bezprawnie przechwytywane bez uprzedniego sądowego upoważnienia, mogła również uzyskać rekompensatę w postępowaniu przed sądem cywilnym. Rząd odwołał się do orzeczenia Sądu Najwyższego z dnia 15 lipca 2009, w którym uznano, że zainstalowanie kamery video w biurze wnioskodawcy i zainstalowanie podsłuchu w jego biurowym telefonie było bezprawne, ponieważ te środki nadzoru zostały powzięte bez uprzedniego sądowego upoważnienia (zob. również par. 219 i 224 poniżej). Ostatecznie, prawo rosyjskie zapewniło kontrolę przechwytywania przez niezależny organ, biuro prokuratorskie.

157.  Rząd wywnioskował, mając na uwadze powyższe, że niniejsza sprawa różniła się od sprawy *Association for European Integration and Human Rights and Ekimdzhiev przeciwko Bułgarii* (nr 62540/00, 28 czerwca 2007), w której Trybunał odmówił zastosowania testu “uzasadnionego prawdopodobieństwa”, ze względu na brak gwarancji dotyczących bezprawnego przechwytywania komunikacji w Bułgarii. Mając to na uwadze, prawo rosyjskie wprowadziło adekwatne i efektywne gwarancje przeciwko nadużyciom w sferze przechwytywania komunikacji, obejmujące dostępne środki odwoławcze. W opinii Rządu, skarżący nie mógł stwierdzić, iż ingerencja stanowiła rezultat istnienia samego ustawodawstwa zezwalającego na tajny nadzór. W przypadku braku “uzasadnionego prawdopodobieństwa”, że komunikacja telefoniczna skarżącego była przechwytywana, nie można uznać go za ofiarę rzekomego naruszenia Artykułu 8 Konwencji.

(ii)  Skarżący

158.  Skarżący wniósł, że mógł uznać się za ofiarę naruszenia Artykułu 8 ze względu na samo istnienie ustawodawstwa zezwalającego na system tajnego przechwytywania komunikacji, bez wykazywania, że takie tajne środki zostały rzeczywiście zastosowane. Istnienie takiego ustawodawstwa stwarzało zagrożenie nadzoru dla wszystkich użytkowników usług telekomunikacyjnych i w związku z tym stwarzało samo w sobie ingerencję w korzystanie w jego prawa ustanowione w Artykule 8 Konwencji. Na poparcie swojego stanowiska skarżący przywołał sprawy *Klass i Inni* (cyt. pow., §§ 34 i 37), *Association for European Integration and Human Rights and Ekimdzhiev* (cyt.pow., § 58) i *Kennedy* (cyt. pow., § 123).

159.  Skarżący utrzymywał, że test “uzasadnionego prawdopodobieństwa” został zastosowany przez Trybunał jedynie w tych sprawach, w których skarżący zarzucił przechwytywanie, podczas gdy w sprawach dotyczących ogólnych skarg na ustawodawstwo i praktykę zezwalającą na zastosowanie środków tajnego nadzoru, zastosowano test “samego istnienia” opisany w sprawie *Klass i Inni (*zob. *Association for European Integration and Human Rights and Ekimdzhiev*, cyt. pow., § 59, oraz *Kennedy*, cyt. pow., §§ 122 i 123, z dalszymi odniesieniami). W sprawie *Liberty i Inni przeciwko Zjednoczonemu Królestwu* (nr 58243/00, §§ 56 i 57, 1 lipca 2008), Trybunał uznał, że nadana władzom możliwość przechwytywania transmisji komunikacyjnej stanowiła ingerencję w prawa skarżących określone w Artykule 8, jako że są one osobami, wobec których ta możliwość mogła zostać zastosowana. W sprawie *Kennedy* (cyt. pow., § 124) test został dalej rozwiniętt, by zawierał ocenę dostępności jakichkolwiek środków odwoławczych na poziomie krajowym oraz ryzyka zastosowania tajnych środków nadzoru wobec skarżącego. Ostatecznie w sprawie *Mersch i Inni przeciwko Luksemburgowi* (nr 10439/83 et al., decyzja Komisji z 10 maja 1985) Komisja uznała, że w sprawach, w których władze nie miały obowiązku informowania osób o zastosowanych wobec nich środkach nadzoru, skarżący mogli uznać się za “ofiary” naruszenia Konwencji ze względu na samo istnienie ustawodawstwa zezwalającego na tajny nadzór, nawet jeśli nie mogli na poparcie tych twierdzeń zarzucić, że faktycznie zostali poddani środkom inwigilacji.

160.  Skarżący zaskarżył, że mógł uznać się za ofiarę naruszenia Artykułu 8, ze względu na samo istnienie ustawodawstwa o tajnym nadzorze oraz z powodu swojej sytuacji osobistej. OSAA rozpatrywane łącznie z Ustawą FSB, Ustawą o Komunikacji oraz Rozporządzeniami wydanymi przez Ministra Komunikacji, takimi jak Rozporządzenie nr 70 zezwala służbom bezpieczeństwa na przechwytywanie z użyciem środków technicznych, każdej komunikacji bez konieczności uzyskania wcześniejszego upoważnienia sądowego. Zakwestionowane ustawodawstwo zezwalało więc na blankietowe przechwytywanie transmisji komunikacyjnej.

161.  Na mocy prawa rosyjskiego nie były dostępne żadne środki pozwalające na zaskarżenie tych przepisów. Dlatego, jeżeli chodzi o możliwość zakwestionowania Rozporządzenia nr 70, skarżący odniósł się do orzeczenia Sądu Najwyższego z dnia 25 września 2000 w przedmiocie skargi Pana N. (zob. par. 128 powyżej), w której uznano, że Rozporządzenie było w swej naturze bardziej techniczne niż prawne i z tego względu nie podlegało oficjalnej publikacji. Złożył również kopię decyzji z dnia 24 maja 2010 Naczelnego Sądu Gospodarczego uznającego, że Rozporządzenia Ministra Komunikacji wymagające od dostawców usług komunikacyjnych zainstalowania urządzeń umożliwiających władzom wykonywanie czynności operacyjno-rozpoznawczych, nie podlegały kontroli sądowej w sądach gospodarczych. Postępowania krajowe wszczęte przez skarżącego wykazały, że Rozporządzenie nr 70 nie mogło zostać efektywnie zakwestionowane przed sądami rosyjskimi. Co więcej, w sytuacjach dotyczących OSAA, Trybunał Konstytucyjny zbadał jej konstytucjonalność przy wielu okazjach i uznał, że była zgodna z Konstytucją. Wreszcie, skarżący podniósł, że w sytuacjach dotyczących kwestionowania indywidualnych środków nadzoru że osoby, które im podlegały, nie były informowane o przechwytywaniu komunikacji, chyba że materiał z przechwytywania został wykorzystany jako dowód w postępowaniu karnym. Przy braku takiego powiadomienia, krajowe środki odwoławcze pozostawały nieefektywne (zob. również par. 217 poniżej).

162. Co się tyczy sytuacji osobistej, skarżący podniósł, że był dziennikarzem oraz przewodniczącym oddziału St. Petersburskiej Fundacji Obrony Glasnost,  która monitorowała wolność mediów krajowych i zapewniała wsparcie prawne dziennikarzom, których prawa zawodowe zostały naruszone (zob. par. 8 pow.). Jego komunikacje w związku z tym podlegały podwyższonemu ryzyku przechwytywania. Skarżący odniósł się do fundamentalnej istotności ochrony źródeł dziennikarzy, podkreślonej w wyroku Wielkiej Izby w sprawie *Sanoma Uitgevers B.V. przeciwko Holandii* ([GC], nr 38224/03, § 50, 14 września 2010).

(b) Ocena Trybunału

163. Trybunał zauważa, że w niniejszej sprawie skarżący twierdzi, że nastąpiła ingerencja w jego prawa spowodowana nie tyle zastosowaniem wobec niego jakichkolwiek szczególnych środków przechwytywania komunikacji, co raczej samym tylko obowiązywaniem przepisów zezwalających na tajne przechwytywanie transmisji komunikacji komórkowej, oraz ryzykiem przechwycenia komunikacji skarżącego.

(i)  Podsumowanie orzecznictwa Trybunału

164.  Trybunał stale utrzymywał w swoim orzecznictwie, że Konwencja nie przewiduje instytucji *actio popularis*, a także, że jego zadaniem nie jest dokonywanie kontroli odpowiedniego prawa i praktyki *in abstracto*, ale określenie, czy sposób, w jaki zostało ono zastosowane lub jaki wywarło wpływ, mógł dać podstawę do stwierdzenia naruszenia Konwencji (zob. między innymi, *N.C. przeciwko Włochom* [GC], nr 24952/94, § 56, ETPCz 2002‑X; *Krone Verlag GmbH & Co. KG przeciwko Austrii (nr 4)*, nr 72331/01, § 26, 9 listopada 2006; oraz *Centre for Legal Resources on behalf of Valentin Câmpeanu przeciwko Rumunii* [GC], nr 47848/08, § 101, ETPCz 2014). Zgodnie z tym, w celu umożliwienia złożenia skargi na mocy Artykułu 35, osoba musi wykazać, że środki, które zaskarżyła, dotyczyły go w sposób bezpośredni. Jest to nieodzowne do zastosowania mechanizmu ochrony Konwencji, mimo że kryterium nie należy stosować podczas postępowania sztywno czy w sposób wykluczający jakąkolwiek elastyczność (zob. *Centre for Legal Resources on behalf of Valentin Câmpeanu,* cyt. pow., § 96).

165.   Z tego też powodu Trybunał dopuścił możliwość ogólnego badania sposobu funkcjonowania w danym systemie prawnym tajnego nadzoru, z uwagi na szczególne cechy środków tajnego nadzoru oraz istotność zapewnienia efektywnej kontroli oraz nadzoru nad nimi. W sprawie *Klass and Others przeciwko Niemcom* Trybunał utrzymał, że osoby mogą, pod pewnymi warunkami, uznać się za ofiary naruszenia wynikającego z samego istnienia tajnych środków lub ustawodawstwa zezwalającego na tajne środki, bez konieczności stwierdzania, że środki te zostały faktycznie zastosowane. Odpowiednie zasady powinny być określone w każdej sprawie dotyczącej rzekomego naruszenia prawa lub praw Konwencji, zastosowania tajnych środków oraz powiązania pomiędzy skarżącym a tymi środkami (zob. *Klass i Inni,* cyt. pow., § 34). Trybunał wyjaśnił swoje stanowisko w sposób następujący:

“36. Trybunał podkreśla, że gdy Państwo zarządza użycie niejawnych środków kontroli i gdy ma to zostać tajemnicą wobec osób kontrolowanych, to gdyby nie przysługiwał im środek prawny przeciwko takiemu zarządzeniu, treść art. 8 byłaby w dużej mierze fikcją. Możliwe jest, że w takiej sytuacji jednostka może być traktowana w sposób sprzeczny z art. 8 lub nawet być pozbawiona prawa gwarantowanego w tym przepisie bez świadomości zaistnienia tego faktu - a zatem bez zdolności użycia środka prawnego czy to na szczeblu krajowym, czy przed organami Konwencji...

Trybunał stwierdza, że nie jest możliwy do zaakceptowania stan, w którym zapewnienie korzystania z prawa gwarantowanego w tej Konwencji mogłoby być uchylone przez zwykły fakt utrzymywania osoby zainteresowanej w niewiedzy co do jej naruszenia. Prawo odwołania się do Komisji Europejskiej osób potencjalnie dotkniętych niejawnym stosowaniem środków kontroli wynika z treści art. 25, ponieważ inaczej pojawia się ryzyko pozbawienia znaczenia treści art. 8.

37.  Okoliczności przedmiotowej sprawy przekonują Trybunał, że kwestionowana Ustawa wprowadziła system kontroli, w ramach którego korespondencja, poczta i telekomunikowanie się wszystkich osób na terenie RFN mogłoby być potencjalnie monitorowane bez ich wiedzy, chyba że uzyskałyby one na ten temat wiedzę wskutek jakiejś niedyskrecji bądź powiadomienia w sytuacjach określonych w wyroku BVG zapadłym w niniejszej sprawie. Zaskarżona Ustawa, w tej właśnie mierze, bezpośrednio dotyczy wszystkich potencjalnych klientów poczty i telekomunikacji w RFN. Co więcej, jak słusznie zauważyli Delegaci, zagrożenie taką kontrolą można uznać za wywołujące samo przez się ograniczenie wolności komunikowania się poprzez pocztę i telekomunikację, a w związku z tym stanowi to bezpośrednią ingerencję w prawo gwarantowane w art. 8 wszystkim użytkownikom lub potencjalnym użytkownikom tych usług...

38.  Biorąc pod uwagę szczególne okoliczności niniejszej sprawy, Trybunał konkluduje [jednomyślnie], że każdy z wnioskodawców był upoważniony do „[roszczenia sobie prawa] do bycia ofiarą naruszenia” Konwencji, nawet gdy nie był w stanie wykazać w swojej skardze, że był przedmiotem zastosowania określonych środków kontroli. Pytanie, czy wnioskodawcy byli rzeczywiście ofiarami jakiegoś naruszenia Konwencji, wymaga także określenia, czy zaskarżona Ustawa jest sama przez się zgodna z przepisami Konwencji ...”

166. Mając na uwadze sprawę *Klass i Inni,* orzecznictwo organów Konwencji rozwinęło dwa równoległe podejścia do statusu ofiary w sprawach dotyczących tajnego nadzoru.

167.  W kilku sprawach Komisja oraz Trybunał utrzymali, że test zastosowany w sprawie *Klass i Inni* nie może być interpretowany na tyle szeroko, by obejmować każdą osobę w Państwie-Stronie, która obawia się, że służby bezpieczeństwa mogą zbierać o niej informacje. Od skarżącego nie można jednak rozsądnie oczekiwać udowodnienia, że informacje dotyczące jego prywatnego życia były zbierane i przechowywane. W zakresie tajnych środków wystarczające jest ustalenie istnienia praktyk zezwalających na tajny nadzór oraz wykazanie, że wystąpiło rzeczywiste prawdopodobieństwo, że służby bezpieczeństwa zbierały i przechowywały informacje dotyczące jego prywatnego życia (zob. *Esbester,* cyt. pow.; *Redgrave,* cyt. pow.; *Christie przeciwko Zjednoczonemu Królestwu*, no. 21482/93, Decyzja Komisji z dnia 27 czerwca 1994; *Matthews,* cyt. pow.; *Halford,* cyt. pow. §§ 47 i 55‑57; oraz *Iliya Stefanov przeciwko Bułgarii*, nr 65755/01, §§ 49 i 50, 22 maja 2008). We wszystkich powyższych sprawa skarżący zarzucili faktyczne przechwytywanie swoich transmisji komunikacyjnych. W niektórych sprawach zostały złożone skargi ogólne na ustawodawstwo i praktykę zezwalającą na tajny nadzór (zob. *Esbester, Redgrave, Matthews,* i *Christie*, wszystkie cyt. pow.).

168.  W innych sprawach Trybunał powtórzył podejście ze sprawy *Klass i Inni,* że samo istnienie prawa i praktyk dopuszczających istnienie i ustanawiających system tajnego nadzoru komunikacji wiąże się z zagrożeniem stosowania nadzoru wobec wszystkich potencjalnych adresatów przepisów. To zagrożenie zdecydowanie wywarło wpływ na zakres korzystania z wolności komunikacji pomiędzy użytkownikami usług telekomunikacyjnych i w związku z tym samo sobie stanowiło ingerencję w korzystanie z praw przez skarżącego na mocy Artykułu 8, niezależnie od jakichkolwiek środków podjętych wobec niego (zob. *Malone* cyt. pow., § 64; *Weber i Saravia,* cyt. pow, § 78; *Association for European Integration and Human Rights i Ekimdzhiev,* cyt. pow. §§ 58, 59 i 69; *Liberty i Inni,* cyt. pow. §§ 56 i 57; oraz *Iordachi i Inni przeciwko Mołdawii*, nr 25198/02, §§ 30-35, 10 lutego 2009). We wszystkich powyższych sprawach skarżący złożyli skargi ogólne na ustawodawstwo i praktykę zezwalającą na stosowanie środków tajnego nadzoru. W niektórych z nich, zaskarżono również faktyczne przechwytywanie transmisji komunikacyjnej (zob. *Malone,* cyt. pow. § 62; oraz *Liberty i Inni,* cyt. pow., §§ 41 i 42).

169. Wreszcie, w swojej ostatniej sprawie w tym przedmiocie, *Kennedy przeciwko Zjednoczonemu Królestwu,* Trybunał utrzymał, że należy mieć na względzie szczególne powody usprawiedliwiające w sprawach dotyczących stosowania tajnych środków odstępstwo Trybunału od ogólnego podejścia, zgodnie z którym odmawia się jednostkom możliwości kwestionowana przepisów prawnych *in abstracto*. Podstawowe znaczenie miało zagwarantowanie, aby tajność owych środków nie skutkowała niemożnością ich skutecznego zaskarżenia, a także zapewnienie możliwości nadzoru krajowych władz sądowniczych lub Trybunału. W celu określenia, w konkretnej sprawie, czy dana osoba może stwierdzać ingerencję poprzez samo istnienie ustawodawstwa dopuszczającego środki tajnego nadzoru, Trybunał musi mieć na uwadze dostępność środków odwoławczych na poziomie krajowym oraz ryzyko zastosowania wobec tej osoby środków tajnego nadzoru. Tam, gdzie nie ma możliwości zakwestionowania rzekomego nałożenia środków tajnego nadzoru na poziomie krajowym, ogólne zaniepokojenie opinii publicznej możliwością nadużycia środków tajnego nadzoru, nie może być uznane za niezasadne. W takich sprawach, nawet jeżeli faktycznie ryzyko inwigilacji jest niewielkie, kontrola Trybunału jest niezbędna (zob. *Kennedy,* cyt. pow., § 124).

(ii)  Harmonizacja podejścia

170.  Trybunał stwierdza na tej podstawie, że istnieje potrzeba doprecyzowania warunków, na mocy których skarżący może uznać się za ofiarę naruszenia Artykułu 8 bez konieczności udowadniania, że środki tajnego nadzoru zostały faktycznie wobec niego podjęte, dzięki czemu przyjęte zostaną przewidywalne i jednolite zasady.

171.  W ocenie Trybunału, kryteria przyjęte w sprawie *Kennedy* są najlepiej dopasowane do potrzeby zapewnienia, że tajność środków nadzoru nie powoduje braku możliwości ich skutecznego zaskarżania oraz nie pozostaje poza nadzorem krajowej władzy sądowniczej oraz Trybunału. Zgodnie z powyższym, Trybunał przyznaje, że skarżący może uznać się za ofiarę naruszenia powstałego samym istnieniem środków tajnego nadzoru lub ustawodawstwa dopuszczającego środki tajnego nadzoru, jeżeli spełnione są wymienione niżej warunki. Po pierwsze, Trybunał powinien wziąć pod uwagę zakres ustawodawstwa dopuszczającego środki tajnego nadzoru poprzez zbadanie, czy skarżący może rzeczywiście zostać nimi dotknięty, albo z powodu przynależności do grupy objętych danymi przepisami, albo dlatego, że dane przepisy bezpośrednio dotyczą wszystkich użytkowników usług komunikacyjnych poprzez ustanowienie systemu, w którym komunikacje każdej osoby mogą podlegać przechwytywaniu. Po drugie, Trybunał powinien wziąć pod uwagę możliwość zastosowania środków odwoławczych na poziomie krajowym oraz uzależnić stopień kontroli od stopnia skuteczności tych środków. Jak Trybunał podkreślił w sprawie *Kennedy*, jeżeli system krajowy nie zapewnia skutecznych środków odwoławczych osobie, która podejrzewa, że została poddana tajnemu nadzorowi, powszechne zaniepokojenie opinii publicznej możliwością nadużycia środków tajnego nadzoru, nie może zostać uznane za nieznajdujące uzasadnienia (zob. *Kennedy*, cyt. pow., § 124). W takich okolicznościach zagrożenie nadzorem może zostać uznane samo w sobie za ograniczające wolną komunikację przez usługi pocztowe i telefoniczne, a przez to ustanawiające potencjalne i powszechne zagrożenie bezpośredniej ingerencji w prawa gwarantowane Artykułem . W związku z tym, kontrola Trybunału jest niezbędna, a tym samym usprawiedliwione jest ustanowienie wyjątku od zasady, która zakazuje kwestionowania [przed Trybunałem] przepisów prawnych *in* *abstracto.*. W takich sprawach dana osoba nie musi wykazywać istnienia ryzyka nałożenia na nią środków tajnego nadzoru. Jeżeli natomiast system krajowy gwarantuje skuteczne środki odwoławcze, powszechne podejrzenie nadużyć jest w mniejszym stopniu uzasadnione. W takich okolicznościach, dana osoba może uznać się za ofiarę naruszenia wynikającego z samego istnienia tajnych środków lub ustawodawstwa dopuszczającego tajne środki wyłącznie wtedy, jeżeli może udowodnić, że w związku ze swoją sytuacją osobistą, potencjalnie podlega ryzyku poddania takim środkom.

172.  Stanowisko przyjęte w sprawie *Kennedy* daje zatem Trybunałowi niezbędny stopień elastyczności do rozwiązywania różnych sytuacji, które mogą powstać w kontekście tajnego nadzoru, biorąc pod uwagę cechy szczególne systemów prawnych w państwach członkowskich, mianowicie dostępne środki odwoławcze, jak i różne sytuacje osobiste skarżących.

(iii)   Stosowanie w niniejszej sprawie

173.  Nie ulega wątpliwości, że komunikacje telefoniczne wchodzą w zakres pojęć “życie prywatne” i “korespondencja” wskazanych w Artykule 8 (zob. na przykład *Liberty i Inni,* cyt. pow., § 56).

174.  Trybunał zauważa, że skarżący w niniejszej sprawie twierdzi, że ingerencja w jego prawa nastąpiła nie tyle w wyniku zastosowania wobec niego szczególnych środków, co bardziej w rezultacie samego istnienia ustawodawstwa dopuszczającego środki tajnego nadzoru oraz ryzyka poddania tego rodzaju środkom.

175.  Trybunał zauważa, że zakwestionowane przepisy ustanawiają system tajnego nadzoru, na mocy którego komunikacje każdej osoby korzystającej z usług telefonicznych rosyjskich dostawców, mogą podlegać przechwytywaniu, bez informowania ich o tym fakcie. W takim właśnie stopniu zakwestionowane przepisy bezpośrednio wpływają na wszystkich użytkowników usług telefonicznych.

176.  Co więcej, z powodów wymienionych poniżej (zob. par. 286 do 300), prawo rosyjskie nie gwarantuje skutecznych środków odwoławczych dla osób, które podejrzewają, że został wobec nich zastosowany tajny nadzór.

177.  Mając na uwadze powyższe, skarżący nie musi wykazywać, że ze względu na swoją sytuację osobistą, podlega ryzku poddania tajnemu nadzorowi.

178.  Mając na uwadze tajną naturę środków nadzoru wynikających z zakwestionowanych przepisów, szeroki zakres ich stosowania, dotyczący wszystkich użytkowników komunikacji telefonicznej, a także brak skutecznych sposobów zakwestionowania rzekomego stosowania środków tajnego nadzoru na poziomie krajowym, Trybunał uznaje zbadanie odpowiedniej legislacji *in* *abstracto* za zasadne.

179*.*W związku z tym, Trybunał uznaje prawo skarżącego do uznania się za ofiarę naruszenia Konwencji, nawet jeśli nie może stwierdzić, że skarżący został poddany konkretnemu środkowi nadzoru. Z tych samych powodów, samo istnienie zakwestionowanej legislacji skutkuje samo w sobie naruszeniem korzystania z jego praw ustanowionych w Artykule 8. W związku z tym Trybunał oddala zarzut Rządu dotyczący niemożliwości nadania skarżącemu statusu ofiary naruszenia Konwencji.

2.  Usprawiedliwienie ingerencji

(a)  Wnioski stron

(i)  Dostępność prawa krajowego

180.  Skarżący podniósł, że załączniki do Rozporządzenia nr 70 opisujące wymagania techniczne dla urządzeń instalowanych przez dostawców usług komunikacyjnych nie zostały nigdy oficjalnie opublikowane i nie były publicznie dostępne. W opinii skarżącego, wpływają one na prawa obywateli w zakresie, w jakim regulują zakres kompetencji organów ścigania w odniesieniu do środków tajnego nadzoru, i dlatego powinny zostać opublikowane. Fakt, że skarżący ostatecznie miał dostęp do [ww.] załączników w postępowaniach krajowych, nie konwalidował braku ich oficjalnej publikacji (odniósł się do *Kasymakhunov i Saybatalov przeciwko Rosji*, nr 26261/05 i 26377/06, § 92, 14 marca 2013). Nie powinno się wymagać od obywateli zaangażowania w postępowania sądowe w celu uzyskania dostępu do regulacji, które ich dotyczą. Trybunał uznał za kluczowe wyjaśnienie, wyszczególnienie i dostępność zasad stosowania środków tajnego nadzoru (*Shimovolos przeciwko Rosji*, nr 30194/09, § 68, 21 czerwca 2011).

181. Rząd podniósł, że Rozporządzenie nr 70 było w naturze techniczne i związku z tym nie podlegało oficjalnej publikacji. Zostało opublikowane w specjalnym biuletynie, *SvyazInform,* w wydaniu nr 6 z roku 1999. Było również nieodpłatnie dostępne w prawniczej bazie danych *ConsultantPlus*. Skarżący przedłożył kopię Rozporządzenia z jego załącznikami przed Trybunałem, co wykazało, że był w stanie uzyskać do niego dostęp. W związku z tym treść przepisów prawa krajowego była dostępna.

(ii)  Zakres stosowania środków tajnego nadzoru

182.  Skarżący podniósł, że Trybunał już wcześniej uznał, że OSAA nie spełniała wymogu “przewidywalności” ze względu na swobodę decyzyjną władz przy zarządzaniu “eksperymentu operacyjnego” obejmującego nagrywanie prywatnych komunikacji poprzez urządzenie transmitujące, co nie podlegało żadnym warunkom, zaś zakres i środki jego wykorzystania nie były określone (zob. *Bykov przeciwko Rosji* [GC], nr 4378/02, § 80, 10 marca 2009). Niniejsza sprawa jest podobna do sprawy *Bykov*. W szczególności, prawo rosyjskie nie określiło szczegółowo kategorii osób, które mogą podlegać środkom przechwytywania komunikacji. W szczególności, środki nadzoru nie zostały ograniczone do osób podejrzanych lub oskarżonych o popełnienie przestępstwa. Każda osoba posiadająca informację o przestępstwie, mogła mieć swój telefon na podsłuchu. Co więcej, przechwytywanie nie było ograniczone do poważnych i szczególnie poważnych przestępstw. Prawo rosyjskie zezwalało na środki przechwytywania w związku z przestępstwami średniej wagi, takimi jak np. kradzież kieszonkowa.

183.  Rząd zwrócił uwagę, że przechwytywanie transmisji komunikacyjnej może być prowadzone tylko przy wcześniejszym uzyskaniu informacji o popełnieniu przestępstwa, jego popełnianiu lub planowaniu jego popełnienia, a także informacji o osobach planujących popełnić przestępstwo, popełniających je lub o osobach, które przestępstwo już popełniły; lub o zdarzeniach czy czynnościach zagrażających bezpieczeństwu narodowemu, militarnemu, gospodarczemu lub ekologicznemu Federacji Rosyjskiej. Trybunał Konstytucyjny utrzymał w swoim orzeczeniu z 14 lipca 1998, że zbieranie informacji o prywatnym życiu danej osoby było dopuszczalne wyłącznie w celu zapobiegania, wykrywania lub prowadzenia śledztwa lub w innych celach wymienionych w OSAA.

184.  Wyłącznie przestępstwa średniej wagi, poważne i szczególnie poważne mogą stanowić podstawę do wydania polecenia o przechwytywaniu komunikacji i wyłącznie osoby podejrzane o ich popełnienie lub mające o nich informacje mogą podlegać środkom przechwytywania. Rząd podniósł w związku z tym, że Trybunał już uznał stosowanie środków nadzoru w stosunku do osoby, która nie jest podejrzewana o popełnienie żadnego przestępstwa, mogą być uznane za uzasadnione w świetle postanowień Konwencji (zob. *Greuter przeciwko Holandii* (dec.), nr 40045/98, 19 marca 2002).

185.  W stosunku do przechwytywania komunikacji dla celów ochrony bezpieczeństwa narodowego, Rząd twierdził, że wymóg “przewidywalności” nie sięga tak daleko, aby zobowiązywał on Państwa Członkowskie do wprowadzenia przepisów określających szczegółowo każde zachowanie prowadzące do wydania decyzji poddającej daną osobę nadzorowi z powodów uzasadnionych “bezpieczeństwem narodowym” (zob. *Kennedy*, cyt. pow., § 159).

(iii)  Czas trwania środków tajnego nadzoru

186.   Skarżący przedłożył, że OSAA nie wskazuje w jakich sytuacjach przechwytywanie nie może być przedłużone na okres powyżej sześciu miesięcy. Nie ustanawia również maksymalnego okresu stosowania środków przechwytywania komunikacji.

187. Rząd stwierdził, że na mocy prawa rosyjskiego przechwytywanie może być autoryzowane przez sędziego na maksymalny czas trwania sześciu miesięcy, który może być przedłużony w razie konieczności. Należy je przerwać, jeżeli śledztwo zakończyło się. Stwierdził również, że rozsądne było pozostawienie czasu trwania przechwytywania swobodzie decyzyjnej władz krajowych, mając na uwadze kompleksowość i czas trwania śledztwa w konkretnej sprawie (zob. *Kennedy*, cyt. pow.). Odniósł się również do sprawy *Van Pelt przeciwko Holandii* (nr 20555/92, decyzja Komisji z dnia 6 kwietnia 1994), gdzie Komisja uznała, że założenie podsłuchu w telefonie skarżącego na prawie dwa lata nie stanowiło naruszenia Konwencji.

(iv)  Procedury przechowywania, dostępu, badania, korzystania, komunikowania i niszczenia przechwyconych danych

188.  Skarżący następnie podniósł, że OSAA nie określiła procedur dla przechowywania, dostępu, badania, korzystania, i niszczenia przechwyconych danych, a także środków ostrożności, jakie należy powziąć podczas komunikowania danych innym stronom. [Akt ten] stanowił, że dane mają zostać zniszczone w ciągu sześciu miesięcy, chyba że dane były potrzebne w celu świadczenia usług lub zapewnienia sprawiedliwości. Nie było jednakże definicji “potrzeby świadczenia usług lub zapewnienia sprawiedliwości”. Prawo rosyjskie przewidywało również wolność prowadzącemu postępowanie sędziemu co do przechowywania lub zniszczenia po zakończeniu procesu, danych wykorzystanych jako dowód.

189. Rząd podniósł, że OSAA wymagała przechowywania nagrań przechwyconych komunikacji w warunkach wyłączających jakiekolwiek ryzyko ich przesłuchania lub skopiowania przez osoby nieupoważnione. Decyzja sądowa upoważniająca przechwytywanie transmisji komunikacyjnej, materiały, które posłużyły jako podstawa dla tej decyzji oraz dane zebrane w wyniku przechwytywania stanowią tajemnicę państwową i mają pozostać w wyłącznym posiadaniu krajowego organu realizującego przechwytywanie. Jeżeli konieczne było transmitowanie ich do śledczego, prokuratora lub sądu, mogły zostać zdeklasyfikowane przez szefów agencji prowadzących czynności operacyjno-śledcze. Upoważnienia do przechwytywania były zdeklasyfikowane przez sąd, który ją wydał. Procedura transmitowania zebranych danych w toku czynności operacyjno-śledczych do właściwych organów śledczych lub sądu, została określona w Rozporządzeniu Ministerstwa Spraw Wewnętrznych z dnia 27 września 2013 (zob. par. 58 powyżej).

190.  Dane zebrane w toku czynności operacyjno-śledczych miały być przechowywane przez jeden rok, a następnie zniszczone, chyba że były potrzebne w celu świadczenia usług lub zapewnienia sprawiedliwości. Nagrania należało przechowywać przez sześć miesięcy, a następnie zniszczyć. Prawo rosyjskie było dzięki temu przewidywalne i zawierało wystarczające gwarancje bezpieczeństwa.

(v)  upoważnienie do stosowania środków tajnego nadzoru

(α)  Skarżący

191.  Skarżący podniósł, że pomimo, że prawo krajowe wymagało uprzedniego upoważnienia do przechwytywania komunikacji, procedura uzyskania takiego upoważnienia nie tworzyła wystarczających gwarancji bezpieczeństwa, chroniących przed nadużyciami. Po pierwsze, w pilnych sprawach komunikacje mogły być przechwytywane bez upoważnienia sądowego do czterdziestu ośmiu godzin. Po drugie, w przeciwieństwie do KPK, OSAA nie ustanawiała żadnych wymagań dotyczących treści upoważnienia do przechwytywania komunikacji. W szczególności, nie wymagała jasnego sprecyzowania kogo dotyczyłoby wydane upoważnienie poprzez wskazanie imienia, numeru telefonu lub adresu (zob. dla porównania, ustawodawstwo Zjednoczonego Królestwa i Bułgarii przywołane w orzeczeniu w sprawie *Kennedy*, cyt. pow., §§ 41 i 160; oraz *Association for European Integration and Human Rights and Ekimdzhiev*, cyt. pow., § 13). Również prawo krajowe nie wymagało sprecyzowania w upoważnieniu do przechwytywania komunikacji, które komunikacje lub rodzaje komunikacji powinny być nagrywane w celu ograniczenia swobody decyzyjnej organów ścigania, w określaniu zakresu środków nadzoru. Prawo rosyjskie nie przewidywało żadnych szczególnych zasad nadzoru w sytuacjach wrażliwych, na przykład w sytuacjach, w których chodzi o poufność źródeł dziennikarzy lub gdzie nadzór dotyczy uprzywilejowanych komunikacji prawnik-klient.

192.  Skarżący następnie wykazał, że prawo krajowe nie nakładało żadnych wymagań na sędziego, by zweryfikować istnienie “uzasadnionego podejrzenia” przeciwko osobie, której sprawa dotyczy ani nakładało obowiązku zastosowania testu “konieczności” lub “proporcjonalności”. Organy nie miały obowiązku załączania materiałów popierających wniosek o przechwytywanie. Co więcej, OSAA wyraźnie zakazała wnioskowania do sędziego o określone materiały – te zawierające informacje o agentach działających pod przykryciem lub informatorach policyjnych albo o organizacji i taktyce stosowania środków operacyjno-rozpoznawczych – poprzez co uniemożliwiono skuteczne zweryfikowanie przez sędziego istnienia wspomnianego “uzasadnionego podejrzenia”. Prawo rosyjskie nie wymaga od sędziego wydania upoważnienia do przechwytywania komunikacji tylko w przypadku, gdy niemożliwe jest osiągnięcie uzasadnionych celów poprzez inne, mniej inwazyjne środki.

193.  Na poparcie swoich twierdzeń, że sędziowie nie weryfikowali istnienia “uzasadnionego podejrzenia” wobec osób, których [komunikacja miała być przechwytywana] i nie stosowali testów “konieczności” ani “proporcjonalności”, skarżący przedstawił kopie notatek analitycznych wydanych przez trzy Sądy Rejonowe w innych regionach Rosji (Tambov, Tula i Republika Dagestan). Sądy podsumowały własne orzecznictwo dotyczące środków operacyjno-rozpoznawczych uwzględniających ingerencję w prywatność komunikacji lub mieszkania w okresie od 2010 do 2013. Jeden z sądów wskazał, że odmówił upoważnienia do podjęcia środków operacyjno-rozpoznawczych, jeżeli nie znajdowały się na liście środków operacyjno-rozpoznawczych OSAA, jeżeli wniosek o upoważnienie nie był podpisany przez właściwego urzędnika lub nie był uzasadniony albo jeżeli sprawa podlegała ustawowym ograniczeniom korzystania z tego środka (na przykład, w przypadku statusu osoby lub natury przestępstwa). Upoważnienie było przyznawane, jeżeli zostały spełnione wszystkie powyższe warunki. Inny sąd stwierdził, że można było odmówić upoważnienia również w sytuacji, w której wniosek był niewystarczająco uzasadniony, to znaczy, jeżeli nie zawierał wystarczających informacji dających sędziemu gwarancję, że środki są legalne i usprawiedliwione. Trzeci sąd oznajmił, że przyznaje upoważnienie, jeżeli wniosły o to organy śledcze. Nigdy nie odmówił wydania wnioskowanego upoważnienia. Wszystkie trzy sądy uznały, że wniosek był wystarczająco uzasadniony, jeżeli odnosił się do istnienia informacji wymienionych w sekcji 8(2) OSAA (zob. par. 31 powyżej). Jeden z sądów stwierdził, że materiały doręczone w celu poparcia wniosku nigdy nie były dołączone do wniosku o upoważnienie; inny sąd zauważył, że niektóre, ale nie wszystkie wnioski były składane wraz z materiałami na ich poparcie, podczas gdy trzeci sąd stwierdził, że wszystkie wnioski były składane z materiałami na ich poparcie. We wszystkich trzech sądach sędziowie nigdy nie żądali od organów ścigania przedłożenia dodatkowych materiałów, takich jak potwierdzenia przyczyn przechwytywania czy udowadniających, że numery, mające być na podsłuchu należą do konkretnej osoby. Dwa sądy przyznały upoważnienie do przechwytywania komunikacji wobec nieokreślonych osób, jeden z nich określił, że upoważnienie to dotyczyło wyłącznie zebrania danych z technicznych kanałów komunikacji. Takie upoważnienie nie określało osoby ani numeru telefonu, który miał być na podsłuchu, ale zezwalało na przechwytywanie wszystkich komunikacji telefonicznych w obrębie popełnienia przestępstwa. Jeden sąd nigdy nie przydzielił takiego upoważnienia. Dwa sądy stwierdziły, że upoważnienia zawsze wskazywały okres trwania przechwytywania, podczas gdy jeden stwierdził, że okres trwania przechwytywania nie był wskazany w wydanym przez niego upoważnieniu. Ostatecznie, żaden z trzech sądów nie zbadał skarg od osób, których komunikacje były przechwytywane.

194.  Skarżący przedstawił również oficjalne statystyki Sądu Najwyższego z okresu od 2009 do 2013 roku. Ze statystyk tych wynika, że w roku 2009 rosyjskie sądy uwzględniły 130,083 z 132,821 wniosków na mocy KPK i 245,645 z 246,228 wniosków na mocy OSAA (99%). W 2010 roku sądy uwzględniły 136,953 z 140,372 wniosków o przechwytywanie na mocy KPK i 276,682 z 284,137 wniosków na mocy OSAA. W 2011 sądy uwzględniły 140,047 z 144,762 wniosków o przechwytywanie na mocy KPK i 326,105 z 329,415 wniosków na mocy OSAA. W 2012 uwzględniły 156,751 z 163,469 wniosków o przechwytywanie na mocy KPK (95%) oraz 372,744 z 376,368 wniosków na mocy OSAA (99%). W 2013 roku sądy uwzględniły 178,149 z 189,741 wniosków o przechwytywanie złożonych na mocy KPK (93%) i 416,045 z 420,242 wniosków o przechwytywanie złożonych na mocy OSAA (99%). Skarżący zwrócił uwagę Trybunału na fakt, że ilość upoważnień do przechwytywania prawie się podwoiła w okresie pomiędzy 2009 a 2013 rokiem. Wykazał również, że wysoki procent przyznanych upoważnień pokazał, że sędziowie nie weryfikowali istnienia “uzasadnionego podejrzenia” wobec podmiotu przechwytywania oraz nie zastosował ostrożnej i rygorystycznej kontroli. W rezultacie upoważnienia do przechwytywania były przyznane w stosunku do ogromnej liczby ludzi w sytuacjach, gdzie informacje mogły być uzyskane poprzez mniej inwazyjne środki.

195.  Skarżący wywnioskował z powyższego, że procedura upoważnienia była wadliwa, a poprzez to nie ograniczała użycia środków nadzoru w sposób konieczny w społeczeństwie demokratycznym.

196.  W stosunku do gwarancji bezpieczeństwa wobec nieupoważnionych przechwytywań, skarżący stwierdził, że od organów ścigania nie wymaga się, na mocy prawa krajowego, przedkładania upoważnienia sądowego dostawcom usług komunikacyjnych przed uzyskaniem dostępu do komunikacji danej osoby. Wszystkie upoważnienia sądowe są dokumentami klasyfikowanymi, w wyłącznym posiadaniu organów ścigania. Obowiązek przekazywania upoważnienia do przechwytywania komunikacji dostawcom usług komunikacyjnych został wspomniany wyłącznie w prawie rosyjskim dotyczącym monitoringu danych komunikacyjnych na mocy KPK (zob. par. 48 powyżej). Urządzenia, które dostawcy usług komunikacyjnych zainstalowali zgodnie z Rozporządzeniami wydanymi przez Ministra Komunikacji, w szczególności z nieopublikowanymi załącznikami do Rozporządzenia nr 70, zezwalały organom ścigania na zdalny i nieograniczony dostęp do wszystkich komunikacji komórkowych wszystkich użytkowników. Dostawcy usług komunikacyjnych zostali zobowiązani również, na mocy Rozporządzenia nr 538 do tworzenia baz danych przechowujących na okres trzech lat informacje o wszystkich użytkownikach oraz usługach, z których korzystają. Tajne służby miały zdalny dostęp do tych baz danych. Sposób, w jaki system tajnego nadzoru był obsługiwany dawał służbom bezpieczeństwa oraz policji środki techniczne do ograniczania procedury upoważnienia oraz do przechwytywania wszystkich komunikacji bez uprzedniego upoważnienia sądowego. W związku z tym, konieczność uzyskania uprzedniego upoważnienia sądowego istniała tylko w sprawach, gdzie przechwytywane dane miały zostać wykorzystane jako dowody w postępowaniach karnych.

197.  Skarżący przedstawił dokumenty, które według niego pokazywały, że organy ścigania bezprawnie przechwytywały komunikacje, bez uzyskania uprzedniego upoważnienia sądowego oraz ujawniały nagarnia osobom nieupoważnionym. Na przykład, przedstawił wydruki z Internetu zawierające transkrypty prywatnych rozmów telefonicznych polityków. Przedstawił również artykuły z wiadomościami opisujące postępowania karne przeciwko kilku wysoko postawionym oficerom policji z departamentu technicznego. Oficerowie byli podejrzani o bezprawne przechwytywanie prywatnych komunikacji polityków i biznesmenów w zamian za łapówki od ich politycznych lub biznesowych rywali. Artykuły odnosiły się do zeznań świadków w ten sposób, że przechwytywanie transmisji komunikacyjnej w zamian za łapówki jest powszechną praktyką oraz, że każdy może kupić od policji transkrypt rozmowy telefonicznej innej osoby.

(β)  Rząd

198.  Rząd podniósł, że na każde przechwytywanie komunikacji telefonicznej lub innej sąd musiał wydać zgodę. Sad wydał decyzję na podstawie uzasadnionego wniosku organów ścigania. Ciężar dowodu spoczywa na organie wnioskującym, który powinien uzasadnić konieczność zastosowania środków przechwytywania. W tym celu organ wnioskujący załączył do wniosku wszystkie odpowiednie materiały, poza materiałami zawierającymi informacje o agentach działających pod przykryciem lub informatorach policyjnych albo o organizacji i taktyce stosowania środków operacyjno-rozpoznawczych. Wyjątek ten był usprawiedliwiony koniecznością zapewnienia bezpieczeństwa i ochroną agentów działających pod przykryciem, a także informatorów policyjnych i członków ich rodzin, a tym samym zgodny z Konwencją.

199.  Rząd dalej odniósł się do Uchwały Sądu Najwyższego z sesji plenarnej z dnia 27 czerwca 2013, która wyjaśniała sądom niższej instancji, że jakiekolwiek ograniczenia praw i wolności człowieka muszą być przewidziane przez prawo oraz być konieczne w demokratycznym społeczeństwie, tj. proporcjonalne do słusznego celu. Sądy zostały poinstruowane, aby opierać się na ustalonych faktach, weryfikować istnienie odpowiednich i wystarczających powodów usprawiedliwiających ograniczenie praw osoby oraz zbalansować interesy innych osób, Państwa i społeczeństwa. OSAA wyraźnie wymagała od sądów podania powodów podjęcia decyzji o upoważnieniu do przechwytywania komunikacji. Zgodnie z decyzją Trybunału Konstytucyjnego z dnia 8 lutego 2007 (zob. par. 42 powyżej), upoważnienie do przechwytywania komunikacji powinno zawierać odniesienia do szczególnych powodów podejrzewania osoby, w stosunku do której został złożony wniosek o podjęcie środków operacyjno-rozpoznawczych ze względu na popełnienie przestępstwa lub czynności zagrażających bezpieczeństwu narodowemu, militarnemu, gospodarczemu lub ekologicznemu. W swojej decyzji z dnia 2 października 2003 (zob. par. 41 powyżej), Trybunał Konstytucyjny utrzymał również, że sędziowie są zobowiązani do uważnego i dokładnego zbadania przedstawionych im materiałów.

200. Jak twierdzi Rząd, w praktyce każde upoważnienie do przechwytywania komunikacji wskazuje organ krajowy odpowiedzialny za wykonanie przechwytywania, przyczyny uzasadniające wprowadzenie środków nadzoru oraz powody, dla których ich wprowadzenie było konieczne, [a także] odwołanie do odpowiednich przepisów prawnych, osobę, której komunikacje mają być przechwytywane, przyczyny podejrzewania osoby o zaangażowanie w popełnienie konkretnego przestępstwa, numer telefonu tej osoby lub kod IMEI, okres, na które upoważnienie zostało przyznane oraz inne niezbędne informacje. W wyjątkowych okolicznościach dopuszczalne było upoważnienie do przechwytywania komunikacji niezidentyfikowanych osób. W zasadzie, w takich sprawach, sędzia upoważniał zbieranie danych z technicznych kanałów komunikacji w celu zidentyfikowania obecności osoby w konkretnym miejscu, w czasie popełnienia tam przestępstwa. Ta praktyka była zgodna z przepisami ustanowionymi w orzecznictwie Trybunału, ponieważ w takich sprawach upoważnienia do przechwytywania komunikacji określało jednolity zestaw lokali (lokalizacji) jako miejsca, w stosunku do którego upoważnienie zostało przyznane (odniesiono się do sprawy *Kennedy*, cyt. pow.).

201.  Prawo rosyjskie zezwalało na przechwytywanie komunikacji bez uprzedniego upoważnienia sądowego w pilnych sprawach. Sędzia musiał zostać poinformowany o takich sprawach w ciągu dwudziestu czterech godzin, a każde upoważnienie do kontynuowania przechwytywania komunikacji musiało zostać wydane w ciągu czterdziestu ośmiu godzin. Odniesiono się do wyroku z dnia 13 grudnia 2013 r wydanego w sprawie karnej w wyniku postępowania odwoławczego, w której Sąd Najwyższy uznał niedopuszczalność dowodową nagrań rozmów telefonicznych uzyskanych bez uprzedniego upoważnienia sądowego w wyniku stosowania „pilnej” procedury. Sąd Najwyższy utrzymał, że pomimo, że sędzia został poinformowany o przechwytywaniu komunikacji, nigdy nie została wydana decyzja o legalności i konieczności tego działania.

(vi)  Kontrola implementacji tajnych środków nadzoru

(α)  Skarżący

202.  W kwestii nadzoru nad przechwytywaniem komunikacji, skarżący stwierdził, że w Rosji efektywność tego nadzoru jest wątpliwa ze względu na brak obowiązku organów przechwytujących do zachowania nagrań przechwytywanej komunikacji. Co więcej, Rozporządzenie nr 70 wyraźnie stanowiło, że informacje o przechwytywaniu nie mogą być zapisywane ani nagrywane.

203.  Skarżący następnie dowodził, że w Rosji ani sędzia, który wydał upoważnienie do przechwytywania komunikacji ani żaden inny niezależny urząd wykwalifikowany do sprawowania kontroli sądowej nie miał kompetencji do kontrolowania sposobu korzystania z wydanego upoważnienia, a w szczególności do weryfikowania, czy nadzór utrzymywał się w zakresie określonym przez upoważnienie do przechwytywania komunikacji oraz czy spełniał różne wymogi zawarte w prawie krajowym.

204. Prawo krajowe nie przewidywało żadnych procedur kontroli przechwytywania komunikacji, które byłyby powierzone prezydentowi, parlamentowi czy rządowi. Na pewno nie mieli oni kompetencji, by kontrolować sposób stosowania środków nadzoru w konkretnych sprawach.

 205.  Co się tyczy kontroli dokonywanej przez Prokuratora Generalnego oraz kompetentnego prokuratora niższego szczebla, nie można uznać ich za niezależnych ze względu na ich pozycję w systemie sprawiedliwości oraz ze względu na pełnione przez nich zadania prokuratorskie. W szczególności, prokuratorzy dawali przyzwolenie na wszystkie wnioski o przechwytywanie komunikacji złożone przez śledczych w ramach postępowań karnych oraz brali udział w związanych z tym sprawach karnych. Mogli wówczas wykorzystać dane uzyskane w wyniku przechwytywania w ramach swoich zadań, szczególnie poprzez przedstawienie ich jako dowodu podczas procesu. W związku z tym mamy do czynienia z konfliktem interesu w przypadku prokuratora pełniącego funkcję strony w postępowaniu karnym i organu kontrolującego przechwytywanie komunikacji.

206. Skarżący dalej wnosił, że kompetencje kontrolne prokuratora były ograniczone, ponieważ niektóre materiały, w szczególności te ujawniające tożsamość agentów działających pod przykryciem lub taktykę, metody i środki wykorzystane przez służby bezpieczeństwa, znajdowały się poza zakresem kontroli. Zakres kontroli prokuratorów również był ograniczony w strefie kontrwywiadu, gdzie inspekcje mogły być podejmowane wyłącznie w następstwie wniesienia skargi indywidualnej. Mając na uwadze tajność środków przechwytywania i brak powiadomienia osoby, której dotyczyły, indywidualne skargi z reguły nie były składane, w wyniku czego środki nadzoru związane w kontrwywiadem *de facto* wydostawały się spod jakiejkolwiek kontroli prokuratorskiej. Znaczące było również, że prokuratorzy nie mieli możliwości odwołania upoważnienia do przechwytywania komunikacji, w celu zaprzestania bezprawnego przechwytywania lub niszczenia bezprawnie uzyskanych danych.

207.  Następnie należy zauważyć, że wydawane dwa razy w roku raporty prokuratora nie zostały opublikowane ani poddane dyskusji. Raporty zostały sklasyfikowane i zawierały wyłącznie informacje statystyczne. Nie zawierały żadnej merytorycznej analizy legalności podejmowanych czynności operacyjno-rozpoznawczych na terenie kraju, ani informacji o wykrytych naruszeniach prawa oraz w zakresie tego, jakie środki zostały podjęte, by im zadośćuczynić. Co więcej, raporty opisały w sposób łączny wszystkie rodzaje czynności operacyjno-rozpoznawczych, nie oddzielając przechwytywania komunikacji od innych środków.

(β)  Rząd

208.  Rząd podniósł, że kontrola czynności operacyjno-rozpoznawczych obejmujących przechwytywanie komunikacji telefonicznych, była wykonywana przez Prezydenta, Parlament i Rząd. W szczególności, Prezydent określał narodową strategię bezpieczeństwa, mianował i dymisjonował przewodniczących organów śledczych. Istniał również specjalny departament przy Administracji Prezydenckiej, który nadzorował czynności organów ścigania, włączając w to czynności operacyjno-rozpoznawcze. Departament ten składał się z urzędników z Ministerstwa Spraw Wewnętrznych oraz FSB, którzy posiadali odpowiedni poziom certyfikatu bezpieczeństwa. Parlament brał udział w procedurze kontrolnej poprzez przyjmowanie poprawek i zmian w ustawodawstwie dotyczącym sposobu prowadzenia czynności operacyjno-rozpoznawczych. Był również uprawniony do powoływania komitetów i komisji, a także zwoływania posiedzeń dotyczących wszystkich kwestii, włączając te związane z czynnościami operacyjno-rozpoznawczymi, a także mógł, w razie konieczności, przesłuchać kierowników organów śledczych. Rząd przyjął dekrety i rozporządzenia zarządzające czynnościami operacyjno-rozpoznawczymi, a także przydzielił organom ścigania odpowiednie środki budżetowe.

209.  Kontrola była również sprawowana przez Prokuratora Generalnego oraz kompetentnych prokuratorów niższego szczebla niezależnych od władz federalnych, regionalnych i lokalnych. Prokurator Generalny i jego zastępcy byli mianowani i dymisjonowani przez Radę Federalną (wyższą izbę Parlamentu). Prokuratorzy nie byli upoważnieni do składania wniosków o przechwytywanie komunikacji. Wnioski te mogły być składane przez Agencję Rządową wykonującą czynności operacyjno-rozpoznawcze w ramach OSAA, lub przez śledczego w ramach KPK. Prokurator nie mógł udzielać śledczemu żadnych instrukcji. W toku inspekcji prokuratora, przewodniczący organu śledczego był zobowiązany do złożenia odpowiednich materiałów prokuratorowi na jego wniosek oraz mógł ponosić odpowiedzialność za niewywiązanie się z tego zobowiązania. Prokuratorzy odpowiedzialni za kontrolę nad czynnościami operacyjno-rozpoznawczymi składali półroczne raporty Prokuratorowi Generalnemu. Raporty jednak nie analizowały przechwytywań komunikacji oddzielnie od innych środków operacyjno-rozpoznawczych.

vii)  Powiadomienie o środkach tajnego nadzoru

(α)  Skarżący

210.  Skarżący następnie podniósł, że prawo rosyjskie nie przewidywało, żeby osoba, której komunikacje były przechwytywane, musiała być o tym powiadomiona przed, w trakcie lub po przechwytywaniu. Przyznał, że dopuszczalne było nieinformowanie osoby przed przechwytywaniem lub w trakcie, ponieważ tajność środków była istotna dla ich skuteczności. Zaznaczył, jednakże, że takie powiadomienie było możliwe po zakończeniu przechwytywania, “tak szybko jak to możliwe, bez stwarzania zagrożenia dla celu wprowadzanego ograniczenia” (odniósł się do *Klass i Inni,* cyt. pow.). W Rosji osoba, której przechwytywanie komunikacji dotyczyło, nie była informowana w żadnym stadium. Mogłaby w związku z tym dowiedzieć się o przechwytywaniu komunikacji tylko wtedy, jeżeli nastąpiłby przeciek informacji lub gdy postępowanie karne przeciwko niej było jawne, a przechwytywane dane zostały wykorzystane jako dowód.

211.  Odnosząc się do możliwości uzyskania dostępu do danych zebranych w toku przechwytywania komunikacji, skarżący stwierdził, że dostęp taki był możliwy tylko w pewnych okolicznościach. Jeżeli postępowanie karne nigdy nie zostało wszczęte lub jeżeli zarzuty zostały oddalone z innych powodów niż tych wymienionych w OSAA, osoba, której komunikacja była przechwytywana, nie była upoważniona do dostępu do tych danych. Co więcej, przed uzyskaniem dostępu, należało udowodnić, że komunikacja była przechwytywana. Mając na uwadze tajność środków nadzoru i brak powiadomienia, przedstawienie dowodów było niemożliwe, chyba że informacja o przechwytywaniu przeciekła. Nawet po spełnieniu tych warunków wstępnych, dana osoba mogła otrzymać wyłącznie ,,informacje o zebranych danych”, nie uzyskując dostępu do samych danych. Ostatecznie, mogły być ujawnione tylko informacje niezawierające tajemnicy państwowej. Mając na uwadze, że na mocy OSAA wszystkie dane zebrane w toku czynności operacyjno-rozpoznawczych stanowiły tajemnicę państwową, a decyzja o zdeklasyfikowaniu ich należała do przewodniczącego organu przechwytującego, dostęp do dokumentów związanych z przechwytywaniem zależał całkowicie od decyzji organu przechwytującego.

212.  Odmowa przyznania dostępu do zebranych danych stanowi przesłankę wniesienia apelacji, a OSAA wymagała od organów przechwytywania przedstawienia, na żądanie sędziego, “materiałów operacyjno-rozpoznawczych zawierających informacje o danych, do których odmówiono dostępu”. Znaczące było, że organy przechwytujące powinny przedstawić “informacje o danych”, a nie dane same w sobie. Materiały zawierające informacje o agentach działających pod przykryciem i informatorach policyjnych nie mogły być przedstawione przed sądem i w związku z tym były wyłączone z zakresu kontroli sądowej.

(β)  Rząd

213.  Rząd podniósł, że na mocy prawa rosyjskiego, podmiot środków tajnego nadzoru nie musiał być informowany o tych środkach w żadnym stadium. Trybunał Konstytucyjny stwierdził (zob. par. 40 powyżej), że dla celu utrzymania tajności środków nadzoru, zasady publicznego charakteru rozprawy i postępowań prywatno-dowodowych nie miały zastosowania w przypadku procedury zmierzającej do uzyskania upoważnienia do przechwytywania komunikacji. Osoba, której ona dotyczyła, nie była uprawniona do brania udziału w tej procedurze ani do informacji o podjętych decyzjach.

214.  Po zakończeniu śledztwa, pozwany był uprawniony do zbadania wszystkich materiałów z akt sprawy karnej, w tym także danych uzyskanych w toku czynności operacyjno-rozpoznawczych. W innym przypadku, w sprawach, w których organ śledczy decydował o niewszczynaniu postępowania karnego przeciwko podmiotowi przechwytywania lub o przerwaniu postępowania karnego ze względu na brak popełnienia rzekomego przestępstwa lub gdy niespełnione było znamię lub znamiona przestępstwa, podmiot przechwytywania był uprawniony uzyskania informacji o zebranych danych. Odmowa udzielenia takiej informacji mogła być zakwestionowana przed sądem, który mógł nakazać udostępnienie informacji, jeżeli uznał odmowę za bezzasadną. Rząd przedłożył kopię decyzji z dnia 4 sierpnia 2009 z Sądu Rejonowego Alekseyevskiy z Regionu Belgorod, według której policja powinna dostarczać w ciągu jednego miesiąca, podmiotowi przechwytywania wszystkie dane o nim zebrane w toku przechwytywania komunikacji “w zakresie, w jakim zezwalały na to wymagania poufności oraz za wyjątkiem danych, które umożliwiłyby ujawnienie tajemnicy Państwowej”.

215. Rząd twierdził, że prawo rosyjskie różniło się od prawa bułgarskiego, skrytykowanego przez Trybunał w jego wyroku *Association for European Integration and Human Rights and Ekimdzhiev* (cyt. pow. § 91),ponieważ przewidywało możliwość zdeklasyfikowania materiałów przechwytywania oraz udzielenia osobie zainteresowanej dostępu do nich. Na poparcie tego twierdzenia, odniósł się do wyroku skazującego z dnia 11 lipca 2010 Sądu Okręgowego Zabaykalsk. Wyrok ten – którego kopia nie została dostarczona Trybunałowi – opierał się, zgodnie z twierdzeniem Rządu, na decyzji sądowej upoważniającej przechwytywanie komunikacji telefonicznej pozwanego, która została zdeklasyfikowana oraz przedstawiona sędziemu na jego żądanie. Rząd również odniósł się do dwóch kolejnych wyroków – Prezydium Sądu Okręgowego Krasnoyarsk oraz Prezydium Sądu Najwyższego Republiki Mariy-El Republic – oddalających na postanowienia sądowe upoważniające przechwytywanie transmisji komunikacyjnej. Nie przedłożono kopii wyroków.

(viii)  Dostępne środki odwoławcze

(α)  Skarżący

216.  Skarżący wniósł, że kwestia powiadamiania o środki nadzoru była nieodzownie związana z efektywnością sądowych środków odwoławczych , ze względu na to, iż co do zasady istniał niewielki zakres spraw umożliwiających zwracanie się do sądów przez osoby zainteresowane, jeśli nie był on powiadomiony o powziętych środkach, bez swojej wiedzy i dlatego mógł zakwestionować ich legalność z mocą wsteczną (odniósł się do *Weber i Saravia*, cyt.pow.).

217.  Skarżący podniósł, że środki odwoławcze dostępne na mocy prawa rosyjskiego były nieefektywne. Co się tyczy możliwości nadzorowanego podmiotu do ubiegania się o kontrolę sądową zastosowanych środków, ciężar dowodu spoczywał na powodzie, który powinien wykazać, że jego telefon był na podsłuchu. Jednakże, odkąd osoby monitorowane nie były informowane o środkach nadzoru do momentu oskarżenia o przestępstwo, niemożliwe było wykazanie dowodu. Kopie wyroków sądów krajowych dostarczone przez Rząd dotyczyły przeszukań i zajęcia mienia, tj. czynności operacyjno-rozpoznawczych, o których osoba zainteresowana wiedziała (zob. par. 220, 221, i 223 poniżej). Skarżący wiedział o braku rozgłosu przy decyzjach sądowych dotyczących uznania skarg osoby, której komunikację przechwytywano bezprawne. Znaczące było również, że żaden z wyroków przedstawionych przez Rząd nie zawierał oceny sądów co do proporcjonalności stosowania spornych środków operacyjno-rozpoznawczych. Postępowania krajowe wszczęte przez skarżącego wyraźnie ukazywały, że środki odwoławcze dostępne na mocy prawa rosyjskiego były nieefektywne. Co więcej, w sprawie *Avanesyan przeciwko Rosji* (nr 41152/06, 18 września 2014) Trybunał uznał, że na mocy prawa rosyjskiego nie było efektywnych środków odwoławczych do zakwestionowania zastosowanych środków operacyjno-rozpoznawczych.

218.  W końcu, skarżący wniósł, że podmiot przechwytywania lub dostawcy usług komunikacyjnych nie mogli zakwestionować rozporządzeń ministra o tajnym przechwytywaniu komunikacji, ponieważ rozporządzenia te uznawane były za bardziej techniczne niż prawne w swej naturze i w związku z tym nie podlegały rewizji sądowej, jak wskazano w decyzjach, o których mowa w paragrafie 161 powyżej.

(β)  Rząd

219.  Rząd podniósł, że w Rosji osoba, która twierdzi, że jej prawa zostały naruszone przez organ państwowy wykonujący czynności operacyjno-rozpoznawcze była upoważniona do wniesienia skargi do osoby kierującej danym organem, prokuratora lub sądu, zgodnie z sekcją 5 OSAA (zob. par. 83 powyżej).

220.  Jak wskazało Zgromadzenie Ogólne Sądu Najwyższego osoba zainteresowana, która dowiedziała się o przechwytywaniu komunikacji mogła odwołać się do sądu powszechnego zgodnie z procedurą ustanowioną w Rozdziale 25 Kodeksu Postępowania Cywilnego (zob. par. 92 powyżej). Zgodnie z twierdzeniem Rządu, powód nie musiał udowadniać, że jego prawa zostały naruszone w rezultacie stosowania środków przechwytywania. Ciężar dowodu spoczywał na organach przechwytywania, który musiał udowodnić, że środki przechwytywania były legalne i usprawiedliwione. Prawo rosyjskie stanowiło, że jeżeli sąd uznał w postępowaniu cywilnym naruszenie praw pozwanego, sąd musiał powziąć kroki w celu zadośćuczynienia naruszeniu oraz naprawienia szkody (zob. par. 97 powyżej). Rząd przedłożył kopie dwóch orzeczeń sądowych wydanych na mocy Rozdziału 25 Kodeksu Postępowania Cywilnego, uznających bezprawność przeszukania i zajęcia mienia lub dokumentów oraz zlecających powzięcie szczególnych środków przez policję służących zadośćuczynieniu naruszeniom.

221.   Co więcej, Rząd zwrócił uwagę, iż Trybunał Konstytucyjny wyjaśnił w swojej decyzji z dnia 15 lipca 2008 (zob. par. 43 powyżej), że osoba, której komunikację przechwytywano była również uprawniona do złożenia wniosku o rewizję orzeczeń sądowych upoważniających do przechwytywania komunikacji. Była ona również na analogicznej zasadzie uprawniona do złożenia apelacji lub kasacji.

222. Jeżeli przechwytywanie komunikacji było podjęte w ramach postępowania karnego, osoba zainteresowana mogła również złożyć skargę na mocy Artykułu 125 KPK. Rząd odniósł się do orzeczenia Sądu Najwyższego z dnia 26 października 2010 oddalającej orzeczenie sądu niższej instancji uznające za niedopuszczalną skargę K. złożoną na podstawie artykułu 125 KPK na odmowę organu śledczego do doręczenia kopii postanowienia sądowego upoważniającego do przechwytywania jej transmisji komunikacyjnej. Sąd Najwyższy utrzymał, że skarga została zbadana na postawie artykułu 125 KPK, pomimo faktu, że skarżąca została już skazana oraz że była uprawniona do otrzymania kopii upoważnienia do przechwytywania komunikacji. Rząd przedłożył kopie dziesięciu orzeczeń sądowych uwzględniających skargi złożone na podstawie artykułu 125 KPK o bezprawnych przeszukiwaniach i zajęciach mienia lub dokumentów. Dostarczył również kopię uniewinniającego wyroku sądu apelacyjnego, w którym uznano, że skazanie w pierwszej instancji oparte było na niedopuszczalnych dowodach uzyskanych w wyniku bezprawnej próby zakupu narkotyków.

223.  Rząd następnie przedłożył, że osoba zainteresowana mogła ubiegać się o zadośćuczynienie na mocy Artykułu 1069 Kodeksu Cywilnego (zob. par. 102 powyżej). Artykuł ten stanowi o rekompensacie szkody majątkowe i niemajątkowe uczynionej osobie fizycznej lub osobie prawnej przez bezprawne działanie Państwa i organów komunalnych oraz funkcjonariuszy państwowych, w sytuacji, gdy wina organu lub władz została ustalona. Zadośćuczynienie za krzywdę było określone zgodnie z zasadami wyznaczonymi w Artykułach 1099-1101 Kodeksu Cywilnego (zob. par. 103 i 104 powyżej). Rząd podkreślił, w szczególności, że krzywda spowodowana rozpowszechnianiem informacji, która może powodować uszczerbek na honorze, godności lub reputacji mogła być zadośćuczyniona niezależnie od winy osoby, która popełniła czyn zabroniony. Rząd przedłożył kopię decyzji z dnia 9 grudnia 2013 Sądu Miejskiego Vichuga regionu Ivanovo, przyznając zadośćuczynienie za krzywdę za bezprawne przechwytywanie konwersacji telefonicznych podejrzanego po uzyskaniu nagrań w wyniku przechwytywania, co nie zostało dopuszczone w charakterze dowodu przed sądem. Rząd przedłożył również decyzję sądową przyznającą zadośćuczynienie za bezprawne przeszukanie i zajęcie dokumentów oraz orzeczenie sądowe przyznające zadośćuczynienie osobie uniewinnionej za niesłuszne skazanie.

224.  Prawo rosyjskie przewidywało również środki odwoławcze na nadużycie władzy (artykuły 285 i 286 Kodeksu Karnego), nieupoważnione zbieranie lub rozpowszechnianie informacji o życiu prywatnym i rodzinnym danej osoby (art. 137 Kodeksu Karnego) oraz naruszenie praw obywateli do prywatności komunikacji (art. 138 Kodeksu Karnego) (zob. par. 19 i 22 powyżej). Rząd odniósł się w związku z tym do wyroku Sądu Najwyższego z dnia 24 października 2002, skazującego E.S. za przestępstwo na mocy art. 138 Kodeksu Karnego za podżeganie urzędnika do dostarczenia mu nazwisk właścicieli kilku numerów telefonicznych oraz szczegółów nagrań telefonicznych związanych z tymi numerami. Odniesiono się również do wyroku Sądu Najwyższego z dnia 15 marca 2007 r., skazującego urzędnika służb celnych za przestępstwo na mocy art. 138 Kodeksu Karnego za przechwytywanie komunikacji telefonicznych P. Przedłożono kopie dwóch kolejnych wyroków skazujących na mocy Artykułu 135 Kodeksu Karnego: pierwsze skazanie dotyczyło sprzedaży sprzętu szpiegowskiego, mianowicie długopisów i zegarków z wbudowanymi kamerami, natomiast drugie skazanie dotyczyło tajnego hakowania baz danych dostawców komunikacji w celu uzyskania szczegółów nagrań połączeń użytkowników.

225.  Ostatecznie, Rząd podniósł, że środki odwoławcze były również dostępne w prawie rosyjskim i pozwalały na zakwestionowanie rzekomej nieskuteczności gwarancji przeciwko nadużyciom w sferze przechwytywania komunikacji (zob. par. 156 powyżej).

226.  Rząd podniósł również, że skarżący nie wykorzystał żadnego opisanego powyżej środka odwoławczego dostępnego na mocy prawa rosyjskiego. W szczególności, zdecydował się na wszczęcie postępowania sądowego przeciwko operatorom sieci mobilnych, do którego dołączył na prawach trzeciej strony Minister Komunikacji.

(b)  Ocena Trybunału

(i)  Zasady Ogólne

227. Trybunał ponownie stwierdza, że każda ingerencja może być usprawiedliwiona wyłącznie na mocy Artykułu 8 § 2 jeżeli jest zgodna z prawem, zmierza do osiągnięcia jednego lub więcej celu prawnego, o którym stanowi paragraf 2 Artykułu 8 oraz jest konieczna w demokratycznym społeczeństwie w celu osiągnięcia takiego zamierzenia (zob. *Kennedy*, cyt. pow., § 130).

228.  Trybunał zauważa w swoim orzecznictwie, że sformułowanie “zgodnie z prawem” wymaga, aby nałożone środki miały zarówno podstawę w prawie oraz były zgodne z zasadą praworządności, która jest wyraźnie zaznaczona w Preambule Konwencji oraz nieodłączna dla przedmiotu i celu Artykułu 8. Prawo musi spełniać wymogi jakościowe: musi być dostępne dla osoby zainteresowanej oraz przewidywalne co do swoich skutków (zob. między innymi, *Rotaru przeciwko Rumunii* [GC], nr 28341/95, § 52, ETPCz 2000‑V; *S. i Marper przeciwko Zjednoczonemu Królestwu* [GC], nr 30562/04 i 30566/04, § 95, ETPCz 2008;i *Kennedy*, cyt. pow., § 151).

229. Trybunał kilkakrotnie podnosił, iż odniesienie się do [kryterium] przewidywalności w sprawach dotyczących przechwytywania komunikacji nie może być takie samo jak w innego typu sprawach. Możliwość przewidzenia w szczególnych przypadkach zastosowania tajnych środków nadzoru, takich jak przechwytywanie transmisji komunikacyjnej, nie może oznaczać, że dana osoba powinna mieć możliwość przewidzenia, kiedy prawdopodobnie władze będą przechwytywać jej komunikację i odpowiednio dostosować się do tej sytuacji. Jednakże, gdy powierzone organom władzy zadania wykonywane są w sposób niejawny, ryzyko arbitralności jest ewidentne. W związku z tym, ważne jest istnienie jasnych, wyszczególnionych zasad odnoszących się przechwytywania komunikacji telefonicznej, zwłaszcza że dostępna technologia stale staje się bardziej zaawansowana. Prawo krajowe musi być wystarczająco jasne, aby dawało obywatelom adekwatną wskazówkę co do okoliczności i warunków, w których władze są upoważnione do stosowania do takich środków (zob. *Malone,* cyt. powyżej, § 67; *Leander przeciwko Szwecji*, 26 marca 1987, § 51, Serie A nr 116; *Huvig przeciwko Francji*, 24 kwietnia 1990, § 29, Serie A nr 176‑B; *Valenzuela Contreras przeciwko Hiszpanii*, 30 lipca 1998, § 46, *Reports of Judgments and Decisions* 1998‑V; *Rotaru,* cyt. powyżej, § 55; *Weber i Saravia*, cyt. powyżej, § 93; oraz *Association for European Integration and Human Rights and Ekimdzhiev,* cyt. powyżej, § 75).

230.  Co więcej, ponieważ uruchomienie kontroli stosowania środków tajnego nadzoru komunikacji w praktyce nie jest dostępne tak dla objętych nią osób jak i dla społeczeństwa, to zasada państwa prawa byłaby naruszona gdyby przyznać niczym nieograniczoną władzę dyskrecjonalną organom władzy wykonawczej lub sędziemu. W konsekwencji, prawo musi wskazywać zakres takiej swobody decyzyjnej przyznanej właściwym organom władzy oraz sposób korzystania z niej z wystarczającą jasnością, aby osoby miały odpowiednią ochronę przed arbitralną ingerencją (zob. między innymi, *Malone*, cyt. powyżej, § 68; *Leander*, cyt. powyżej, § 51; *Huvig*, cyt. powyżej, § 29; oraz *Weber i Saravia*, cyt. powyżej, § 94).

231.  W swoim orzecznictwie na temat środków tajnego nadzoru Trybunał wskazał następujące minimalne gwarancje ochronne, które powinny zostać określone w prawie w celu uniknięcia nadużycia władzy: określenie natury przestępstw, których popełnienie może stanowić przesłankę do zarządzenia przechwytywania; zdefiniowanie kategorii osób podlegających podsłuchowi telefonicznemu; określenie limitu czasowego podsłuchu; ustanowienie procedury dla badania, wykorzystania, przechowywania uzyskanych danych; wprowadzenie środków ostrożności podczas komunikowania danych innym stronom; oraz określenie okoliczności, w których nagrania mogą lub muszą być usunięte lub zniszczone (zob. *Huvig*, cyt. powyżej, § 34; *Amann* *przeciwko Szwajcarii* [GC], nr 27798/95, §§ 56-58, ETPCz 2000‑II; *Valenzuela Contreras*, cyt. powyżej, § 46; *Prado Bugallo przeciwko Hiszpanii*,nr 58496/00, § 30, 18 lutego 2003; *Weber i Saravia*, cytowany powyżej, § 95; oraz *Association for European Integration and Human Rights and Ekimdzhiev,* cyt. powyżej, § 76).

232.  Co do pytania, czy ingerencja była “konieczna w demokratycznym społeczeństwie” do osiągnięcia celu prawnego, Trybunał uznał, że starając się znaleźć równowagę między interesem Państwa, jakim jest ochrona bezpieczeństwa narodowego poprzez środki tajnego nadzoru oraz istotność ingerencji w prawa skarżącego do jego prywatnego życia, władze państwowe mają pewien margines swobody w wyborze środków do osiągnięcia celu prawnego ochrony bezpieczeństwa narodowego. Jednakże margines ten jest przedmiotem nadzoru europejskiego obejmującego zarówno ustawodawstwo jak i decyzje wdrażające je w życie. Co się tyczy ryzyka, że system tajnego nadzoru ustanowiony w celu ochrony bezpieczeństwa narodowego może stanowić zagrożenia dla demokracji lub nawet ją zniweczyć pod pretekstem jej obrony, Trybunał musi zostać przekonany, że istnieją efektywne i adekwatne gwarancje przeciwko nadużyciom stosowania tego systemu. Ocena zależy od wszystkich warunków sprawy, takich jak natura, zakres i czas trwania możliwych środków, przyczyny ich zastosowania, władze właściwe do wydania zezwolenia do ich stosowania i nadzoru nad stosowaniem, a także środki odwoławcze przewidziane przez prawo krajowe. Trybunał musi określić, czy procedury dla nadzoru zarządzenia restrykcyjnych środków oraz ich implementacji są wystarczające, aby stwierdzić, że “ingerencja” była “konieczna w demokratycznym społeczeństwie” (zob. *Klass i Inni*, cyt. wyżej, §§ 49, 50 i 59; *Weber and Saravia*, cyt. wyżej, § 106; *Kvasnica v. Slovakia*, nr. 72094/01, § 80, 9 czerwca 2009; i *Kennedy*, cyt. powyżej, §§ 153 i 154).

233.  Kontrola i nadzór nad środkami tajnego nadzoru mogą zaistnieć w trzech etapach: kiedy zastosowanie tych środków zostało zarządzone, kiedy są one stosowane lub gdy zakończyło się ich stosowanie. Co do pierwszych dwóch etapów, sama natura i logika tajnego nadzoru dyktuje, że nie same środki tajnego nadzoru ale również towarzysząca im kontrola ich stosowania powinny być poprowadzone bez wiedzy danej osoby. W konsekwencji, jeżeli osoba zostanie pozbawiona możliwości skorzystania ze skutecznego środka odwoławczego z własnej inicjatywy lub wzięcia bezpośredniego udziału w procedurach kontrolnych, istotne jest, aby ustanowione procedury same w sobie dostarczały adekwatne i odpowiednie gwarancje bezpieczeństwa praw jednostki. W dodatku, wartości demokratycznego społeczeństwa muszą być respektowane tak wiernie jak to możliwe w procedurach nadzorczych, jeżeli chcemy, aby granice „konieczności” w znaczeniu Artykułu 8 § 2 nie były przekraczane. W przypadku gdy nadużycia są z łatwością możliwe do przewidzenia w indywidualnych sprawach i mogą mieć szkodliwe konsekwencje dla demokratycznego społeczeństwa jako całości, co do zasady pożądane jest powierzenie kontroli nadzorczej sędziemu, gdyż kontrola sędziowska stwarza najlepsze gwarancje niezależności, bezstronności i właściwego postępowania (zob. *Klass i Inni*, cyt. powyżej, §§ 55 i 56).

234.  Co do trzeciego etapu mającego miejsce po zakończeniu nadzoru, kwestia następczego powiadomienia o środkach nadzoru jest nierozerwalnie połączona z efektywnością środków odwoławczych przed sądami i w związku z tym istnieniem efektywnych gwarancji zabezpieczających przed nadużyciami organów stosujących środki nadzoru. W zasadzie jest niewielki zakres spraw, w których osoby zainteresowane mogą składać odwołanie do sądów, jeśli nie zostały one później powiadomione o powziętych bez ich wiedzy środkach nadzoru, co dałoby możliwość zakwestionowania ich legalności z mocą wsteczną (zob. *Klass and i Inni,* cy. powyżej, § 57, oraz *Weber i Saravia*, cyt. powyżej, § 135). [Taka kontrola sądowa jest także możliwa] jeżeli osoba, która podejrzewa, że jej komunikacje są lub były przechwytywane, tak więc jurysdykcja sądowa nie zależy od powiadomienia podmiotu przechwytywania, że nastąpiło przechwytywanie jego transmisji komunikacyjnej (zob. *Kennedy,* cyt. powyżej, § 167).

(ii)  Zastosowanie zasad ogólnych w niniejszej sprawie

235.  W odniesieniu do ogólnego zarzutu skarżącego na ustawodawstwo rosyjskie dotyczące niejawnego przechwytywania transmisji komunikacyjnej przez telefony komórkowe, Trybunał stwierdza, że nastąpiła ingerencja, o której mowa w Artykule 8 § 1. Zgodnie z tym, badając, czy ingerencja w prawo określone w Artykule 8 § 1 była uzasadniona, Trybunał musi sprawdzić, czy zakwestionowane przepisy same w sobie są zgodne z Konwencją.

 236.  W sprawach, w których przepisy zezwalające na tajny nadzór są kwestionowane przed Trybunałem, legalność ingerencji jest blisko związana z pytaniem, czy kryteria testu “konieczności” zostały spełnione i w związku z tym Trybunał winien łączne zbadać przestrzeganie wymogów “zgodności z prawem” i “konieczności” (zob. *Kennedy*, cyt., powyżej, § 155; zob. również *Kvasnica,* cyt. powyżej, § 84). Z zasadą „jakości prawa” związany jest nie tylko wymóg, aby prawo krajowe było dostępne i przewidywalne w swoim stosowaniu, ale wymagane jest także, aby prawo zapewniało, że środki tajnego nadzoru będą stosowane tylko wtedy, kiedy będzie to “konieczne w demokratycznym społeczeństwie”. [Wymaganie to powinno zostać spełnione] w szczególności przez zapewnienie adekwatnych i efektywnych zabezpieczeń oraz gwarancji chroniącymi przed nadużyciami.

237.  Nie ulega dyskusji pomiędzy stronami, że przechwytywanie komunikacji telefonicznej ma podstawy w prawie krajowym. Jest ono regulowane w szczególności przez KPK i OSAA, jak i Ustawę o Komunikacji oraz Rozporządzenia wydane przez Ministra Komunikacji. Co więcej, Trybunał uznaje za oczywiste, że środki nadzoru określone w prawie rosyjskim służą osiągnięciu celów prawnych w postaci ochrony bezpieczeństwa narodowego i publicznego, zapobieżenia zbrodni oraz ochrony gospodarczego dobrobytu państwowego (zob. par. 26 powyżej). W związku z tym, należy ustalić, czy prawo krajowe jest dostępne i zawiera adekwatne i efektywne zabezpieczenia i gwarancje, aby spełnić wymogi “przewidywalności” i “konieczności w demokratycznym społeczeństwie”.

238.  Trybunał w związku z tym oceni dostępność prawa krajowego, zakres i czas trwania środków tajnego nadzoru, procedury dla przechowywania, dostępu, badania, wykorzystania, komunikowania i niszczenia przechwyconych danych, procedury wydawania upoważnienia do przechwytywania komunikacji, ustalenia nadzoru implementacji środków tajnego nadzoru, mechanizmy powiadamiania i środki odwoławcze przewidziane przez prawo krajowe.

(α)  Dostępność prawa krajowego

239.  Strony nie kwestionują, że prawie wszystkie przepisy prawa dotyczące tajnego nadzoru – włączając KPK i OSAA, Ustawę o Komunikacji oraz większość Rozporządzeń wydanych przez Ministra Komunikacji – zostały oficjalnie opublikowane i są publicznie dostępne. Jednakże strony spierały się, czy załącznik do Rozporządzenia nr 70 Ministra Komunikacji spełnia wymóg dostępności.

240.  Trybunał zauważa, że załączniki do Rozporządzenia nr 70 nigdy nie zostały opublikowane w ogólnie dostępnej oficjalnej publikacji, ponieważ zostały uznane w swojej naturze na techniczne (zob. par. 128 powyżej).

241.  Trybunał przyznaje, że załączniki do Rozporządzenia nr 70 głównie opisują wymagania techniczne dla urządzeń przechwytywania, mających zostać zainstalowanymi przez dostawców usług komunikacyjnych. Jednocześnie, poprzez wymaganie, że powyższe urządzenia muszą zapewniać organom ścigania bezpośredni dostęp do wszystkich komunikacji przez telefony komórkowe wszystkich użytkowników oraz nie mogą zapisywać ani rejestrować informacji o przechwytywaniach podjętych przez organy ścigania (zob. par. 115 do 122 powyżej), załączniki do Rozporządzenia nr 70 wpływają na prawa użytkowników do poszanowania ich życia prywatnego i korespondencji. Trybunał w związku z powyższym uznaje, że muszą być dostępne publicznie.

 242.  Publikacja Rozporządzenia Ministra Komunikacji w oficjalnym magazynie *SvyazInform*,kolportowanym przez subskrypcję, powoduje, że jest ono dostępne tylko dla specjalistów komunikacji, nie dla ogółu obywateli. Równocześnie, Trybunał zauważa, że tekst Rozporządzenia z załącznikami, może być dostępny poprzez prywatnie zarządzaną prawną bazę danych, która odtwarza je z publikacji z *SvyazInform* (zob. par. 115 powyżej). Trybunał wyraża ubolewanie nad ogólnym brakiem dostępności oficjalnej publikacji Rozporządzenia nr 70. Jednakże, biorąc pod uwagę fakt, że zostało opublikowane w oficjalnym magazynie ministerstwa, a także, że ogół społeczeństwa może uzyskać dostęp poprzez internetową prawną bazę danych, Trybunał nie uważa, by konieczne było dalsze omawianie kwestii dostępności prawa krajowego. Zamiast tego skoncentruje się na wymogach “przewidywalności” i “konieczności”.

(β)  Zakres stosowania środków tajnego nadzoru

243.  Trybunał powtarza, że prawo krajowe musi zdefiniować zakres stosowania środków nadzoru poprzez wydanie obywatelom adekwatnych wskazówek co do okoliczności, w których władze publiczne są uprawnione do stosowania danych środków – w szczególności poprzez jasne określenie natury przestępstwa, które może dać podstawę do wydania decyzji o przechwytywaniu i poprzez zdefiniowanie kategorii osób podlegających podsłuchowi telefonicznemu (zob. par. 231 powyżej).

244.  Co do natury przestępstw, Trybunał podkreśla, że warunek “przewidywalności” nie wymaga od Państwa wyczerpującego nazwania przestępstw, których popełnienie może stanowić podstawę wydania decyzji upoważniającej do przechwytywania komunikacji. Jednakże, powinny zostać wskazane wystarczające szczegóły o naturze wspomnianych przestępstw (zob. *Kennedy*, cyt. powyżej, § 159). Zarówno OSAA jak i KPK stanowi, że komunikacje telefoniczne i inne mogą być przechwytywane w związku z przestępstwem średniej wagi, poważnym przestępstwem lub szczególnie poważnym przestępstwem – tj. przestępstwem, za które Kodeks Karny przewiduje maksymalną karę ponad trzech lat pozbawienia wolności, jeśli zostało popełnione, jest popełniane lub planowane (zob. par. 31 do 33 powyżej). Trybunał stwierdza, że natura przestępstw, które mogą stanowić podstawę do wydania decyzji o przechwytywaniu komunikacji jest wystarczająco jasna. Równocześnie zauważa z zaniepokojeniem, że prawo rosyjskie zezwala na tajne przechwytywanie transmisji komunikacyjnej w stosunku do bardzo szerokiego zakresu przestępstw, włączając na przykład, jak wskazał skarżący, kradzież kieszonkową (zob. par. 182 powyżej; zobacz również, dla porównania, *Iordachi i Inni*, cyt. powyżej, §§ 43 i 44).

245.  Trybunał dalej zauważa, że przechwytywanie komunikacji może zostać nakazane nie tylko w stosunku do podejrzanego lub oskarżonego, ale również w stosunku do osoby, która ma informacje o przestępstwie bądź inne informacje dotyczące danej sprawy karnej (zob. par. 32 powyżej). Trybunał wcześniej uznał, że środki przechwytywania w stosunku do osoby, która nie była podejrzana o popełnienie przestępstwa, ale mogła posiadać o nim informacje, mogły zostać uznane za uzasadnione w świetle wymogów Artykułu 8 Konwencji (zob. *Greuter,* cyt. powyżej). Jednocześnie Trybunał stwierdza brak jakichkolwiek wyjaśnień w ustawodawstwie rosyjskim lub ustanowionym orzecznictwie, w jaki sposób w praktyce należy rozumieć pojęcie “osoby, która może mieć informacje o przestępstwie” (zob., dla podobnych wyjaśnień, *Iordachi i Inni*, cyt. powyżej, § 44).

246.  Trybunał podnosi, że OSAA reguluje nie tylko przechwytywanie komunikacji dla celów zapobiegania lub wykrywania przestępstw, ale stanowi również, że komunikacje telefoniczne i inne mogą być przechwytywane w celu uzyskania informacji o zdarzeniach lub czynnościach zagrażających bezpieczeństwu narodowemu, militarnemu, gospodarczemu lub ekologicznemu Rosji (zob. par. 31 powyżej). Natomiast brak jest określenia w prawie rosyjskim, które to zdarzenia lub czynności mogą być uznane za zagrażające takim względom bezpieczeństwa.

247. Trybunał uznał wcześniej, że wymóg “przewidywalności” prawa nie zmierza tak daleko, by wymusić na Państwie wydanie przepisów prawnych wymieniających szczegółowo każde zachowanie, które może powodować wydanie decyzji o poddaniu osoby tajnemu nadzorowi ze względów “bezpieczeństwa narodowego”. Z natury rzeczy, zagrożenia dla bezpieczeństwa narodowego mogą różnić się w swoim charakterze i mogą być nieoczekiwane lub trudne do zdefiniowania zawczasu (zob. *Kennedy*, cyt. powyżej, § 159). Jednocześnie, Trybunał zaznaczył, że w kwestiach dotyczących praw fundamentalnych, sprzeczne z zasadą państwa prawa (filaru zapisanej w Konwencji zasady demokratycznego społeczeństwa) byłoby przyznanie organom władzy wykonawczej nieskrępowanej swobody decyzyjnej sprawach z zakresu bezpieczeństwa narodowego. W konsekwencji, prawo musi wskazywać granice każdej swobody decyzyjnej przyznanej właściwym władzom oraz sposób jej wykonywania z wystarczającą jasnością, mając na uwadze cel prawny wspomnianych środków, tak aby udzielić jednostkom adekwatną ochronę przed arbitralną ingerencją (zob. *Liu przeciko Rosji*, nr 42086/05, § 56, 6 grudnia 2007, z dalszymi odniesieniami).

248.  Znaczące jest, że OSAA nie zawiera żadnych wskazówek co do okoliczności, na podstawie których komunikacja może być przechwytywana ze względu na zdarzenia lub czynności zagrażające bezpieczeństwu narodowemu, militarnemu, gospodarczemu lub ekologicznemu Rosji. Poprzez to władze mają prawie nieograniczony stopień swobody decyzyjnej przy określaniu, które zdarzenia lub działania, stanowią takie zagrożenie, oraz czy zagrożenie to jest wystarczająco poważne, aby usprawiedliwiało tajny nadzór, tym samym tworząc możliwość dla nadużyć (zobacz, podobną argumentację, *Iordachi i Inni,* cyt. powyżej, § 46).

249.  Stwierdzając to, Trybunał nie traci wzglądu na fakt, że w Rosji wymagane jest uprzednie upoważnienie sądowe przechwytywania. Takie upoważnienie sądowe może wyznaczyć granice swobody decyzyjnej organów ścigania w interpretowaniu szerokiej definicji “osoby, która może mieć informację o przestępstwie”, “osoby, która może mieć informacje przydatne w sprawie karnej” oraz “zdarzeniach lub czynnościach zagrażających bezpieczeństwu narodowemu, militarnemu, gospodarczemu lub ekologicznemu Rosji” poprzez podążanie ustaloną interpretacją sądową definicji lub ustalonej praktyki weryfikującej, czy istnieją wystarczające powody do przechwytywania konkretnych komunikacji osoby w danej sprawie. Trybunał akceptuje, że wymaganie uprzedniego upoważnienia sądowego stanowi istotne zabezpieczenie przed arbitralnością. Efektywność tego zabezpieczenia zostanie zbadana poniżej.

(γ)  Czas trwania środków tajnego nadzoru

250.  Trybunał uznał, że nie jest nieuzasadnione, by przez cały czas trwania przechwytywania komunikacji właściwe władze krajowe, które mają kompetencje do wydawania i ponawiania nakazów przechwytywania dysponowały swobodą decyzyjną, pod warunkiem jednak istnienia adekwatnych zabezpieczeń, takie jakich jednoznaczne określenie w przepisach prawa krajowego okresu, po którym nakaz przechwytywania wygasa, warunków, na mocy których nakaz może być ponowiony oraz okoliczności, w których musi zostać uchylony (zob. *Kennedy*, cyt. powyżej, § 161; zobacz również *Klass i Inni*, cyt. powyżej, 52, oraz *Weber i Saravia*, cyt. powyżej, § 98).

251.  Co do pierwszej gwarancji, zarówno KPK i OSAA stanowią, że wydane przez sędziego upoważnienie do przechwytywania komunikacji nie może dotyczyć okresu przekraczającego sześć miesięcy (zob. par. 38 i 47 powyżej). Istnieje zatem jasne wskazanie w prawie krajowym co do długości okresu, po którym upoważnienie do przechwytywania komunikacji przestaje obowiązywać. Po drugie, warunki, na mocy których upoważnienie może być ponowione są również jasno określone w prawie. W szczególności, na mocy zarówno KPK, jak i OSAA sędzia może wydłużyć czas trwania przechwytywania komunikacji maksymalnie na okres sześciu miesięcy po aktualnym zbadaniu wszystkich właściwych materiałów (id.). Jednakże, co do trzeciej gwarancji dotyczącej warunków, na mocy których przechwytywanie musi zostać przerwane, Trybunał zauważa, że wymóg przerwania przechwytywania komunikacji, kiedy ustała taka konieczność jest wskazany wyłącznie w KPK. Niestety OSAA nie zawiera takiego wymagania (id.). W praktyce oznacza to, że przechwytywanie w ramach postępowania karnego jest wspierane przez większą ilość gwarancji zabezpieczających niż przechwytywanie prowadzone poza ramami takiego postępowania, w szczególności w związku ze “zdarzeniami lub czynnościami zagrażającymi bezpieczeństwu narodowemu, militarnemu, gospodarczemu lub ekologicznemu”.

252. Trybunał wnioskuje z powyższego, że podczas gdy przepisy prawa rosyjskiego zawierają jasne zasady co do określenia czasu trwania i ponowienia przechwytywania komunikacji, ustanawiając adekwatne gwarancje zabezpieczające przed nadużyciami, przepisy OSAA o przerwaniu środków nadzoru nie określają wystarczających gwarancji przeciwko arbitralnej ingerencji.

(δ)  Procedury przechowywania, dostępu, badania, wykorzystania, komunikowania oraz niszczenia przechwyconych danych

253.  Prawo rosyjskie przewiduje, że dane zebrane w wyniku stosowania środków tajnego nadzoru stanowią tajemnicę państwową i powinny zostać zabezpieczone i przechowywane na warunkach wyłączających jakiekolwiek ryzyko nieupoważnionego dostępu. Mogę zostać ujawnione tym urzędnikom państwowym, którzy rzeczywiście potrzebują danych do wykonywania swoich obowiązków oraz mają właściwy poziom poświadczenia bezpieczeństwa. Należy powziąć kroki, aby zapewnić, że ujawnione zostaną tylko te informacje, które są potrzebne odbiorcy do wykonywania jego obowiązków i nic ponadto. Urzędnicy odpowiedzialni za bezpieczne przechowywanie danych oraz nieudostępnianie osobom bez wymaganego poświadczenia bezpieczeństwa, zostali wskazani w niebudzący wątpliwości sposób (zob. par. 51 i 57 powyżej). Prawo krajowe również wyznacza warunki i sposób postępowania w przypadku udostępnienia prokuratorom przechwyconych danych zawierających informacje o przestępstwie. Opisuje, w szczególności, wymagania dla bezpiecznego składowania danych oraz warunki ich wykorzystania jako dowodu w sprawie karnej (zob. par. 58 do 64 powyżej). Trybunał jest usatysfakcjonowany, że prawo rosyjskie zawiera jasne zasady odnoszące się do przechowywania, wykorzystania i przekazywania przechwyconych danych, co zmniejsza ryzyko nieupoważnionego dostępu lub ujawnienia (zob. podobną argumentację w sprawie *Kennedy*, cyt. powyżej, §§ 62 i 63).

254.  Jeżeli chodzi o zniszczenie przechwyconych materiałów, prawo krajowe stanowi, że przechwycony materiał musi zostać zniszczony po sześciu miesiącach przechowywania, jeżeli osoba, której dotyczy, nie została oskarżona o popełnienie przestępstwa. Jeżeli osoba została oskarżona o popełnienie przestępstwa, sędzia musi podjąć decyzję na końcu postępowania karnego co do dalszego przechowywania oraz zniszczenia przechwyconego materiału wykorzystanego jako dowód (zob. par. 65 i 66 powyżej).

255.  Co do spraw, w których dana osoba nie została oskarżona o popełnienie przestępstwa, Trybunału nie przekonuje argumentacja skarżącego, że prawo rosyjskie zezwala na przechowywanie przechwyconych materiałów przez okres przekraczający ustawowy limit czasu (zob. par. 188 powyżej). Okazuje się, że przepisów, do których odwołuje się skarżący nie stosuje się do spraw dotyczących przechowywania danych zebranych w wyniku przechwytywania komunikacji. Trybunał uznaje sześciomiesięczny limit czasu przechowywania określony w prawie rosyjskim za rozsądny. Równocześnie, ubolewa nad brakiem wymogu natychmiastowego zniszczenia danych nieadekwatnych do celu, w jakim zostały uzyskane (porównaj *Klass i Inni*, cyt. powyżej, § 52, i *Kennedy*, cyt. powyżej, § 162). Automatyczne przechowywanie wyraźnie nieadekwatnych danych na okres sześciu miesięcy nie może zostać uznane za usprawiedliwione w świetle Artykułu 8.

256. Co więcej, co do spraw, w których dana osoba została oskarżona o popełnienie przestępstwa, Trybunał z niepokojem zauważa, że prawo rosyjskie zezwala na nieograniczoną swobodę decyzyjną sędziego przy decydowaniu o przechowywaniu lub niszczeniu danych wykorzystanych jako dowód po zakończeniu procesu (zob. par. 66 powyżej). Prawo rosyjskie nie daje obywatelom żadnych wskazówek co do okoliczności, w których przechwytywany materiał może być przechowywany po zakończeniu procesu. W związku z tym Trybunał uznaje, że prawo krajowe nie jest w tym punkcie wystarczająco jasne.

(ε)  upoważnienie do przechwytywania komunikacji

Procedury upoważnienia

257.  Trybunał weźmie pod uwagę szereg czynników przy ocenie, czy procedury upoważnienia są w stanie zapewnić, że tajny nadzór nie jest zlecany przypadkowo, nieregularnie oraz bez właściwej i odpowiedniej analizy. W szczególności należy zbadać, które organy są właściwe do wydania upoważnienia do prowadzenia nadzoru, jaki jest zakres kontroli prowadzonego nadzoru oraz jaka jest treść upoważnienia do przechwytywania komunikacji.

258.  Co do organów właściwych do wydania upoważnienia do prowadzenia nadzoru, wydanie upoważnienia do prowadzenia podsłuchu telefonicznego przez organ pozasądowy może być uznane za zgodne z Konwencją (zob. np. *Klass i Inni,* cyt. powyżej, § 51; *Weber i Saravia*, cyt. powyżej, § 115; oraz *Kennedy*, cyt. powyżej, § 31), pod warunkiem, że organ ten wykazuje się dostateczną niezależnością w stosunku do władzy wykonawczej (zob. *Dumitru Popescu przeciwko Rumunii (no. 2)*, nr 71525/01, § 71, 26 kwietnia2007).

259.  Prawo rosyjskie zawiera istotne zabezpieczenia przed arbitralnym lub niekontrolowanym tajnym nadzorem. Zgodnie z nim, na każde przechwytywanie komunikacji telefonicznej lub innej musi zostać wydana zgoda sądu (zob. 34 i 44 powyżej). Organy ścigania w celu uzyskania upoważnienia do przechwytywania komunikacji, składają uzasadniony wniosek w tym przedmiocie do sędziego, który może zażądać od organu przedstawienia materiałów na poparcie wniosku (zob. 37 i 46 powyżej). Sędzia musi podać powody wydania postanowienia upoważniającego do przechwytywania komunikacji (zob. par. 38 i 44 powyżej).

260.  Co się tyczy zakresu kontroli organów wydających upoważnienie [do przechwytywania komunikacji], Trybunał powtarza, że muszą być w stanie zweryfikować istnienie uzasadnianego podejrzenia przeciwko danej osobie, w szczególności, czy są faktycznie wskazania do podejrzewania osoby o planowanie, popełnianie lub popełnienie czynu zabronionego lub innych czynów (np. czynów zagrażających bezpieczeństwu narodowemu), które dają podstawę do zastosowania środków tajnego nadzoru. Należy również potwierdzić, czy wnioskowane przechwytywanie spełnia wymogi “konieczności w demokratycznym społeczeństwie”, o której mowa w Artykule 8 § 2 Konwencji, w tym także, czy jest ono proporcjonalne w stosunku do zakładanego celu, a więc należy zbadać, czy możliwe byłoby jego osiągnięcie poprzez mniej restrykcyjne środki (zob. *Klass i Inni,* cyt. powyżej, § 51; *Association for European Integration and Human Rights i Ekimdzhiev,* cyt. powyżej,§§ 79 i 80; *Iordachi i Inni*, cyt. powyżej, § 51; oraz *Kennedy,* cyt. powyżej, §§ 31 i 32).

261.  Trybunał zauważa, że nadzór sądowy w Rosji jest w swym zakresie ograniczony. Dlatego, materiały zawierające informacje o agentach działających pod przykryciem lub informatorach policyjnych lub o organizacji i metodzie stosowania środków operacyjno-rozpoznawczych, nie mogą być złożone sędziemu i w związku z tym są wyłączone z zakresu sądowej rewizji (zob. par. 37 powyżej). Trybunał stwierdza, że nieujawnianie odpowiednich informacji sądom, pozbawia je możliwości oceny, czy występuje wystarczająca faktyczna podstawa do podejrzewania osoby, wobec której wnoszono o podjęcie środków operacyjno-rozpoznawczych, o popełnienie przestępstwa lub czynności zagrażających bezpieczeństwu narodowemu, militarnemu, gospodarczemu lub ekologicznemu (zob., *mutatis mutandis*, *Liu,* cyt. powyżej, §§ 59-63). Trybunał uznał wcześniej, że istnieją techniki, które mogą być zastosowane, które odpowiadają na uzasadnione obawy odnoszące się do natury i źródeł służb wywiadowczych, a także przydzielają jednostce znaczący środek sprawiedliwości proceduralnej (zob. *mutatis mutandis*, *Chahal przeciwko Zjednoczonemu Królestwu*, 15 listopada1996, § 131, *Reports of Judgments and Decisions* 1996‑V).

262.  Co więcej Trybunał obserwuje, że w Rosji sędziowie nie są poinstruowani, ani przez KPK ani przez OSAA, o konieczności weryfikacji istnienia “uzasadnionego podejrzenia” przeciwko danym osobom lub o stosowaniu testu “konieczności” i “proporcjonalności”. Równocześnie, ETPCz zauważa, że Trybunał Konstytucyjny wyjaśnił w swoich decyzjach, że ciężar dowodu spoczywa na organie wnioskującym, który powinien wykazać, że przechwytywanie jest konieczne oraz, że sędzia badający wniosek o przechwytywanie powinien zweryfikować podstawy dla tych środków oraz przyznać upoważnienie wyłącznie wtedy, jeżeli organ ten przekona, że przechwytywanie byłoby zgodne z prawem, konieczne i usprawiedliwione. Trybunał Konstytucyjny utrzymał również, że decyzje sądowe upoważniające do przechwytywania komunikacji, powinny uwzględniać przyczyny oraz odnosić się do szczególnych przyczyn podejrzewania, że przestępstwo zostało popełnione, jest popełniane lub planowane lub, że trwają czynności zagrażające bezpieczeństwu narodowemu, militarnemu, gospodarczemu lub ekologicznemu, jak i osoba, wobec której wnoszono o przechwytywanie komunikacji jest zamieszana w te działania przestępcze lub w inny sposób niebezpieczne (zob. par. 40 i 42 powyżej). Trybunał Konstytucyjny w związku z tym rekomenduje, aby podczas badania wniosku o wydanie upoważnienia do przechwytywania komunikacji, sądy rosyjskie weryfikowały istnienie uzasadnionego podejrzenia przeciwko osobie, której dotyczy oraz wydawały upoważnienie wyłącznie wtedy, jeżeli spełniałoby ono warunki konieczności i proporcjonalności.

263.  Jednakże, Trybunał zauważa, że prawo krajowe nie wymaga jednoznacznie od sądów powszechnych stosowania się do tez opinii Trybunału Konstytucyjnego w zakresie sposobu, w jaki przepisy prawne powinny być interpretowane, jeżeli taka opinia została wyrażona w decyzji, a nie w wyroku (zob. par. 106 powyżej). W rzeczy samej, materiały przedłożone przez skarżącego pokazują, że sądy krajowe nie zawsze podążają za wyżej wspomnianymi rekomendacjami Trybunału Konstytucyjnego zawartymi w decyzjach, nie w wyrokach. Z opracowań wydanych przez sądy rejonowe wynika, że wnioski o przechwytywanie komunikacji z reguły nie są podpierane żadnymi materiałami, a sędziowie sądów rejonowych nigdy nie żądają od organów przechwytujących złożenia takich materiałów oraz, że zaledwie odniesienie do istnienia informacji o przestępstwie lub czynnościach zagrażających bezpieczeństwu narodowemu, militarnemu, gospodarczemu lub ekologicznemu bywa uznawane za wystarczające do udzielenia upoważnienia. Wniosek o upoważnienie zostaje odrzucony tylko wtedy, jeżeli nie jest podpisany przez właściwą osobę lub nie zawiera odniesienia do przestępstwa, w stosunku do którego przechwytywanie jest dozwolone na gruncie prawa krajowego (zob. par. 193 powyżej). Tym samym, opracowania sądów rejonowych rozpatrywane łącznie z informacją statystyczną z okresu od 2009 do 2013 dostarczoną przez skarżącego (zob. par. 194 powyżej) wskazują na to, że w codziennej praktyce sądy rosyjskie nie weryfikują, czy wystąpiło “uzasadnione podejrzenie” przeciwko danej osobie oraz nie stosują testu “konieczności” ani “proporcjonalności”.

264.  Wreszcie, co się tyczy treści upoważnienia do przechwytywania komunikacji, musi ono wyraźnie identyfikować konkretną osobę, która ma zostać poddana nadzorowi, lub miejsce, w którym nadzór byłby wykonywany. Identyfikacja taka może być sporządzona z wykorzystaniem imienia, adresu, numeru telefonu lub innymi odpowiednimi informacjami (zob. *Klass i Inni,* cyt. powyżej, § 51; *Liberty i Inni,* cyt. powyżej, §§ 64 i 65; *Dumitru Popescu (nr  2),* cyt. powyżej, § 78; *Association for European Integration and Human Rights i Ekimdzhiev,* cyt. powyżej,§ 80; oraz *Kennedy*, cyt. powyżej, § 160).

265.  Trybunał zauważa, że KPK wymaga, aby wniosek o upoważnienie do przechwytywania komunikacji jasno określał konkretną osobą, której komunikacje mają podlegać przechwytywaniu, jak i czas trwania przechwytywania (zob. par. 46 powyżej). Natomiast OSAA nie zawiera żadnych wymagań ani co do treści wniosku o przechwytywanie ani co do treści upoważnienia do przechwytywania komunikacji. W rezultacie, sądy czasami przyznają upoważnienie do przechwytywania komunikacji, w którym nie ma wskazania konkretnej osoby ani numeru telefonu, mającego być na podsłuchu, ale zezwalające na przechwytywanie wszystkich komunikacji telefonicznych na obszarze, gdzie doszło do popełnienia przestępstwa. Niektóre upoważnienia nie wspominają o czasie trwania upoważnienia do przechwytywania komunikacji (zob. par. 193 powyżej). Trybunał stwierdza, że takie upoważnienia, które nie są wyraźnie zakazane przez OSAA, przyznają bardzo szeroki zakres swobody decyzyjnej organom ścigania co do wyboru przechwytywanych komunikacji oraz czasu ich trwania.

266.  Trybunał dalej zauważa, że w pilnych sprawach możliwe jest przechwytywanie komunikacji przez maksymalnie 48 godzin bez uprzedniego upoważnienia sądowego. Sędzia musi zostać poinformowany o każdej takiej sprawie w ciągu dwudziestu czterech godzin od rozpoczęcia przechwytywania. Jeżeli upoważnienie sądowe nie zostanie wydane w ciągu czterdziestu ośmiu godzin, przechwytywanie musi zostać natychmiast zakończone (zob. par. 35 powyżej). Trybunał zbadał już “pilną” procedurę przewidzianą przez prawo bułgarskie i uznał, że jest zgodna z Konwencją (zob. *Association for European Integration and Human Rights i Ekimdzhiev*, cyt. powyżej, §§ 16 i 82). Jednakże, inaczej niż w przepisach bułgarskich, rosyjski “tryb pilny” nie przewiduje wystarczających gwarancji zabezpieczających, by zapewnić, że będzie się z niego korzystać w sposób oszczędny i tylko w uzasadnionych przypadkach. Tym samym, mimo, że w zakresie karnym OSAA ogranicza odwoływanie się do trybu pilnego w sprawach, gdzie istnieje nagłe zagrożenie, że popełniono poważne lub szczególnie poważne przestępstwo, to jednocześnie nie zawiera żadnych ograniczeń w sprawie tajnego nadzoru w związku z wydarzeniami lub czynnościami zagrażającymi bezpieczeństwu narodowemu, militarnemu, gospodarczemu lub ekologicznemu. Pozostawia władzom nieograniczony stopień swobody decyzyjnej przy określaniu, w których sytuacjach zastosowanie pozasądowego trybu pilnego jest usprawiedliwione, co stwarza pole do nadużyć (zob. dla porównania, *Association for European Integration and Human Rights and Ekimdzhiev*, cyt. powyżej, § 16). Co więcej, pomimo, że prawo rosyjskie wymaga natychmiastowego powiadomienia sędziego o każdym stadium pilnego przechwytywania komunikacji, jego kompetencje są ograniczone do wydawania zgody na przedłużenie środków przechwytywania powyżej czterdziestu ośmiu godzin. Sędzia nie ma możliwości oceny, czy użycie trybu pilnego było usprawiedliwione lub decydowania, czy materiał uzyskany podczas czterdziestu ośmiu godzin [niekontrolowanego nadzoru] powinien być zachowany lub zniszczony (zobacz, dla porównania, *Association for European Integration and Human Rights and Ekimdzhiev*, cyt. powyżej, § 16). Prawo rosyjskie w związku z tym nie przewiduje efektywnej rewizji sądowej trybu pilnego.

267.  Mając na uwadze powyższe rozważania, Trybunał stwierdza, że procedury upoważnienia stanowione przez prawo rosyjskie nie zabezpieczają przed przypadkowym, nieregularnym i niekontrolowanym zezwalaniem na środki tajnego nadzoru.

Dostęp władz do komunikacji

268.  Trybunał bierze pod uwagę argument skarżącego, że służby bezpieczeństwa dysponują środkami technicznymi do przechwytywania komunikacji telefonicznych bez uzyskania upoważnienia sądowego, ponieważ mają bezpośredni dostęp do wszystkich komunikacji oraz że ich zdolności do przechwytywania komunikacji poszczególnych osób nie są zależne od dostarczenia upoważnienia do przechwytywania dostawcy usług komunikacyjnych.

269.  Trybunał stwierdza, że wymaganie do okazania upoważnienia do przechwytywania komunikacji dostawcom usług komunikacyjnych przed uzyskaniem dostępu do komunikacji osoby jest jedną z ważniejszych gwarancji zabezpieczających przeciwko nadużyciom organów ścigania, zapewniając że właściwe upoważnienie zostanie uzyskane we wszystkich sprawach dotyczących przechwytywania. W Rosji organy ścigania nie muszą, na mocy prawa krajowego, przedstawiać dostawcom usług komunikacyjnych upoważnienia do przechwytywania, przed uzyskaniem dostępu do komunikacji danej osoby (zobacz, dla porównania, Rezolucję Rady UE cytowaną w paragrafie 145 powyżej), wyłączając sprawy pozostające w związku z monitorowaniem danych wynikających z komunikacji, na mocy KPK (zob. par. 48 powyżej). W rzeczy samej, zgodnie z Rozporządzeniami wydanymi przez Ministra Komunikacji, w szczególności załącznikami do Rozporządzenia nr 70, dostawcy usług komunikacyjnych muszą zainstalować urządzenie umożliwiające organom ścigania bezpośredni dostęp do wszystkich komunikacji telefonicznych wszystkich użytkowników (zob. par. 115 do 122 powyżej). Dostawcy usług komunikacyjnych mają również obowiązek na mocy Rozporządzenia nr 538 tworzenia baz danych przechowujących informacje o wszystkich użytkownikach, usługach, z których korzystają, na okres trzech lat; a służby specjalne mają bezpośredni zdalny dostęp do tych baz danych (zob. par. 132 i 133 powyżej). Organy ścigania mają zatem bezpośredni dostęp do wszystkich komunikacji telefonicznych oraz danych wynikających z komunikacji.

270.  Trybunał stwierdza, że sposób, w który system tajnego nadzoru funkcjonuje w Rosji, daje służbom bezpieczeństwa i policji środki techniczne do obchodzenia procedury uzyskania odpowiedniego upoważnienia, a tym samym do przechwytywania komunikacji bez uzyskiwania uprzedniego upoważnienia sądowego. Pomimo, że możliwość niewłaściwego działania przez nieuczciwego, skłonnego do zaniedbań i nadgorliwego urzędnika, nigdy nie może być całkowicie uregulowane w jakimkolwiek systemie (zob. *Klass i Inni*, cyt, powyżej, § 59), Trybunał uznaje, że system, taki jak rosyjski, który umożliwia tajnym służbom i policji bezpośrednie przechwytywanie transmisji komunikacyjnej wszystkich obywateli nie wymagając przedstawienia odpowiedniego upoważnienia do przechwytywania dostawcom usług komunikacyjnych lub komukolwiek innemu szczególnie sprzyja nadużyciom. Konieczność stworzenia gwarancji zabezpieczających przeciwko arbitralności i nadużyciu jest zatem szczególnie istotna.

271.  Trybunał zbada w związku z tym, ze szczególną uwagą, czy ustanowiony w prawie rosyjskim sposób kontroli implementacji środków tajnego nadzoru jest w stanie zapewnić, iż wszelkie przechwytywanie komunikacji będzie wykonywane w sposób zgodny z prawem na podstawie odpowiedniego upoważnienia sądowego.

(ζ)  Nadzór nad implementacją środków tajnego nadzoru

272.  Trybunał stwierdza, że Rozporządzenie nr 70 wymaga, aby urządzenie zainstalowane przez dostawców usług komunikacyjnych nie nagrywało ani nie zapisywało informacji o przechwytywaniu (zob. par. 120 powyżej). Trybunał uznał, że zobowiązanie organów przechwytujących do przechowywania nagrań z przechwytywania jest szczególnie istotne do zapewnienia, by organ dokonujący kontroli posiadał skuteczny dostęp do szczegółów podjętych czynności nadzoru (zob. *Kennedy*, cyt. powyżej, § 165). Zakaz zapisywania lub nagrywania przechwytywania określony w prawie rosyjskim uniemożliwia organom nadzorującym wykrycie przechwytywania komunikacji powziętego bez właściwego upoważnienia. Łącznie z możliwościami technicznymi organów ścigania, zgodnie z tym samym Rozporządzeniem 70, do bezpośredniego przechwytywania wszystkich komunikacji, przepis ten sprawia, że wszystkie ustalenia dotyczące nadzoru nie wykrywają bezprawnych przechwytywań, w związku z czym są nieefektywne.

273.  Co do nadzoru przechwytywania prowadzonego na podstawie właściwego upoważnienia sądowego, Trybunał zbada, czy zasady prowadzenia nadzoru istniejące w Rosji mogą zapewnić, że wymagania ustawowe dotyczące implementacji środków nadzoru, przechowywania, dostępu, wykorzystania, przetwarzania, komunikowania i niszczenia przechwyconego materiału będą respektowane.

274.  Sąd, który przyznał upoważnienie do przechwytywania komunikacji nie ma kompetencji do nadzoru jego implementacji. Nie jest informowany o rezultacie przechwytywania i nie ma możliwości sprawdzenia, czy wymagania określone w decyzji przyznającej upoważnienie zostały spełnione. Zresztą sądy rosyjskie w ogóle nie mają kompetencji do sprawowania pełnego nadzoru nad przechwytywaniem komunikacji. Nadzór sądowy jest ograniczony do etapu wstępnego upoważnienia. Następnie nadzorem zajmują się Prezydent, Parlament, Rząd, Prokurator Generalny i właściwi prokuratorzy niższego rzędu.

275. Trybunał uznał wcześniej, że chociaż w zasadzie pożądane jest powierzenie kontroli nadzorczej sędziemu, to kontrola dokonywana przez organy pozasądowe, może być uznana za zgodną z Konwencją, pod warunkiem, że organ sprawujący kontrolę jest niezależny od organów [dokonujących przechwytywania komunikacji] oraz dysponuje odpowiednią władzą i kompetencją do wykonywania efektywnej i stałej kontroli (zob. *Klass i Inni,* cyt. powyżej, § 56)*.*

276. Gdzie mowa o Prezydencie, Parlamencie i Rządzie, prawo rosyjskie nie wyznacza sposobu, w jaki mają nadzorować przechwytywanie komunikacji. Nie obowiązują żadne publicznie dostępne regulacje lub instrukcje opisujące zakres ich rewizji, warunki, na mocy których może być podjęta, procedury rewizji środków nadzoru lub zadośćuczynienia w przypadku wykrycia naruszenia (zob. dla podobnego wnioskowania, *Association for European Integration and Human Rights and Ekimdzhiev*, cyt. powyżej, § 88).

277.  Co do nadzoru sprawowanego przez prokuratorów, Trybunał podnosi, że prawo krajowe wyznacza zakres i procedury nadzoru prokuratorskiego nad czynnościami operacyjno-rozpoznawczymi (zob. par. 69 do 80 powyżej). Stanowi, że prokuratorzy mogą podjąć inspekcje rutynowe i *ad hoc* organów wykonujących czynności operacyjno-rozpoznawcze oraz są uprawnieni do zbadania właściwych dokumentów, włączając te poufne. Mogą podjąć środki do zatrzymania lub zadośćuczynienia wykrytym naruszeniom prawa oraz, aby pociągnąć do odpowiedzialności winną osobę. Muszą składać półroczne raporty o rezultatach swoich inspekcji do Biura Prokuratora Generalnego. Trybunał przyjmuje, że ramy prawne przewidują, przynajmniej teoretycznie istnienie kontroli prokuratora nad wykonywaniem środków tajnego nadzoru. Należy zatem zbadać, czy prokuratorzy są niezależni od władz wykonujących nadzór i czy przydzielono im wystarczającą władzę i kompetencje do sprawowania efektywnej i stałej kontroli.

278. Co do wymogu niezależności, w poprzedniej sprawie Trybunał wziął pod uwagę sposób mianowania i status prawny członków organu sprawującego nadzór. W szczególności uznał za wystarczająco niezależne organy składające się z członków parlamentu (wywodzących się zarówno z większości jak i opozycji) lub z osób wykwalifikowanych do pełnienia funkcji sądowych, mianowanych zarówno przez parlament lub przez Prezesa Rady Ministrów (zob. na przykład, *Klass i Inni*, cyt. powyżej, §§ 21 i 56; *Weber i Saravia*, cyt. powyżej, §§ 24, 25 i 117; *Leander*, cyt. powyżej, § 65; (zob. *L. przeciwko Norwegii*, nr 13564/88, decyzja Komisji z dnia 8 czerwca 1990); oraz *Kennedy*, cyt. powyżej, §§ 57 i 166). Jednakże, Minister Spraw Wewnętrznych – który jest nie tylko osobą z nominacji politycznej, ale i członkiem władzy wykonawczej, bezpośrednio zaangażowanym we wdrażanie szczególnych środków nadzoru – został uznany za niewystarczająco niezależnego (zob. *Association for European Integration and Human Rights and Ekimdzhiev,* cyt. powyżej, §§ 85 i 87). Podobnie, Prokurator Generalny i kompetentni prokuratorzy niższego rzędu zostali uznani za niewystarczająco niezależnych (zob. *Iordachi i Inni,* cyt. powyżej, § 47).

279.  W przeciwieństwie do organów nadzorczych wymienionych powyżej, w Rosji prokuratorzy są mianowani i odwoływani przez Prokuratora Generalnego po konsultacji z regionalnymi władzami wykonawczymi (zob. par. 70 powyżej). Ten fakt może wzbudzić wątpliwości co do ich niezależności od władzy wykonawczej.

280.  Co więcej, istotne jest, aby każde funkcja, której podejmują się prokuratorzy w ramach systemu ochrony praw człowieka, nie stwarzała żadnego konfliktu interesów (zob. *Menchinskaya przeciwko Rosji*, nr 42454/02, §§ 19 i 38, 15 stycznia 2009). Trybunał stwierdza, że biura prokuratorskie nie specjalizują się w nadzorowaniu przechwytywania komunikacji (zob. par. 71 powyżej). Taki nadzór stanowi tylko jedną część ich szerokich i zróżnicowanych zadań, do których należą: oskarżanie o popełnienie przestępstwa oraz nadzór nad śledztwem. W ramach ich funkcji prokuratorskich, prokuratorzy wydają zezwolenia na wnioski o przechwytywanie składane przez śledczych w ramach postępowań karnych (zob. par. 44 powyżej). To połączenie funkcji w ramach jednego biura prokuratorskiego, a także fakt, że to samo biuro wydaje zezwolenia w odpowiedzi na wnioski o przechwytywanie komunikacji, a następnie nadzoruje [sposób w jaki odpowiednie organy korzystają z wydanego zezwolenia], również budzi wątpliwości co do niezależności prokuratorów (zob., dla porównania, *Ananyev i Inni przeciwko Rosji*, nr 42525/07 i 60800/08, § 215, 10 stycznia 2012, dotyczące nadzoru przez prokuratorów jednostek penitencjarnych, gdzie uznano, że prokuratorzy spełniali wymóg niezależności względem organów systemu penitencjarnego).

281.  Jeśli chodzi o władzę i kompetencje prokuratorów, Trybunał zauważa, że istotne jest, aby organ nadzorczy miał dostęp do wszystkich właściwych dokumentów, włączając w to materiały zamknięte, a także istotne jest, aby wszystkie osoby zaangażowane w prowadzenie czynności polegających na przechwytywaniu komunikacji wykonywały obowiązek ujawnienia prokuratorowi każdego wymaganego materiału (zob. *Kennedy*, cyt. powyżej, §  166). Prawo rosyjskie stanowi, że prokuratorzy są uprawnieni do badania właściwych materiałów, także tych poufnych. Ważne jest również, by zauważyć, że informacje o służbach bezpieczeństwa, agentach działających pod przykryciem oraz o taktyce, metodach i środkach przez nich używanych, pozostawały poza zakresem prokuratorskiej kontroli (zob. par. 74 powyżej). Zakres tej kontroli jest w związku z tym ograniczony. Co więcej, przechwytywanie wykonywane przez FSB w zakresie kontrwywiadu, może podlegać kontroli jedynie w następstwie złożenia skargi indywidualnej (zob. par. 76 powyżej). Ponieważ jednostki nie są informowane o przechwytywaniu komunikacji (zob. par. 81 powyżej i par. 289 poniżej), jest wysoce nieprawdopodobne, że taka skarga zostanie złożona. W rezultacie, środki nadzoru związane z kontrwywiadem *de facto* nie podlegają prokuratorskiej kontroli.

282.  Możliwości działania organu nadzorczego w przypadku wykrytych naruszeń stanowią również istotny element w ocenie efektywności tego nadzoru (zob. na przykład, *Klass and Others*, cyt. powyżej, § 53, gdzie organ dokonujący przechwytywania komunikacji musiał natychmiast zakończyć przechwytywanie, jeżeli Komisja G10 uznała je za nielegalne lub niepotrzebne; i *Kennedy*, cyt. powyżej, § 168, gdzie każdy materiał z przechwytywania miał zostać zniszczony tak szybko jak możliwie, gdy Komisarz Komunikacji uznał, że przechwytywanie było bezprawne). Trybunał uznaje za słuszne, że prokuratorzy mają pewną władzę w stosunku do wykrytych przez nich naruszeń. Mogą zatem podjąć środki, aby zaprzestać dokonywania wykrytych naruszeń prawa lub im zadośćuczynić, oraz pociągnąć właściwe osoby do odpowiedzialności (zob. par. 79 powyżej). Jednakże nie występują szczególne przepisy wymagające zniszczenia bezprawnie uzyskanych materiałów z przechwytywania (zob. *Kennedy*, cyt. powyżej, § 168).

283.  Trybunał musi również zbadać, czy czynności organu nadzoru są poddane publicznej kontroli (zob. na przykład, *L. przeciwko Norwegii*, cyt. powyżej, gdzie nadzór był wykonany przez Komitet Kontroli, który zdaje coroczny raport przed Rządem, który jest publikowany i dyskutowany przez Parlament; *Kennedy*, cyt. powyżej, § 166, gdzie nadzór przechwytywania były sprawowany przez Komisarza Komunikacji, który składa coroczne raporty przed Prezesem Rady Ministrów, które są publicznym dokumentem przedkładanym parlamentowi; oraz, dla porównania, *Association for European Integration and Human Rights and Ekimdzhiev,* cyt. powyżej, § 88, gdzie Trybunał uznał wadliwość systemu, w którym ani Minister Spraw Wewnętrznych ani żaden inny urzędnik nie musiał regularnie składać raportów przed niezależnym organem lub do wiadomości publicznej o całości dokonywanej operacji ani o środkach zastosowanych w poszczególnych sprawach). W Rosji prokuratorzy muszą składać półroczne raporty omawiające wyniki śledztwa przed Biurem Prokuratora Generalnego. Jednakże, raporty te wskazują wszystkie typy środków operacyjno-rozpoznawczych, zebrane łącznie, bez osobnego wyszczególnienia przechwytywania komunikacji. Co więcej, raporty zawierają jedynie informacje statystyczne o ilości podjętych środków operacyjno-rozpoznawczych oraz o ilości wykrytych naruszeń, bez określania natury naruszeń lub środków powziętych w celu zadośćuczynienia. Istotne jest, że raporty te stanowią dokumenty poufne. Nie są publikowane lub w inny sposób dostępne publicznie (zob. par. 80 powyżej). To wskazuje, że w Rosji nadzór sprawowany przez prokuratorów jest prowadzony w sposób, o którym nie można uzyskać wiedzy i który jest możliwy do skontrolowania.

284.  Ostatecznie, Trybunał zauważa, że Rząd powinien wskazać odpowiednie przykłady ilustrujące praktyczną skuteczność zasad prowadzonego nadzoru, (zob. *mutatis mutandis*, *Ananyev i Inni*, cyt. powyżej, §§ 109 i 110). Jednakże, Rząd rosyjski nie przedłożył żadnych raportów z inspekcji ani decyzji prokuratorów o powzięciu środków służących zaprzestaniu wykrytym naruszeniom prawa lub służących zadośćuczynieniu. To wskazuje, że Rząd nie przedstawił, że kontrola prokuratorów nad środkami tajnego nadzoru jest w praktyce skuteczna. Trybunał również zwraca na uwagę na złożone przez skarżącego dokumenty ukazujące niemożność uzyskania przez prokuratorów dostępu do sklasyfikowanych materiałów dotyczących przechwytywania komunikacji (zob. par. 14 powyżej). Ten przykład również budzi wątpliwości co do efektywności nadzoru prokuratorów w praktyce.

285.  Mając na uwadze powyżej zidentyfikowane defekty oraz szczególną wagę [skutecznej] kontroli w systemie, gdzie organy ścigania mają bezpośredni dostęp do wszystkich komunikacji, Trybunał stwierdza, że nadzór prokuratorów nad przechwytywaniem komunikacji obecnie nie jest w stanie zapewnić adekwatnych i efektywnych gwarancji zabezpieczeń przez nadużyciami.

(η)  Informowanie o przechwytywaniu komunikacji i dostępnych środkach odwoławczych

286.  Trybunał rozpozna teraz kwestię informowania o przechwytywaniu komunikacji, która jest nieodłącznie związana ze skutecznością sądowych środków odwoławczych (zob. orzecznictwo cytowane w paragrafie 234 powyżej).

287.  W praktyce, wymóg informowania może nie być wykonalny w każdej sprawie. Czynność lub zagrożenie, przeciwko którym kierowane są konkretne środki nadzoru, mogą trwać latami, nawet dekadami po zawieszeniu tych środków. Informowanie każdej osoby dotkniętej zawieszonym środkiem, może narazić na szwank długotrwały cel, który oryginalnie przyświecał nadzorowi. Co więcej, informowanie to może skutkować wyjawieniem metod pracy i pól operacji służb wywiadowczych oraz identyfikować ich agentów. Stąd, fakt, że osoby, których dotyczą środki tajnego nadzoru nie są informowane od razy po zaprzestaniu przechwytywania, nie może sam w sobie być podstawą do przyjęcia wniosku, że ingerencja nie była “konieczna w demokratycznym społeczeństwie”, ponieważ brak wiedzy o stosowanych środkach tajnego nadzoru, zapewnia skuteczność przechwytywania komunikacji. Jak tylko po zakończeniu stosowania środków tajnego nadzoru zaistnieje możliwość poinformowania objętej nimi osoby w sposób niestwarzający zagrożenia dla celu wprowadzonego ograniczenia [prawa do prywatności], odpowiednie informacje powinny zostać jej przekazane (zob. *Klass i Inni,* cyt. powyżej, § 58, oraz *Weber i Saravia*, cyt. powyżej, § 135). Trybunał również bierze pod uwagę Rekomendację Komitetu Ministrów regulującą wykorzystanie danych osobowych w sektorze policji, która stanowi, że jeżeli działania policji nie są już prowadzone, konkretne osoby, gdy tylko jest to wykonalne, powinny być informowane o tym, że policja przechowuje o nich informacje, ilekroć dane dotyczące jednostek zostały zebrane i przechowywane bez ich wiedzy i jeżeli nie zostały usunięte (§2.2, zob. par. 143 powyżej).

288.  W sprawach *Klass i Inni* oraz *Weber i Saravia,* Trybunał zbadał przepisy niemieckie, które stanowią, że informacja o nadzorze powinna być udzielona, gdy tylko zostanie on zakończony, jeśli nie będzie zagrożony jego cel. Trybunał wziął pod uwagę, że był to niezależny organ, Komisja G10, która miała władzę o decydowaniu, czy osoba podlegająca monitorowaniu powinna być poinformowana o środkach nadzoru. Trybunał uznał, że przepis o którym mowa, zapewniał skuteczność mechanizmu informowania, który wpływał na utrzymywanie ingerencji w tajemnicy w limitach czasowych niezbędnych do osiągnięcia powziętych celów prawnych (zob. *Klass i Inni,* cyt. powyżej, § 58, oraz *Weber i Saravia*, cyt. powyżej, § 136). W sprawach *Association for European Integration and Human Rights and Ekimdzhiev* oraz *Dumitru Popescu (nr 2),* Trybunał uznał, że brak wymogu informowania podmiotu przechwytywania komunikacji w dowolnym czasie był niezgodny z Konwencją, w ten sposób, że pozbawiał podmiot przechwytywania jakiejkolwiek okazji do wnoszenia o zadośćuczynienie za bezprawną ingerencję w jego prawa na mocy Artykułu 8 oraz sprawiał, że środki odwoławcze dostępne w prawie krajowym, były jedynie teoretyczne i iluzoryczne, a nie praktyczne i skuteczne. Prawo krajowe nie stworzyło zatem prawdziwej gwarancji zabezpieczającej przed niewłaściwym stosowaniem szczególnych środków nadzoru (zob. *Association for European Integration and Human Rights and Ekimdzhiev*, cyt. powyżej, §§ 90 i 91, oraz *Dumitru Popescu (nr 2),* cyt. powyżej, § 77). Dla porównania, w sprawie *Kennedy* niewprowadzenie wymogu informowania podmiotu przechwytywania w jakimkolwiek momencie, było zgodne z Konwencją, ponieważ w Zjednoczonym Królestwie każda osoba, która podejrzewała, że jej komunikacja była przechwytywana, mogła zwrócić się do Trybunału do spraw Środków Śledczych (Investigatory Powers Tribunal), którego jurysdykcja nie zależała od powiadomienia podmiotu przechwytywania o przechwytywaniu jego komunikacji (zob. *Kennedy,* cyt. powyżej, § 167).

289.  Jeśli zaś chodzi o okoliczności niniejszej sprawy, to Trybunał podnosi, że w Rosji osoby, których komunikacje były przechwytywane, nie są o tym fakcie informowane w żadnym czasie ani w żadnych okolicznościach. To wskazuje, że jeżeli postępowanie karne zostało wszczęte przeciwko podmiotowi przechwytywania i dane przechwycone zostały wykorzystane jako dowód, lub jeżeli nastąpił przeciek, to osoba zainteresowana raczej nigdy nie dowie się o przechwytywaniu swojej komunikacji.

290.  Trybunał bierze pod uwagę fakt, że osoba, która w jakiś sposób dowiedziała się o przechwytywaniu swojej komunikacji, może żądać informacji na temat odpowiednich danych (zob. par. 81 powyżej). Warto wspomnieć w związku z tym, że w celu uzyskania uprawnienia do złożenia takiego żądania, osoba musi być w posiadaniu faktów o środkach operacyjno-rozpoznawczych, którym została poddana. To wskazuje, że dostęp do informacji jest warunkowany możliwością danej osoby do udowodnienia przechwytywania jej komunikacji. Co więcej, podmiot przechwytywania nie jest uprawniony do uzyskania dostępu do dokumentów dotyczących przechwytywania jej komunikacji; jest on w najlepszym wypadku uprawniony do otrzymania “informacji” o zebranych danych. Taka informacja jest dostarczana tylko w bardzo nielicznych przypadkach, mianowicie, jeżeli wina osoby nie została udowodniona zgodnie z procedurami przewidzianymi przez prawo, tj. gdy nie została ona oskarżona, lub zarzuty zostały oddalone w związku z udowodnieniem, że rzekome przestępstwo nie zostało popełnione lub gdy nie zostały spełnione znamiona przestępstwa. Jest również znaczące, że tylko informacja, która nie zawiera tajemnicy państwowej, może być ujawniona podmiotowi przechwytywania oraz, że na mocy prawa rosyjskiego informacje o urządzeniach użytych podczas czynności operacyjno-rozpoznawczych, stosowanych metodach, zaangażowanych funkcjonariuszach, oraz zebranych danych stanowią tajemnicę państwową (zob. par. 52 powyżej). Mając na uwadze powyższe cechy rosyjskiego prawa możliwość uzyskania informacji o przechwytywaniu komunikacji wydaje się być nieefektywna.

291.  Trybunał będzie miał na uwadze wyżej wymienione czynniki – brak powiadomienia i brak skutecznej możliwości wnioskowania o uzyskanie informacji o przechwytywaniu komunikacji od władz – podczas oceny skuteczności środków odwoławczych dostępnych w prawie rosyjskim.

292.  Prawo rosyjskie stanowi, że osoba twierdząca, że jej prawa zostały lub są naruszone przez władze państwowe wykonujące czynności operacyjno-rozpoznawcze może złożyć skargę do kierownika danego organu, prokuratora lub do sądu (zob. par. 83 powyżej). Trybunał przypomina, że odwołanie do bezpośredniego przełożonego organu, którego czynności są zakwestionowane, nie spełnia wymaganych standardów niezależności stanowiących wystarczającą ochronę przed nadużyciami władzy (zob., dla porównania, *Khan przeciwko Zjednoczonemu Królestwu*, nr 35394/97, §§ 45-47, ETPCz 2000‑V; *Dumitru Popescu (nr 2),* cyt. powyżej, § 72; oraz *Avanesyan,* cyt. powyżej, § 32). Prokuratorzy również nie posiadają niezależności oraz mają ograniczony zakres rewizji, jak wykazano powyżej (zob. par. 277 do 285 powyżej). Pozostaje więc kwestia do rozważenia, czy skarga do sądu może być postrzegana jako efektywny środek odwoławczy.

293.  Występują cztery procedury prawne, które, zgodnie z twierdzeniem Rządu, mogą być wykorzystane przez osobę chcącą złożyć skargę na przechwytywanie jej transmisji komunikacyjnej: apelacja, kasacja, wniosek o rewizję nadzorczą postanowienia sądu upoważniającego do przechwytywania komunikacji, kontrola sądowa w następstwie skargi złożonej na podstawie Artykułu 125 KPK; kontrola sądowa w następstwie skargi na podstawie Ustawy o Rewizji Sądowej i Rozdziału 25 Kodeksu Postępowania Cywilnego; powództwo cywilne na podstawie Artykułu 1069 Kodeksu Cywilnego. Trybunał przeanalizuje je po kolei.

294.  Pierwsza procedura przywołana przez Rząd to apelacja, kasacja lub wniosek o rewizję nadzorczą postanowienia sądu upoważniającego do przechwytywania komunikacji. Jednakże Trybunał Konstytucyjny jasno stwierdził, że podmiot przechwytywania nie miał prawa odwołania od orzeczenia sądowego upoważniającego do przechwytywania jego komunikacji (zob. par. 40 powyżej; zob. również *Avanesyan*, cyt. powyżej, § 30). Prawo krajowe milczy co do możliwości złożenia kasacji. Mając na uwadze, że Rząd nie przedstawił żadnych przykładów rozpatrywania kasacji w tego rodzaju sprawach, Trybunał ma poważne wątpliwości co do istnienia prawa do złożenia kasacji na postanowienie sądowe upoważniające do przechwytywania komunikacji. Jednocześnie, osoba, której komunikacja podlega przechwytywaniu jest wyraźnie upoważniona do złożenia wniosku o rewizję nadzorczą (zob. par. 43 powyżej). Jednakże, w celu złożenia wniosku o rewizję nadzorczą na postanowienie sądowe upoważniające do przechwytywania komunikacji, osoba, której ono dotyczy musi być świadoma, że takie postanowienie zostało wydane. Chociaż Trybunał Konstytucyjny utrzymał, że nie jest konieczne załączanie kopii zakwestionowanego orzeczenia sądowego do wniosku o rewizję nadzorczą (ibid.), ciężko jest wyobrazić sobie, jak osoba może złożyć taki wniosek bez posiadania chociażby minimum informacji o orzeczeniu, które kwestionuje (takich jak data wydania oraz dane sądu, [który je wydał]). W przypadku braku powiadomienia o środkach nadzoru na mocy prawa rosyjskiego, dana osoba praktycznie nie ma możliwości uzyskania informacji, chyba że miałaby ona zostać ujawniona w kontekście postępowania karnego przeciwko niej lub jeżeli nastąpiła pewna niedyskrecja, w wyniku czego doszłoby do ujawnienia informacji.

295.  Jeśli chodzi o skargę na mocy Artykułu 125 KPK, to może być ona złożona tylko przez uczestnika postępowania karnego podczas trwania śledztwa (zob. par. 88 i 89 powyżej). Ten środek odwoławczy jest w związku z tym dostępny wyłącznie dla osób, które dowiedziały się o przechwytywaniu ich komunikacji w ramach prowadzonego przeciwko nim postępowania karnego. Nie może być wykorzystany przez osobę, przeciwko której nie wszczęto żadnego postępowania w wyniku przechwytywania jej komunikacji oraz która nie wie, czy jej komunikacja była przechwytywana. Warto również wspomnieć, że Rząd nie przedłożył żadnych orzeczeń sądowych rozpoznających skargę na mocy Artykułu 125 KPK o przechwytywaniu komunikacji. W związku z tym nie przywołano przykładów z orzecznictwa sądów krajowych, które wskazywałyby na praktyczną skuteczność przywołanego środka odwoławczego. (zob. dla porównania, *Rotaru*, cyt. powyżej, § 70, i *Ananyev i Inni,* cyt. powyżej, §§ 109 i 110).

296.  Co do wniosku o rewizję sądową na mocy Ustawy o Rewizji Sądowej, Rozdziału 25 Kodeksu Postępowania Cywilnego oraz nowego Kodeksu Postępowania Administracyjnego oraz co do skargi cywilnej składanej na podstawie Artykułu 1069 Kodeksu Cywilnego, ciężar dowodu spoczywa na powodzie, który musi wykazać, że przechwytywanie miało miejsce, a w związku z tym jego prawo zostało naruszone (zob. par. 85, 95, 96 i 105 powyżej). Przy braku powiadomienia lub innej formy dostępu do oficjalnych dokumentów, praktycznie niemożliwe jest udowodnienie wymaganych okoliczności. W rzeczy samej, skarga skarżącego została odrzucona przez sądy krajowe ze względu na brak dowodów, że jego komunikacje telefoniczne były przechwytywane (zob. par. 11 i 13 powyżej). Trybunał zauważa, że Rząd przedstawił kilka orzeczeń sądowych wydanych na mocy Rozdziału 25 Kodeksu Postępowania Cywilnego lub Artykułu 1069 Kodeksu Cywilnego (zob. par. 220 do 223 powyżej). Jednakże, wszystkie te orzeczenia, z jednym wyjątkiem, dotyczą przeszukań lub zajęć dokumentów lub rzeczy, tj. środków operacyjno-rozpoznawczych powziętych za wiedzą osoby, której dotyczą. W takich sprawach, podmiot przechwytywania miał możliwość spełnienia ciążącego na nim obowiązku udowodnienia odpowiednich okoliczności, ponieważ wiedział o przechwytywaniu swoich komunikacji w toku postępowania karnego przeciwko niemu.

297. Następnie Trybunał bierze pod uwagę argument Rządu, że prawo rosyjskie przewiduje środki odwoławcze i zadośćuczynienie w przypadku nadużycia władzy, zbierania lub rozpowszechniania danych o życiu prywatnym i rodzinnym danej osoby bez upoważnienia, a także naruszenia prawa obywatela do prywatności komunikacji. Ze względu na powody wykazane w poprzedzających paragrafach, te środki odwoławcze są również dostępne dla osób, które mogą przedstawić organom ścigania co najmniej niektóre faktyczne informacje o przechwytywaniu ich komunikacji (zob. par. 24 powyżej).

298.  Trybunał wnioskuje z powyższego, że środki odwoławcze, na które powołuje się Rząd, są dostępne wyłącznie dla osób, które są w posiadaniu informacji o przechwytywaniu ich komunikacji. Ich skuteczność jest w związku z tym osłabiona przez brak sformułowania wymagania powiadomienia osoby, której komunikacja jest przechwytywana oraz poprzez brak innej adekwatnej możliwości wnioskowania o uzyskanie informacji o przechwytywaniu od władz. Zgodnie z tym, Trybunał podnosi, że prawo rosyjskie nie przewiduje skutecznych środków odwoławczych przeciwko tajnemu nadzorowi w sprawach, w których nie wszczęto postępowania karnego przeciwko podmiotowi przechwytywania. Nie jest zadaniem Trybunału w niniejszej sprawie decydować, czy te środki odwoławcze będą skuteczne w sprawach, w których osoba dowiaduje się o przechwytywaniu swoich komunikacji w toku postępowania karnego przeciwko niej (zob. jednakże *Avanesyan*, cyt. powyżej, gdzie uznano niektóre ze środków odwoławczych za nieefektywne do zaskarżenia “inspekcji” w mieszkaniu skarżącego).

299. Ostatecznie, co do środków odwoławczych mających zakwestionować rzekomą nieskuteczność gwarancji przeciwko nadużyciom w prawie rosyjskim przez sądami rosyjskimi,  Trybunału nie przekonują argumenty Rządu, że takie środki odwoławcze są efektywne (zob. par. 156 i 225 powyżej). Co do możliwości zakwestionowania OSAA przed Trybunałem Konstytucyjnym, Trybunał zauważył, że Trybunał Konstytucyjny zbadał konstytucyjność OSAA przy wielu okazjach i uznał, że była zgodna z Konstytucją (zob. par. 40 do 43, 50, 82 i 85 do 87 powyżej). W tych okolicznościach Trybunał uznaje za mało prawdopodobne, aby skarga skarżącego do Trybunału Konstytucyjnego, poruszająca te same kwestie, które zostały już przezeń zbadane, miała jakiekolwiek szanse na powodzenie. Trybunał nie jest również przekonany, że kwestionowanie Rozporządzenia nr 70 przez Sądem Najwyższym lub sądami niższej instancji stanowiłoby skuteczny środek odwoławczy. W rzeczy samej, skarżący zakwestionował Rozporządzenie nr 70 w postępowaniu krajowym. Jednakże, zarówno sądy rejonowe jak i okręgowe uznały, że skarżący nie miał podstaw do kwestionowania Rozporządzenia, ponieważ zainstalowane urządzenia zgodnie z tym rozporządzeniem same w sobie nie stanowiły ingerencji w prywatność jego komunikacji (zob. par. 10, 11 i 13 powyżej). Jest również znaczące, że Sąd Najwyższy uznał, że Rozporządzenie nr 70 było bardzie techniczne niż prawne w swej naturze (zob. par. 128 powyżej).

300.  Mając na uwadze powyższe rozważania, Trybunał uznaje, że prawo rosyjskie nie przewiduje skutecznych środków odwoławczych dla osoby, która podejrzewa, że została poddana tajnemu nadzorowi. Poprzez pozbawianie podmiotu przechwytywania efektywnych możliwości zakwestionowania przechwytywania w sposób wsteczny, tym samym prawo rosyjskie nie tworzy istotnych gwarancji zabezpieczających przed niewłaściwym wykorzystaniem środków tajnego nadzoru.

301.  Z powyższych przyczyn, Trybunał oddala również zarzut Rządu co do niewyczerpania krajowych środków odwoławczych.

(θ)  Wnioski

302.  Trybunał wnioskuje, że przepisy prawne w Rosji regulujące przechwytywanie transmisji komunikacyjnej nie przewidują adekwatnych i skutecznych gwarancji przeciwko ryzyku wystąpienia nadużyć, które jest nieodłączne w każdym systemie inwigilacji, a które jest szczególnie wysokie w systemie, gdzie tajne służby i policja mają bezpośredni dostęp, poprzez środki techniczne, do wszystkich komunikacji telefonicznych. W szczególności, okoliczności, w których władze publiczne są upoważnione do stosowania środków tajnego nadzoru, nie są określone wystarczająco jasno. Przepisy o przerwaniu stosowania środków tajnego nadzoru nie przewidują wystarczających gwarancji przeciwko arbitralnej ingerencji. Prawo krajowe zezwala na automatyczne przechowywanie nieadekwatnych danych i nie jest wystarczająco jasno określone, w jakich przypadkach materiał z przechwytywania będzie przechowywany lub zniszczony po zakończeniu procesu. Procedury upoważnienia nie są w stanie zapewnić, ze środki tajnego nadzoru zlecane są będą tylko wówczas, gdy jest to “koniecznie w demokratycznym społeczeństwie”. Nadzór nad przechwytywaniem komunikacji nie spełnia obecnie wymogów niezależności, jak i tych odnoszących się do powierzonej władzy i kompetencji, które byłyby wystarczające do wykonywania efektywnej i stałej kontroli. Skuteczność środków odwoławczych jest osłabiona przez brak powiadamiania osoby, której komunikacje są przechwytywane o tym fakcie, lub przez brak odpowiedniego dostępu do dokumentów dotyczących przechwytywania.

303.  Jest istotne, że zidentyfikowane wyżej braki systemu prawnego wydają się mieć znaczenie dla faktycznego funkcjonowania systemu tajnego nadzoru, który istnieje w Rosji. Trybunału nie przekonują zapewnienia Rządu, że każde przechwytywanie komunikacji w Rosji jest wykonywane zgodnie z prawem na podstawie odpowiedniego upoważnienia sądowego. Przykłady zaprezentowane przez skarżącego w postępowaniach krajowych (zob. par. 12 powyżej) i w postępowaniach przez Trybunałem (zob. par. 197 powyżej) wskazują na istnienie arbitralności i nadużywania środków tajnego nadzoru, czego przyczyną są przewidziane w przepisach nieadekwatne gwarancje zabezpieczające [przed nadużyciami] (zob., dla podobnego wnioskowania *Association for European Integration and Human Rights and Ekimdzhiev,* cyt. powyżej, § 92; i, dla porównania, *Klass i Inni*, cyt. powyżej, § 59, i *Kennedy*, cyt. powyżej, §§ 168 i 169).

304.  Ze względu na braki zidentyfikowane powyżej, Trybunał uznaje, że prawo rosyjskie nie spełnia wymogów “jakości prawa” i nie jest w stanie prowadzić “ingerencji” w sposób “konieczny w demokratycznym społeczeństwie”.

305.  W związku z tym, nastąpiło naruszenie Artykułu 8 Konwencji.

II.  RZEKOME NARUSZENIE ARTYKUŁU 13 KONWENCJI

306.  Skarżący podniósł, że nie przysługiwały mu żadne efektywne środki odwoławcze dla swojej skargi na mocy Artykułu 8. Powołał się na Artykuł 13 Konwencji, który brzmi następująco:

“Każdy, kogo 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.”

307.  Mając na uwadze ustalenia na mocy Artykułu 8 Konwencji w paragrafach 286 do 300 powyżej, Trybunał stwierdza, że mimo że skarga na mocy Artykułu 13 Konwencji jest silnie powiązana ze skargą na mocy Artykułu 8 i w związku z tym musi zostać uznana za dopuszczalną, nie jest konieczne badanie jej oddzielnie (zob. *Liberty i Inni,* cyt. powyżej, § 73).

III.  STOSOWANIE ARTYKUŁU 41 KONWENCJI

308.  Artykuł 41 Konwencji stanowi:

“Jeżeli 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.  Szkody

309.  Skarżący domagał się 9 000 euro (EUR) z tytułu szkody niemajątkowej.

310.  Rząd stwierdził, że roszczenie jest wygórowane, biorąc pod uwagę, że skarżący zakwestionował przepisy prawa rosyjskiego *in abstracto* nie odczuwając osobiście ich skutków. Uznanie naruszenia stanowiłoby, w związku z tym, wystarczające zadośćuczynienie.

311.  Trybunał powtarza, że w kontekście wykonywania wyroków zgodnie z Artykułem 46 Konwencji, wyrok, w którym uznano naruszenie Konwencji lub jej Protokołów nakłada na odpowiednie Państwa zobowiązanie prawne nie tylko do zapłaty osobom zainteresowanym każdej sumy przyznanej w ramach zadośćuczynienia, ale również do wyboru, podlegającego nadzorowi Komitetowi Ministrów, ogólnych lub/i, jeżeli jest właściwe, indywidualnych środków do przyjęcia w porządku krajowym, aby wyeliminować naruszenie uznane przez Trybunał oraz do przyznania realnego zadośćuczynienia w celu przywrócenia w najwyższym możliwym stopniu, sytuacji istniejącej przed naruszeniem. Co więcej, podczas ratyfikacji Konwencji, Umawiające się państwa zobowiązują się do zapewnienia, że ich prawo krajowe będzie z nią zgodne (zob. *Association for European Integration and Human Rights i Ekimdzhiev,* cyt. powyżej, § 111, z dalszymi odniesieniami).

312.  Trybunał stwierdza, że uznanie naruszenia stanowi wystarczające zadośćuczynienie za szkody niemajątkowe poniesione przez skarżącego.

B.  Koszty i wydatki

313.  W postępowaniu przez Izbą Trybunału skarżący wniósł roszczenie na kwotę 26,579 rubli rosyjskich (RUB, około 670 euro (EUR) wg kursu z dnia złożenia wniosku) z tytułu wydatków związanych z tłumaczeniem i korespondencją. Powoływał się na rachunki za usługi faxu i poczty, a także umowy o usługi tłumaczenia.

314.  Skarżący przed Wielką Izbą przedstawił roszczenie na kwotę 22,800 funtów brytyjskich (ok. 29,000 euro wg kursu dnia złożenia wniosku) i 13,800 euro z tytułu kosztów prawnych. Powoływał się na arkusze czasu pracy adwokatów. Powołując się na rachunki i faktury, wnosił również o wypłatę 6,833.24 funtów brytyjskich (ok. EUR 8,700 wg kursu z dnia złożenia wniosku) za tłumaczenia, podróże i inne wydatki administracyjne.

315.  Rząd zaakceptował roszczenie w przedmiocie kosztów i wydatków poniesionych przed Izbą, ponieważ były one poparte dokumentami dowodowymi. Co do roszczeń w przedmiocie kosztów i wydatków poniesionych przed Wielką Izbą, Rząd stwierdził, że roszczenia zostały przedstawione dłużej niż miesiąc po rozprawie. Co do kosztów prawnych, Rząd stwierdził, że część tych opłat pokryła praca wykonana przez przedstawicieli, zanim skarżący podpisał pełnomocnictwo na rzecz Pani Levine. Co więcej, ilość przedstawicieli i ilość godzin spędzonych przez nich na przygotowywaniu do sprawy była nadmierna. Dodatkowo, nie było dowodów, że skarżący zapłacił koszty pomocy prawnej, o których mowa ani, że umowa zobowiązywała go do ich zapłaty. Co do tłumaczeń i innych wydatków administracyjnych, Rząd stwierdził, że skarżący nie przedłożył żadnych dokumentów wykazujących, że zapłacił żądane kwoty. Nie udowodnił również, że wydatki na tłumaczenie były rzeczywiście konieczne, mając na uwadze, że niektórzy adwokaci skarżącego mówili po rosyjsku. Stawki żądane przez tłumaczy były wygórowane. Wreszcie, koszty podróży były również nadmierne.

316.  Zgodnie z orzecznictwem Trybunału, skarżący jest uprawniony do zwrotu kosztów i wydatków w tym zakresie, w którym wykazał, że były one rzeczywiście i koniecznie poniesione oraz w rozsądnej wysokości. W niniejszej sprawie, mając na uwadze posiadane dokumenty i powyższe kryteria, Trybunał uznał za rozsądne przyznanie sumy 40,000 euro na pokrycie wszystkich kosztów powiększonej o jakikolwiek podatek, jaki może zostać nałożony na skarżącego.

C.  Odsetki za zwłokę

317.  Trybunał uznaje za właściwe, by odsetki z tytułu niewypłacenia zasądzonych kwot zostały ustalone zgodnie ze stopą kredytową Europejskiego Banku Centralnego powiększoną o trzy punkty procentowe.

Z TYCH PRZYCZYN TRYBUNAŁ

1.  *Dołącza,* jednogłośnie, do meritum sprawy zarzut Rządu co do braku statusu ofiary skarżącego i niewyczerpania krajowych środków odwoławczych oraz *uznaje* skargę za dopuszczalną;

2.  *Uznaje*, jednogłośnie, że nastąpiło naruszenie Artykułu 8 Konwencji i *oddala* wyżej wymienione zarzuty Rządu;

3.  *Uznaje,* jednogłośnie, że nie ma potrzeby badania skargi na podstawie Artykułu 13 Konwencji;

4.  *Uznaje*, przewagą głosów szesnaście do jednego, że uznanie naruszenia stanowi samo w sobie wystarczające słuszne zadośćuczynienie za szkodę niemajątkową doznaną przez skarżącego;

5.  *Uznaje*, jednogłośnie,

(a)  że pozwane Państwo ma zapłacić skarżącemu w ciągu trzech miesięcy, kwotę 40,000 EUR (czterdzieści tysięcy euro), powiększoną o podatek, jaki może zostać nałożony na skarżącego, z tytułu zwrotu poniesionych kosztów i wydatków;

(b)  że od upływu wyżej wymienionego trzymiesięcznego terminu do momentu zapłaty od kwot tych będą naliczane zwykłe odsetki obliczone według stopy procentowej Europejskiego Banku Centralnego na koniec dnia powiększonej o trzy punkty procentowe;

6.  *Oddala*, jednogłośnie, pozostałą część wniosku skarżącego o słuszne zadośćuczynienie.

Sporządzono w języku angielskim i francuskim i obwieszczono podczas publicznej rozprawy w Gmachu Europejskiego Trybunału Praw Człowieka w Strasburgu, dnia 4 grudnia 2015 roku.

 Lawrence Early Dean Spielmann
 Radca Prawny Przewodniczący

Zgodnie z artykułem 45 ust. 2 Konwencji oraz artykułem 74 ust. 2 Regulaminu Trybunału do niniejszego wyroku załączono następujące opinie odrębne:

(a)  Opinia zbieżna Sędziego Dedova;

(b)  Częściowo zbieżna opinia Sędzi Ziemele.

D.S.
T.L.E.

OPINIA ZBIEŻNA SĘDZIEGO DEDOVA

**1.  Kompetencje Trybunału do zbadania prawa krajowego *in abstracto***

Jak zauważył Rząd, mogą pojawić się wątpliwości co do kompetencji Trybunału do badania jakości i efektywności prawa krajowego *in abstracto* bez ustalenia statusu ofiary skarżącego i bez ustalenia, że nastąpiła ingerencja w jego prawo do poszanowania życia prywatnego w praktyce, a nie wyłącznie w teorii.

Takie podejście zostało już przyjęte przez Trybunał w sprawach o przechwytywanie danych w celu zapobieżenia potencjalnym nadużyciom władzy. W dwóch głównych sprawach, *Kennedy przeciwko Zjednoczonemu Królestwu* (nr 26839/05, §§ 122-123, 18 maja 2010) oraz *Klass i Inni przeciwko* Niemcom(6 września 1978, § 34, Serie A nr 28), przeciwko dwóm prominentnym państwom demokratycznym, mianowicie Zjednoczonemu Królestwu i Republice Federalnej Niemiec, Trybunał uznał efektywność odpowiedniego systemu krajowego przeciwko arbitralności. Jednakże, co należy przyjąć z żalem, nie możemy ignorować faktu, że te dwa państwa były ostatnio zamieszane w większe, szeroko publikowane skandale dotyczące nadzoru. Po pierwsze, konwersacje Kanclerz Niemiec prowadzone przez telefon komórkowy były przechwytywane przez krajowe tajne służby; po drugie, władze Zjednoczonego Królestwa udostępniły tajnym służbom USA informacje o całej wcześniej zgromadzonej państwowej bazie danych komunikacji, co skutkowało tym, że władze USA mogły przejmować dane obywateli Zjednoczonego Królestwa bez podlegania jakimkolwiek przepisom krajowym dotyczącym bezpieczeństwa.

To wskazuje, że coś było nie tak z podejściem Trybunału od samego początku. Prawdopodobnie o wiele bardziej skuteczne byłoby rozpatrywanie poszczególnych skarg, przez co Trybunał miałby okazję do ustalenia zakresu ingerencji i uznania naruszenia Konwencji, co w rzeczy samej robi w przypadku nieusprawiedliwionych przeszukań mieszkania skarżącego. Mówiąc ogólnie, problem w tych sprawach nie dotyczy kompetencji sądów krajowych, ale sposobu, w jaki sędziowie autoryzują wnioski o przeszukania w związku ze śledztwem.

Tym samym zamiast rozpoznawać faktyczne naruszenie prawa, badana jest potencjalna możliwość ingerencji władz. Poniżej przywołane są przykłady ze sprawy Kennedy:

“119. Trybunał konsekwentnie orzekał, że jego zadaniem nie jest weryfikacja prawa i praktyki *in abstracto*, lecz ustalenie, czy sposób ich zastosowania wobec skarżącego nie przyczynił się do naruszenia Konwencji (zob. *inter alia*, *Klass i Inni*, cytowany wyżej, § 33; *N.C. przeciwko Włochom [GC]*, nr 24952/94, § 56, ETPC 2002-X; *Krone Verlag GmbH & Co. KG przeciwko Austrii (nr 4)*, nr 72331/01, § 26, 9 listopada 2006)”;

i ze sprawy *Klass*:

“36... Trybunał stwierdza, że nie jest do zaakceptowania stan, w którym zapewnienie korzystania z prawa gwarantowanego w tej Konwencji mogłoby być uchylone przez zwykły fakt utrzymywania osoby zainteresowanej w niewiedzy co do jej naruszenia. Prawo odwołania się do Komisji osób potencjalnie dotkniętych niejawnym stosowaniem środków kontroli wynika z treści art. 25, ponieważ inaczej pojawia się ryzyko pozbawienia znaczenia treści art. 8.”

Niemniej wspomniany wyżej niemiecki oraz angielski skandal potwierdza, że prędzej czy później osoba zainteresowana stanie się świadoma przechwytywania. Znaleźć można istotne przykłady w kontekście rosyjskim (zob. *Shimovolos przeciwko Rosji*, nr 30194/09, 21 czerwca 2011). Skarżący w prezentowanej sprawie nie jest świadomy jakiegokolwiek przechwytywania łączności i fakt ten nie może być zignorowany przez Trybunał.

Trybunał wielokrotnie unikał badania spraw *in abstracto* (zob. *Silver i Inni przeciwko Zjednoczonemu Królestwu,* 25 marca 1983, Seria A nr 61, § 79; *Nikolova przeciwko Bułgarii [GC]*, nr 31195/96, § 60, ETPC 1999‑II; *Nejdet Şahin i Perihan Şahin przeciwko Turcji* [GC], nr 13279/05, §§ 68-70, 20 października 2011; *Sabanchiyeva i Inni przeciwko Rosji*, nr 38450/05, § 137, ETPC 2013; *Monnat przeciwko Szwajcarii*, nr 73604/01, §§ 31-32, ETPC 2006-X). Można byłoby zatem przypuszczać, iż sprawy przechwytywania są wyjątkowe. Musielibyśmy jednak poznać powody, dla których Trybunał miałby zmienić sposób postępowania podczas badania takich spraw. Jednak nie posiadamy wiedzy na temat, jakie te powody mogłyby być. Jeśli ustawodawstwo stwarza ryzyko arbitralności, musimy tym samym poznać rezultat takiej arbitralności. Nie jestem pewien, czy kilka przykładów (niezwiązanych ze sprawą skarżącego) udowodni, iż cały system zabezpieczeń powinien zostać skorygowany i wzmocniony. Zaakceptuję takie podejście, jeśli Trybunał przedstawi serię indywidualnych, powtarzalnych petycji ukazujących, że Rozporządzenie nr 70 (dotyczące związku sprzętu służącego do przechwytywania z siecią użytkowników) nie jest techniczne w naturze, lecz stwarza w Rosji problemy strukturalne. W takim wypadku potrzebna będzie jednakże pilotażowa procedura oraz pilotażowy wyrok.

Wszystkie sprawy, w których Trybunał doszukał się pogwałcenia Konwencji (więcej niż 15 tysięcy wyroków), oparte są na nadużyciu władzy, nawet tam, gdzie ustawodawstwo krajowe charakteryzuje się dobrą jakością. Każde nadużycie władzy jest kwestią etyki i nie może być wyeliminowane wyłącznie poprzez środki ustawodawcze.

Trybunał konsekwentnie utrzymywał, że jego zadaniem nie jest weryfikacja prawa i działalności krajowej *in abstracto* bądź zajmowanie stanowiska wobec zgodności przepisów ustawodawstwa Konwencji, lecz ustalenie, czy sposób, w jaki zostały zastosowane lub też w jaki dotyczyły skarżącego, nie przyczynił się do naruszenia Konwencji (zob. w kontekście Artykułu 14, *Religionsgemeinschaft der Zeugen Jehovas i Inni przeciwko Austrii*, nr 40825/98, § 90, 31 lipca 2008).

Artykuł 34 Konwencji nie stwarza jednostkom możliwości wystąpienia ze swego rodzaju *actio popularis* w celu uzyskania interpretacji Konwencji; nie pozwala jednostkom składać skarg przeciwko przepisom prawnym *in abstracto* tylko dlatego, że według nich naruszają one Konwencję. Zasadniczo nie wystarcza, że pojedynczy skarżący twierdzi, iż samo istnienie przepisów narusza jego prawa konwencyjne; natomiast konieczne jest, aby prawo nie było stosowane na jego niekorzyść (zob. *Klass*, cytowany wyżej, § 33). Te zasady nie mogą być stosowane w sposób dowolny.

**2.  Władza ustawodawcza i sądownicza: Trybunał powinien szanować zróżnicowanie**

Sprawa ta jest bardzo ważna z uwagi na rozdzielenie funkcji pomiędzy Trybunałem a Zgromadzeniem Parlamentarnym Rady Europy, gdyż niezbędne jest rozdzielenie kompetencji ustawodawstwa i sądownictwa. Zgromadzenie Parlamentarne przejmuje rekomendacje, rezolucje i opinie, które stanowią wytyczne dla Komitetu Ministrów, rządów krajowych, parlamentów i partii politycznych. W rezultacie, poprzez konwencje, ustawodawstwo i praktykę, Rada Europy promuje prawa człowieka, demokrację i państwo prawa. Monitoruje postęp krajów członkowskich w tych obszarach i wykonuje zalecenia poprzez niezależnych, wyspecjalizowanych członków. Europejski Trybunał Praw Człowieka rozpoznaje skargi indywidualne i międzypaństwowe, w których pojawiają się zarzuty naruszenia praw obywatelskich i politycznych ustanowionych w Europejskiej Konwencji Praw Człowieka. Biorąc pod uwagę powyższe rozdzielenie funkcji, zbadanie sprawy *in abstracto* jest podobne do sprawozdania biegłego, lecz nie do wyroku.

Morten Kjaerum, Dyrektor Agencji Praw Podstawowych Unii Europejskiej (FRA), przeprowadził wspólną debatę na temat podstawowych praw podczas Europejskiej Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE) 4 września 2014 roku. Dyrektor podkreślił:

“Ujawnione przez Snowdena informacje dotyczące masowej inwigilacji podkreśliły fakt, że ochrona danych osobowych jest zagrożona. Po analizie sytuacji w dzisiejszej Europie zauważamy, iż ochrona prawa do prywatności jest niedostateczna. Śledząc zeszłoroczne debaty, pozytywnie odbieramy podanie Parlamentu Europejskiego do Agencji Praw Podstawowych o dalsze dochodzenie w sprawie praw podstawowych i odpowiednich zabezpieczeń wobec programów inwigilacji na skalę globalną. Oczywiście będziecie powiadomieni pod koniec tego roku o wynikach powyższego badania.

Nie chodzi jednak tylko o wielkie programy inwigilacji. Pojawiły się także wątpliwości wobec nadzoru działania ogólnego mechanizmu ochrony danych w sytuacjach, kiedy podajemy dane organom służby zdrowia, organom podatkowym i innym instytucjom, publicznym lub prywatnym. Jako Agencja Praw Podstawowych dostrzegamy, że krajowe struktury kontroli w UE są obecnie zbyt słabe, aby spełniły swoje zadanie. Organy ochrony danych ustanowione we wszystkich krajach członkowskich mają istotną rolę w egzekwowaniu całkowitego systemu ochrony danych, lecz władze i zasoby krajowych organów ochrony danych pilnie wymagają wzmocnienia, a ich niezależność odpowiednich gwarancji.

W końcu podkreśliłbym również, że instytucje, którym powierzone zostają dane, prywatne czy publiczne, powinny przyjąć odpowiedzialność na dużo wyższym poziomie niż ten, którego doświadczamy dzisiaj w sytuacji, gdy tworzone przez nich zabezpieczenia nie są wystarczające.”

Spostrzeżenia te zostały zaadresowane bardziej do nowo wybranych członków Parlamentu Europejskiego (aniżeli do sędziów), odnosząc się do kwestii budzących obawy w Europie i pobudzając do utworzenia bardziej wyspecjalizowanego systemu ochrony danych. Celem przemowy było zainicjowanie publicznej debaty w celu odnalezienia skutecznych środków i promowania właściwych standardów etycznych społeczeństwa; sala sądowa nie jest miejscem dla tego rodzaju debat.

Chciałbym zasugerować, aby Trybunał z większą rzetelnością skupił się na poszczególnych zakłóceniach i skuteczności odpowiednich środków w celu zapobiegania tym konkretnym naruszeniom (tak jak Trybunał zwykle czyni w przypadku wszystkich innych spraw). Podstawowym celem Trybunału musi być: ustalenie, iż miała miejsce ingerencja oraz zbadanie, czy była ona zgodna z prawem i niezbędna w demokratycznym społeczeństwie. Dla sędziów jest to etycznie niedopuszczalne, aby zakładać, iż każdy obywatel danego kraju może być poddany bezprawnej inwigilacji bez wiedzy na ten temat. Wydany wyrok nie może opierać się na tego rodzaju zarzutach.

Trybunał użył wielu instrumentów w walce z naruszaniem przepisów. Jednym z nich było stwierdzenie naruszenia Artykułu 10 w związku z odmową dostarczenia przez kontrwywiad informacji składającej wniosek organizacji na temat osób poddanych inwigilacji w określonym czasie (*Youth Initiative for Human Rights przeciwko Serbii*, nr 48135/06, 25 czerwca 2013). W sentencji tego wyroku Trybunał wezwał Rząd do zagwarantowania, iż kwestionowane informacje zostaną udostępnione organizacji skarżącej (nie czekając na rozwiązania zaproponowane przez Komitet Ministrów). Przyznaję, że była to skuteczna metoda i orzeczniczy sukces.

**3.  Powinno zostać przyjęte podejście “realnego prawdopodobieństwa”**

Ustalenie statusu skarżącego jako ofiary jest integralną częścią postępowania sądowego. Artykuł 34 Konwencji stanowi: “Trybunał może przyjmować skargi każdej osoby, organizacji pozarządowej lub grupy jednostek, która uważa, że stała się ofiarą naruszenia przez jedną z Wysokich Układających się Stron praw zawartych w niniejszej konwencji lub jej protokołach.” Pojęcie “ofiary” nie implikuje zaistnienia prawomocności (zob. *Brumărescu przeciwko Rumunii* [GC], nr 28342/95, § 50, ETPC 1999‑VII).

Trybunał uprzednio orzekł, że tak długo, jak istnienie reżimu inwigilacji może ingerować w prywatność, stwierdzenie o naruszeniu praw stanowi przedmiot oceny sądu tylko , gdy występuje “realne prawdopodobieństwo”, że osoba została poddana nieprawnej inwigilacji (zob. *Esbester przeciwko Zjednoczonemu Królestwu,* nr 18601/91, decyzja Komisji z 2 kwietnia 1993; *Redgrave przeciwko Zjednoczonemu Królestwu*, wniosek nr 202711/92, decyzja Komisji z 1 września 1993; *Matthews przeciwko Zjednoczonemu Królestwu*, wniosek nr 28576/95, decyzja Komisji z 16 października 1996). Te odwołania prowadzą do stwierdzenia niedopuszczalności skarg ze względu na to, że wszystkie zarzuty przechwytywania zostały uznane za ewidentnie niezasadne.

Jednakże, Trybunał całkowicie zmienił postępowanie w przypadku sprawy *Klass: “…* nie można wykluczyć, iż środki tajnej inwigilacji były wobec niego podjęte lub że istniało potencjalne ryzyko ich zastosowania” (*Klass*, cytowany wyżej, §§ 125-129). Dzisiaj dostrzegamy, że ta zmiana orzecznictwa nie była efektywna.

Pojęcie “realnego prawdopodobieństwa” sugeruje pojawienie się negatywnych następstw dla skarżącego, który jest potencjalnie poddany tajnej inwigilacji z racji określonych informacji udostępnionych władzom poprzez przechwytywanie komunikacji, a także wykluczenie możliwości, że informacje te mogłyby być odkryte innymi środkami. Trybunał niebezpiecznie uprościł podejście w celu rozpatrzenia istoty tych spraw, zakładając, że osoby poddane tajnemu nadzorowi przez władze nie zawsze są poinformowane o użyciu tych środków i w rezultacie skarżący nie mogą udowodnić naruszenia ich praw. W takich wypadkach Trybunał orzekał, że skarżący muszą być uznani za zdolnych do składania skarg, nawet jeśli nie mogą udowodnić poniesionej szkody. Skarżący w sprawach *Klass* i *Liberty* (*Liberty i Inni przeciwko Zjednoczonemu Królestwu*, nr 58243/00, 1 lipca 2008) byli prawnikami i teoretycznie “mogli być poddani tajnej inwigilacji w wyniku możliwych kontaktów z klientami podejrzanymi o nielegalne działania” (*Klass*, § 37).

W sprawie *Kennedy* skarżący stwierdził, że połączenia miejscowe na jego telefon nie były przez niego odbierane i że otrzymywał wiele marnujących czas głuchych telefonów. Skarżący podejrzewał, że jego poczta, telefon oraz korespondencja elektroniczna były przechwytywane, tak więc Trybunał poważnie wziął to pod uwagę, odrzucając zastrzeżenia Rządu wobec zdolności skarżącego do wykazania przechwytywania w kontekście Artykułu 8 oraz wobec zaistnienia realnego prawdopodobieństwa. Trybunał odrzucił także niewyczerpane zgłoszenia w duchu tego, że skarżący nie sprawdził jakości usług telekomunikacyjnych jego operatora, lecz złożył wnioski o udzielenie dostępu do danych od MI5 i GCHQ (agencji wywiadu Zjednoczonego Królestwa odpowiedzialnych za bezpieczeństwo narodowe) wynikających z Ustawy o ochronie danych osobowych z 1998 roku.

Wracając do okoliczności aktualnej sprawy, można słusznie wywnioskować, że połączenia między urządzeniami telekomunikacyjnymi a sprzętem do przechwytywania informacji niekoniecznie wiążą się z tym, że przechwytywanie komunikacji telefonicznych skarżącego rzeczywiście miało miejsce. Trybunał nie może także oprzeć swoich ustaleń o domniemanie “możliwości niepoprawnych działań przez nieuczciwych, dopuszczających się zaniedbań, nadgorliwych urzędników” (zob. *Klass*, §§ 49, 50, 59; *Weber i Saravia przeciwko Niemcom* (dec.), nr 54934/00, § 106, ETPC 2006‑XI; *Kennedy*, §§ 153-154). Tym samym Trybunał nie może generalnie zakładać (w celu rozpatrzenia sprawy *in abstracto*) istnienia państwowej przemocy skierowanej przeciw ruchom opozycyjnym i innym demokratycznym instytucjom pozwanego państwa, nawet jeśli odpowiednie rozporządzenia zostały uchwalone przez Zgromadzenie Parlamentarne. Trybunał musi zachować swoją bezstronność i neutralność.

**4.  Rola sądownictwa w społeczeństwie obywatelskim**

Niemniej jednak opowiedziałem się za dopuszczalnością i za uznaniem naruszenia Artykułu 8 Konwencji ze względu na to, że zasadnicze znaczenie zabezpieczeń chroniących łączności prywatne przed arbitralną inwigilacją, szczególnie w kontekście niezwiązanym ze stosowaniem prawa karnego, nie zostało nigdy uwzględnione podczas postępowań o charakterze krajowym. Rosyjskie sądy odmówiły rozpoznania zarzutów skarżącego, błędnie nawiązując do natury technicznej zaskarżonych rozporządzeń ministerialnych. Jako sędzia sądu krajowego nie mogę zignorować faktu, iż w Rosji istnieje powszechne podejrzenie, że inwigilacja jest prowadzona wobec postaci życia politycznego, biznesowego, działaczy i przywódców opozycji, dziennikarzy, urzędników państwowych, osób sprawujących pieczę nad majątkiem państwa – innymi słowy wobec wszystkich, którzy są zaangażowani w sprawy publiczne. Takie podejrzenie wynika z przeszłych doświadczeń reżimu totalitarnego z czasów Związku Radzieckiego czy z długiej historii Imperium Rosyjskiego.

Ten wyrok mógłby służyć jako podstawa do usprawnienia systemu ustawodawstwa w sferze czynności operacyjno-rozpoznawczych oraz do ustalenia skutecznego systemu kontroli publicznej nad inwigilacją.
Co więcej, wyrok ten świadczy o tym, że jeśli istnieje w społeczeństwie powszechne podejrzenie i nie ma żadnej innej możliwości obalenia tego podejrzenia bez zawarcia umowy społecznej i dokonania stosownych zmian w prawie i praktyce krajowej, to tam, gdzie problem nie zostanie zidentyfikowany przez inne organy władzy, sądy muszą działać aktywnie w celu ułatwienia tych zmian. Jest to nawet bardziej ewidentne, gdy nie ma dostępnych żadnych innych środków chroniących demokrację
i praworządność. Jest to istotne zadanie, które organy władzy sądowniczej muszą pełnić w społeczeństwie obywatelskim.

Trybunał mógłby być skrytykowany za niedostarczenie bardziej precyzyjnego uzasadnienia dla podjętego badania *in abstracto* w określonym kontekście społecznym, zwłaszcza że swoje uzasadnienie oparł jedynie na odwołaniu się do orzecznictwa jego własnej Izby. Jednakże, wydanie wyroku w niniejszej sprawie jest wyjątkowo trudne, ponieważ przed jej rozstrzygnięciem sędziowie musieli ustalić, czy wszystkie inne środki okazały się zbyteczne. Natomiast w sprawie *Clapper przeciwko  Amnesty International USA* (568 U.S. , 2013) Sąd Najwyższy Stanów Zjednoczonych nie podjął kroku naprzód mimo istnienia programu masowej inwigilacji i “powszechnego podejrzenia” jego istnienia (lub innymi słowami, autorstwa Justice Breyer: “[krzywda] ma takie samo prawdopodobieństwo wystąpienia jak i większość przyszłych wydarzeń, które zdrowy rozsądek i zwykła znajomość natury ludzkiej nam podpowiadają i przewidują”). W zamian za to odrzucił argument skarżących (w tym organizacji praw człowieka, organizacji prawnych oraz medialnych) jako niewystarczający i uznał, że z natury na rodzaj wykonywanej przez nich pracy bycie podmiotem inwigilacji jest prawdopodobne.

Powinienem się tutaj zatrzymać, pozostawiając dyskusję nad sądową agresją, aktywizmem bądź powściągliwością pracownikom naukowym. Chciałbym tylko zakończyć moją opinię, cytując spostrzeżenie Edwarda Snowdena: “Z każdym wygranym procesem, z każdą zmianą prawa wykazujemy, że fakty są bardziej przekonujące od strachu. Jako społeczeństwo na nowo odkrywamy, że wartością prawa nie jest to, co ono ukrywa, lecz to, co chroni”.

OPINIA ZBIEŻNA SĘDZI ZIEMELE

1.  Całkowicie zgadzam się z uznaniem naruszenia przepisów w tej sprawie. Trybunał dokonał zasadniczo bardzo ważnego osądu, gdyż tajna inwigilacja prowadzona w taki sposób, jak opisano to w niniejszej sprawie, jest w istocie niezgodna z zasadą państwa prawa oraz z zasadami demokracji.

2. Szczególnie w takim kontekście nie mogę zgodzić się z decyzją Trybunału, aby nie przyznać kompensaty za poniesioną długotrwale krzywdę. Uważam, że roszczenie o odszkodowanie skarżącego jest bardzo rozsądne (zob. paragraf 309 wyroku) oraz że orzeczenie o naruszeniu przepisów, choć co do zasady jest istotne w tej sprawie, to nie jest odpowiednio zadowalające w szczególnej sytuacji skarżącego. Tym samym nie zgadzam się z punktem 4 sentencji wyroku.